НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ

РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, УЧИНЕНИХ З ВИКОРИСТАННЯМ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ

(методичні рекомендації)

Київ 2016

УДК 343.98 : 343.346.8 : 004
ББК Х 629.4
Р 654

Авторський колектив: Арешонков В. В. – кандидат юридичних наук (Національна академія внутрішніх справ); **Вакуленко О.Ф.** – Головне слідче управління Національної поліції; **Василинчук В. І.** – доктор юридичних наук, професор (Національна академія внутрішніх справ); **Вознюк А. А.** – кандидат юридичних наук, старший науковий співробітник (Національна академія внутрішніх справ); **Волков О. О.** – Головне слідче управління Національної поліції; **Галаган В. І.** – кандидат юридичних наук, доцент (Національна академія внутрішніх справ); **Дрозд О. Ю.** – кандидат юридичних наук, доцент (Національна академія внутрішніх справ); **Кінаш О. Л.** – Головне слідче управління Національної поліції; **Кузьмічова-Кисленко Є. В.** – кандидат юридичних наук (Національна академія внутрішніх справ); **Плєва К. В. –** кандидат юридичних наук (Національна академія внутрішніх справ); **Стрільців О. М.** – кандидат юридичних наук, старший науковий співробітник (Національна академія внутрішніх справ); **Тарасенко О. С.** – кандидат юридичних наук (Національна академія внутрішніх справ); **Фурман Я. В.** – кандидат юридичних наук (Національна академія внутрішніх справ); **Цуцкірідзе М. С.** – кандидат юридичних наук (Головне слідче управління Національної поліції.

Рецензенти

Рибальський О. В. – професор кафедри інформаційних технологій навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ, доктор технічних наук, професор;

Іщенко А. В. – професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ, доктор юридичних наук, професор, Заслужений юрист України.

Рекомендовано Головним слідчим управлінням Національної поліції України та науково-методичною радою Національної академії внутрішніх справ.

Р 654 Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів [Текст] : метод. рек. / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. – К., 2016. – 55 с.

Методичні рекомендації містять кримінально-правову характеристику злочинів, учинених з використанням шкідливих програмних чи технічних засобів. Розкрито особливості здійснення слідчих (розшукових) дій під час досудового розслідування вказаної категорії злочинів: запропоновано алгоритм розслідування, визначено особливості здійснення огляду, окремих видів допиту, а також напрями встановлення осіб, які розповсюджують шкідливі програмні засоби.

Для оперативних працівників, слідчих, а також науковців, викладачів, слухачів і курсантів вищих навчальних закладів МВС України.

УДК 343.98:343.346.8:004
ББК Х 628.3

ЗМІСТ

РОЗДІЛ 1
Кримінально-правова характеристика злочинів, що вчиняються з використанням шкідливих програмних чи технічних засобів

Стаття 361-1. *Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут*

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку,

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,

караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

1.1 Об'єктивні ознаки

1.1.1 Об'єкт

Основним об'єктом даного злочину вважаються окремі суспільні відносини щодо встановленого порядку функціонування ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку.

Родовим об'єктом злочину є врегульовані законом суспільні відносини забезпечення безпеки автоматизованої обробки інформації.

Додатковим об'єктом злочину, передбаченого ст. 361-1 КК України, можуть бути суспільні відносини, пов'язані із забезпеченням власності на комп'ютерну інформацію, та відносини надання й отримання послуг електрозв'язку, виключно санкціонованого доступу до програмного і технічного забезпечення, комп'ютерної інформації, засобів мереж електрозв'язку, тобто право користувачів на доступ до зазначеної інформації та користування нею. Невід'ємною складовою зазначених правовідносин є:

– право власника (користувача) на безпеку конфіденційного чи таємного користування програмним і технічним забезпеченням, комп'ютерною інформацією, засобами мереж електрозв'язку;

– обов'язок оточуючих утримуватися від несанкціонованого втручання в роботу цих елементів. Право конфіденційності чи таємності у користуванні програмним і технічним забезпеченням, комп'ютерною інформацією, а також засобами мереж електрозв'язку є похідним від права власника (користувача) контролювати доступ до наявної інформації шляхом встановлення певного режиму, передбаченого ст. 28 Закону України «Про інформацію».

Потрібно зазначити, що специфіка механізму заподіяння шкоди цим суспільним відносинам у результаті вчинення означеного злочину полягає в тому, що через створення, розповсюдження або збут шкідливих програмних чи технічних засобів створюється реальна загроза порушення суспільних відносин власності на інформацію або відносин надання послуг електрозв'язку.

Предметом злочинного посягання можуть бути:

Електронно-обчислювальна машина (комп'ютер, ЕОМ) – комплекс технічних засобів, призначених для автоматизованої обробки інформації в процесі вирішення обчислювальних та інформаційних завдань;

Периферійне обладнання – технічні засоби, що мають підпорядкований кібернетичний статус в інформаційній системі: будь-який пристрій, що забезпечує передачу даних та команд між процесором і користувачем відносно певного центрального процесора; комплекс зовнішніх пристроїв ЕОМ, які не знаходяться під безпосереднім управлінням центрального процесора (принтер, монітор, сканер та ін.);

Інформація матеріалізується в носіях інформації, якими можуть бути фізичні об'єкти, поля і сигнали, хімічні середовища, накопичення даних в інформаційних системах.

Носії цифрової інформації – незалежні накопичувачі електронних даних, призначені для їх запису, зберігання та відтворення за допомогою спеціального програмного комплексу (дискети, лазерні диски різних форматів, флеш-карти), сигнали (у каналах зв'язку), поля (оперативна пам'ять ЕОМ та її периферійних пристроїв).

Комп'ютерна інформація – інформація, що циркулює в обчислювальному середовищі та зафіксована на фізичному носії у формі, яка є доступною для сприйняття ЕОМ, а також та, що передається телекомунікаційними каналами: сформована в обчислювальному середовищі та передається за допомогою електромагнітних сигналів з однієї ЕОМ в іншу, з ЕОМ – на периферійний пристрій чи на керівний датчик обладнання. Залежно від носія її можна класифікувати як зафіксовану на: магнітній стрічці, дискетах, лазерних дисках, магнітооптичних дисках, жорсткому диску ЕОМ, у пам'яті ЕОМ, системи ЕОМ або їх мережі.

Автоматизована система (АС) – система, що реалізує інформаційну технологію виконання встановлених функцій за допомогою персоналу і комплексу засобів автоматизації.

Комп'ютерна мережа – система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа – це система зв'язку через кабельне чи повітряне середовище.

Мережі електрозв'язку – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

1.1.2 Шкідливі програмні та технічні засоби як предмет кримінального правопорушення

Предметом злочину є шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку.

Під комп'ютерною програмою Закон України «Про авторське право та суміжні права» розуміє набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах.

Комп'ютерні програми складаються з:

1. Системних програм – операційні системи, програми технічного обслуговування: драйвери, програми-оболонки, допоміжні програми – утиліти).

2. Прикладних програм – комплекс спеціалізованих програм, призначених для вирішення певного класу завдань, наприклад, текстові редактори, антивірусні програми та системи, програми захисту від несанкціонованого доступу, табличні процесори, системи управління базами даних (СУБД), графічні редактори, системи ділової та наукової графіки, системи автоматизованого проектування, інтегровані системи, бухгалтерські програми, програми управління технологічними процесами і т. ін.

3. Інструментальних програм (систем програмування), що складаються з мов програмування, а також трансляторів – комплексу програм, які забезпечують автоматичний переклад з алгоритмічних і символічних мов у машинні коди.

Під ***шкідливим програмним засобом*** необхідно розуміти спеціально створені комп'ютерні програми, які прямо або побічно призначені для несанкціонованого втручання у роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку: порушують роботу як окремих програм, баз даних, видачі викривленої інформації, так і апаратних та периферійних засобів;

порушують нормальне функціонування мереж; дезорганізують процес обробки інформації; сприяють втраті або перекручуванню інформації; копіюють інформацію без збереження первинної копії тощо[1].

Шкідливі програмні продукти відрізняються від дефективного програмного забезпечення тим, що останнє є легальним програмним забезпеченням, але містить шкідливі помилки, які не були виправлені до випуску. Крім того, існує велика кількість програм, які за своєю природою не є шкідливими програмними засобами, але здатні спричинити порушення в роботі електронно-обчислювальних машин.

Так, якщо несанкціоноване втручання у роботу комп'ютерів, автоматизованих систем чи комп'ютерних мереж було здійснено, наприклад, методом підбору кодів та паролів, то такі діяння слід кваліфікувати за ст. 361 КК України. Якщо ж таке втручання опосередковане шкідливою комп'ютерною програмою або шкідливими технічними засобами, кваліфікацію необхідно здійснювати за сукупністю злочинів, передбачених статтями 361 та 361-1 КК України.

Як предмет злочину комп'ютерні програми (програмні засоби) повинні бути шкідливими, тобто здатними забезпечити несанкціонований доступ до інформації, а також змінити, знищити, пошкодити, заблокувати комп'ютерну інформацію чи ту, яка передається мережами електрозв'язку.

Цей факт має встановлюватися експертизою комп'ютерної техніки і програмних продуктів, виходячи з кожного конкретного випадку (наприклад, з урахуванням рівня архітектурної будови комп'ютера та віднесення його до того чи іншого покоління ЕОМ, або за іншими ознаками).

Найпоширенішими різновидами шкідливих програмних засобів є:

1) *комп'ютерні віруси* – комп'ютерні програми, здатні після несанкціонованого проникнення до операційної системи ЕОМ чи до АС порушити нормальну роботу комп'ютера, АС чи комп'ютерної мережі, а також знищити, пошкодити або змінити комп'ютерну інформацію чи спричинити інші негативні наслідки. Характерною ознакою вірусів вважається їх здатність до самовідтворення та модифікації програми, до якої вони приєднуються;

− *автономні агенти* – програми або фрагменти програм, які діють незалежно від користувача, самостійно вибирають систему для «нападу» і використовують її вразливі місця (найбільш відомими автономними агентами є комп'ютерні віруси, які не тільки самостійно обирають об'єкт «зараження», але ще й створюють копії самих себе, розсилаючи їх іншим абонентам);

− *«троянський кінь»* − програма, яка приховано встановлюється будь-яким способом на віддаленому комп'ютері, як правило, шляхом вбудовування в іншу легальну програму. При цьому програма-носій, виконуючи свої прямі функції,

[1] Кодификатор компьютерных преступлений Генерального Секретариата Интерпола 1991 года / [Электронный ресурс]. – Режим доступа : http://www.interpol.int/Public/TechnologyCrime/default.asp.

здійснює додаткові функції, закладені в неї розробником (наприклад, збирання та передача в мережу паролів, або реєстрація всіх натискань клавіш на клавіатурі);

2) *засоби перехоплення трафіку (сніффери)* – програми, які дозволяють перехоплювати дані, що передаються по мережах електрозв'язку, а також призначені для нейтралізації паролів, логінів користувачів та інших засобів захисту комп'ютерних програм чи комп'ютерної інформації від несанкціонованого доступу;

3) *програми-шпигуни,* які після їх проникнення до певної АС, комп'ютерної мережі, операційної системи ЕОМ чи окремої комп'ютерної програми забезпечують несанкціонований доступ сторонньої особи до інформації, яка зберігається у ЕОМ, АС, мережі чи програмі або ж непомітно для власника чи законного користувача здійснюють несанкціоновану передачу такої інформації сторонній особі.

Вчинення такого виду злочину в сфері використання ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку полягає у:

- несанкціонованому втручанні у роботу ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку;

- створенні з метою використання, розповсюдження або збуту, а також розповсюдженні або збуті шкідливих програмних продуктів, призначених для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку;

- несанкціонованих діях з інформацією, яка оброблюється в ЕОМ (комп'ютерах), АС, комп'ютерних мережах чи мережах електрозв'язку;

- порушенні правил експлуатації ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

Залежно від місця створення шкідливого програмного чи технічного засобу і місця їх подальшого використання способи створення можна розділити на:

- створення безпосередньо на місці їх використання;

- створення поза місцем їх використання.

За способом створення шкідливого програмного засобу можна виділити на дві групи:

- створення вірусу;

- внесення змін в існуючі шкідливі програмні засоби.

Способами створення шкідливих програмних засобів є:

1. Реалізація алгоритму шкідливого програмного засобу без використання користувальницьких бібліотек функцій мови програмування, тобто його модифікація.

2. Реалізація алгоритму шкідливого програмного засобу з використанням користувача бібліотек функцій мови програмування.

3. Створення (компонування) шкідливих програмних засобів з використанням спеціальних засобів автоматизованої розробки.

4. Створення шкідливого програмного засобу шляхом використання

програм-конструкторів (спеціальні утиліти), що дозволяють генерувати вихідні дані із заздалегідь необхідними зловмиснику функціями, об'єктних модулів або безпосередньо заражених файлів.

Внесення змін до існуючих програм можливе двома способами:

1. Внесення злочинцем змін в існуючу програму шляхом зміни її машинного коду з використанням власного оригінального алгоритму реалізації.

2. Внесення злочинцем змін в існуючу програму шляхом зміни її машинного коду з використанням запозиченого алгоритму реалізації.

Виходячи з технічних особливостей комп'ютерної інформації, розповсюджуватися шкідливий програмний засіб можливо лише в декількох фізичних формах:

- разом з машинним носієм (наприклад, передача дискети, компакт-диска, флеш-диска та ін.);

- разом з комп'ютером (наприклад, переміщення ноутбука власником з одного місця в інше);

- усередині локальної мережі або в глобальній мережі Інтернет по лініях зв'язку (наприклад, перенесення вірусу з жорсткого диску сервера на локальні комп'ютери або перенесення «зараженого» листа електронною поштою).

За способами розповсюдження шкідливих програмних засобів їх можна поділити на:

- активні;

- пасивні.

Активні способи вчинення злочину характеризуються діями злочинця, пов'язаними з його доступом до комп'ютерної інформації, подальшим впровадженням шкідливого програмного засобу. Активні способи розповсюдження шкідливих програмних засобів мають чітко виражену багатоступеневу структуру дій: доступ до комп'ютерної системи − доступ до програмного забезпечення або інших файлів у комп'ютерній системі − впровадження шкідливого програмного засобу – використання (управління функціонуванням) шкідливого програмного засобу.

Активні способи можна розділити на три групи залежно від способу доступу до комп'ютерної інформації:

1. Безпосередній доступ до комп'ютерної інформації.

2. Опосередкований (віддалений) доступ до комп'ютерної інформації.

3. Змішаний (безпосередній та опосередкований (віддалений)) доступ до комп'ютерної інформації.

До пасивних способів розповсюдження шкідливих програмних засобів слід віднести всі способи, при яких дії злочинця не пов'язані з отриманням доступу до комп'ютерної інформації, а саме:

1. Розміщення файлів із шкідливим програмним засобом у локальних мережах ЕОМ.

2. Розміщення файлів із шкідливим програмним засобом у мережі

Інтернет.

3. Розсилка шкідливих програмних засобів по електронній пошті.

4. Розміщення файлів із шкідливим програмним засобом на ЕОМ загального користування.

На підставі зазначеного можна зробити висновок, що шкідливими програмними засобами є комп'ютерні програми, які за своїм функціональним призначенням та алгоритмічною побудовою здатні безпосередньо впливати на встановлений процес роботи ЕОМ (комп'ютерів), АС та комп'ютерних мереж.

Основним критерієм оцінки такого програмного засобу є його «шкідливий вплив». Причому характерною їх ознакою є те, що зазначений вплив здійснюється без відома законного користувача або всупереч його волі. Дія ж шкідливої програми може бути як керованою ззовні, так і повністю автономною (внаслідок прописаного у ній самій алгоритму).

Шкідливі технічні засоби – це різного роду прилади, обладнання, устаткування тощо, за допомогою яких без використання комп'ютерних програм здійснюється вплив на роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку з метою впливу на процес обробки інформації, призвести до її витоку, втрати (знищення), підробки (фальсифікації), блокування, спотворення процесу обробки або до порушення встановленого порядку її маршрутизації.

Підключення та вплив можуть здійснюватися у двох формах:

фізичній – безпосереднє підключення до ЕОМ, АС або комп'ютерних мереж чи мереж електрозв'язку за допомогою встановлення апаратних закладних пристроїв;

електронній – шляхом формування сигналів, полів, середовищ створити умови для несанкціонованого доступу до ЕОМ, АС або комп'ютерних мереж чи мереж електрозв'язку.

Такі підключення можуть здійснюватися з доступом чи без доступу в приміщення за допомогою індукційних або гальванічних сполучень, маніпуляцій з телекомунікаційними пристроями і системами виробничого радіозв'язку, радіорелейного чи супутникового зв'язку, а також цифрових мобільних телефонів.

По відношенню ж до технічних засобів таке визначення є досить умовним, оскільки це, передусім, прилади, устаткування, які не мають функціонально закладених у них шкідливих властивостей, і їх використання може бути як соціально-корисним або нейтральним, так і шкідливим, залежно від мети використання. Так, устаткування, призначене для діагностики роботи комп'ютерної мережі, може бути використане для виявлення та ліквідації неполадок у роботі (тобто за прямим призначенням), так і для з'ясування слабких місць у захисті ЕОМ, АС або комп'ютерних мереж чи мереж електрозв'язку під час незаконного підключення. Пристрій, що імітує (емулює) роботу карт певного оператора зв'язку, може в рівній мірі використовуватись як для копіювання карт у разі їх втрати законними

користувачами, для налагодження роботи мережі, так і для здійснення безоплатних розмов або безоплатного доступу до мережі Інтернет. Пристрої, за допомогою яких здійснюється пригнічення інформаційних сигналів, використовуються як для захисту конфіденційної інформації (із соціально-корисною метою), так і для блокування передачі даних, яка здійснюється на законних підставах (із шкідливою метою).

Тобто ті ж самі технічні засоби можуть у різних випадках використовуватися як для діагностики та налагодження роботи ЕОМ (комп'ютерів), АС або комп'ютерних мереж чи мереж електрозв'язку, так і для незаконного (несанкціонованого) втручання у встановлений процес їх роботи. Обов'язковою ознакою шкідливих технічних засобів є те, що своїм призначенням вони сприяють несанкціонованому втручанню в роботу ЕОМ, АС або комп'ютерних мереж чи мереж електрозв'язку, або безпосередньо здатні спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації і можуть виступати у разі їх використання в подальшому як засоби вчинення злочину. Відсутність цієї ознаки виключає можливість визнати вказані програмні чи технічні засоби предметом злочину, передбаченого ст. 361-1 КК України. Отже, говорити про шкідливість технічних засобів можливо лише в контексті мети їх застосування, яка й буде визначати злочинність діяння або відсутність ознак злочину в діях особи.

1.1.3 Об'єктивна сторона

Об'єктивна сторона аналізованого злочину характеризується вчиненням наступних діянь:

- створення шкідливих програмних засобів;
- створення шкідливих технічних засобів;
- використання шкідливого технічного засобу;
- використання шкідливого програмного засобу;
- збут шкідливого програмного засобу;
- збут шкідливого технічного засобу;
- розповсюдження шкідливого програмного засобу;
- розповсюдження шкідливого технічного засобу.

Створення шкідливих програмних засобів – це дії, в результаті яких відбувається фізична матеріалізація (факт створення) шкідливого програмного засобу на носії інформації або в просторових формах. Під створенням шкідливої програми необхідно розуміти творчу діяльність суб'єкта, спрямовану на створення якісно нової програми, завідомо наділеної функціями, виконання яких спричиняє протиправний вплив на комп'ютерну інформацію, процеси її автоматизованої обробки та електронно-обчислювальні засоби.

Створення шкідливих програмних засобів включає в себе написання алгоритму шкідливої програми для ЕОМ з наступним (обов'язковим) перетворенням його у машинну мову. Причому внесення змін до вже

існуючої комп'ютерної програми, внаслідок чого вона набуває ознак шкідливості, або якщо у неї додалися нові шкідливі функції, чи у результаті подібних змін було створено якісно нову шкідливу програму для ЕОМ, також слід вважати створенням. Характер змін, що вносяться в існуючу програму, може бути різним: додавання, вилучення, дублювання частини машинного коду та інші можливі модифікації програми, які можуть стосуватися і шкідливих функцій.

Обов'язковою умовою доказування під час досудового розслідування має бути визначення мети створення програмного засобу, а саме, його використання, розповсюдження або збут для несанкціонованого втручання. Тобто, якщо вказане забезпечення було створене, наприклад, виключно з дослідницькою метою, то таке діяння не повинно вважатися караним. Якщо ж мала місце злочинна ціль (будь-яка з перелічених), кримінальна відповідальність повинна наставати за сам факт створення, незалежно від реалізації такої мети.

Так, на початку квітня 2010 року ОСОБА_2, діючи умисно з корисливих мотивів, перебуваючи у себе вдома, а саме на орендованій квартирі у м. Харкові, використовуючи власний ноутбук торгової марки «DELL», моделі «Vostro3700», серійний номер № 2FH87L1, можливість доступу до мережі Інтернет, а також власний досвід у сфері створення програмного забезпечення, на мові програмування «С++» шляхом написання вихідних кодів розпочав створення шкідливого програмного засобу - шкідливої комп'ютерної програми під назвою «ІНФОРМАЦІЯ_11», призначеної для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), якій у подальшому ним було надано умовну назву «ІНФОРМАЦІЯ_12», з метою його збуту через мережу Інтернет.

Створення шкідливих технічних засобів полягає у виготовленні будь-яким способом відповідного пристрою, обладнання чи устаткування. Причому, зважаючи на специфічність такого устаткування, виготовлення може полягати не лише у його фізичному збиранні, а й, наприклад, у розробці чи налагодженні устаткування відповідним чином або його програмуванні (перепрограмуванні), після чого пристрій набуватиме ознак шкідливості.

Так, гр-н К. у м. Ірпінь, з корисливих мотивів, придбав у невстановленої особи чисту картку-емулятор (тобто здатну імітувати дію іншого пристрою) та коди KI та IMSI сім-картки китайського оператора мобільного зв'язку. Надалі він вставив у свій мобільний телефон картку-емулятор та ввів у неї отримані коди KI та IMSI, внаслідок чого зазначена картка стала клоном оригінальної сім-картки, за допомогою якої стало можливо здійснювати емуляцію її роботи. Таким чином, даний громадянин створив шкідливий технічний засіб, призначений для несанкціонованого втручання в роботу мереж електрозв'язку, після чого активував означену сім-картку в своєму власному телефоні та здійснював дзвінки на свій

телефон, у якому знаходилась сім картка оператора мобільного зв'язку «Білайн», унаслідок чого отримав грошовий бонус на вказаний номер.

Оскільки у своєму первинному вигляді картка-емулятор не мала шкідливих функцій, що також характеризує і окремо взяті коди зв'язку, то можна вважати, що здатність впливати на процес роботи мереж електрозв'язку технічний засіб отримав унаслідок його відповідного налагодження (програмування).

Таким чином, створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів пропонується вважати закінченим з моменту набуття створюваної програми або пристрою ознак шкідливості (тобто їх властивості негативно впливати на встановлений порядок обробки інформації).

Розповсюдження шкідливих програмних засобів – це будь-яка дія, безпосередня чи опосередкована пропозиція, за допомогою якої ці об'єкти (зокрема, комп'ютерні віруси) поширюються чи починають автоматично відтворюватись у ЕОМ, АС або комп'ютерних мережах чи мережах електрозв'язку в результаті їх «закладання» в програмне забезпечення, а також створення умов, за яких інші особи можуть здійснити доступ до них або отримати у користування з будь-якого місця і в будь-який час за власним вибором, у тому числі мережею та іншим способом на платній чи безоплатній основі.

За результатами такої діяльності ці об'єкти (шкідливі програмні засоби) поширюються чи починають автоматично відтворюватись у ЕОМ, АС або комп'ютерних мережах чи мережах електрозв'язку в результаті їх «закладання» в програмне забезпечення чи надання доступу до цих об'єктів невизначеному колу осіб на платній чи безоплатній основі.

Способи розповсюдження можуть бути різні: самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням комп'ютерної мережі, установка (інсталяція) таких засобів у процесі виготовлення, ремонту, реалізації, ознайомлення інших осіб зі змістом програмних і технічних засобів комбінації названих способів.

Спосіб *«закладання» шкідливих програмних засобів* у програмне забезпечення полягає в тому, що особа, яка розповсюджує ці засоби, включає шкідливу програму до складу використовуваного програмного забезпечення. Один із таких способів розповсюдження шкідливих програм одержав назву «троянський кінь». Суть його полягає в тому, що винний розповсюджує якесь корисне програмне забезпечення, наприклад, текстовий редактор, перекладач або навчальну програму, однак, крім корисних функцій, програма містить і приховані, призначені для порушення права власності на інформацію.

Розповсюдження шляхом *використання комп'ютерних мереж* полягає, як правило, у наданні доступу до шкідливих програм шляхом їх розміщення на мережевих носіях інформації або в розсиланні електронною поштою копій шкідливих програм.

Так, Кіровським районним судом м. Кіровограда засуджено А. у вчиненні злочину, передбаченого частиною першою ст. 361-1 КК України, який, користуючись локальною комп'ютерною мережею гуртожитків, діючи умисно, завантажив у власний комп'ютер програмні засоби. Ці засоби пізніше під час експертизи було визнано програмами для віддаленого зчитування паролів або нейтралізації засобів захисту комп'ютерних програм чи інформації, які після встановлення паролів та їх нейтралізації дають можливість доступу до певної комп'ютерної інформації, комп'ютерної програми, комп'ютерної мережі, операційної системи та здійснення непомітно для власника чи законного користувача несанкціонованої передачі інформації сторонній особі. Після цього А. надав вільний доступ до свого комп'ютера всім абонентам локальної мережі.

Розповсюдження шкідливих технічних засобів – є їх установлення в оплатній або безоплатній формі в ЕОМ, АС або комп'ютерних мереж чи мереж електрозв'язку, які продаються або передаються на іншій основі, наприклад, здаються в оренду.

У разі вчинення такого злочину в формі розповсюдження його слід вважати закінченим з моменту надання доступу до такого засобу іншим особам, або ж дій, після яких починається його автоматичне відтворення і поширення.

Збут шкідливих програмних чи технічних засобів – оплатне або безоплатне (продаж, дарування, обмін, сплата боргу, позика тощо) відчуження фізичного носія зі шкідливим програмним засобом іншій особі. Типовим прикладом збуту шкідливих програм є продаж дисків із записаними на них шкідливими програмами.

Збут шкідливих програмних або технічних засобів відрізняється від розповсюдження тим, що він пов'язаний з відчуженням предмета. Так, якщо при розповсюдженні предмет залишається в особи (шкідливе програмне забезпечення продовжує знаходитися на мережевому ресурсі, з якого розповсюджується, повертається шкідливий технічний засіб, що передавався для використання), то в результаті збуту він відчужується, тобто не залишається в особи, яка його збуває.

Розповсюдження та збут шкідливих програмних чи технічних засобів можуть вчинятися як особою, що створила шкідливі засоби, так і іншою, яка не брала участі в їх утворенні. Як розповсюдження, так і збут є закінченими складами злочину з моменту передачі шкідливих програмних або технічних засобів, незалежно від того, чи зміг отримувач ними розпорядитися чи ні.

У разі збуту таких засобів злочин є закінченим з моменту передачі іншій особі хоча б однієї програми, яка є шкідливим програмним засобом, чи шкідливого технічного засобу.

Диспозицією частини першої ст. 361-1 КК України передбачено кримінальну відповідальність за *створення шкідливих програмних чи технічних засобів* з метою їх використання, але не криміналізовано використання, як таке, що є нелогічним, оскільки безпосереднє

використання, вочевидь, має більшу суспільну небезпечність, ніж створення з метою використання, тому що при використанні шкідливої програми настає шкідливий наслідок або створюється небезпека його настання.

ОСОБА_1 у березні 2012 року незаконно збув шкідливий програмний засіб «KGB Keylogger 4.2», призначений для несанкціонованого втручання в роботу електронно-обчислювальних машин, оскільки в лютому 2012 року ОСОБА_1, маючи знання в сфері користування мережею Інтернет, перебуваючи в невстановленому в ході досудового розслідування місці, з метою подальшого незаконного збуту, скачав на власний флеш-накопичувач з невстановленого в ході досудового розслідування Інтернет-сайту шкідливий програмний засіб «KGB Keylogger 4.2», основним функціональним призначенням якого є несанкціоноване та приховане копіювання інформації, яка обробляється на комп'ютері, з послідуючим її відправленням на конкретну електронну скриньку. 16 березня 2012 року ОСОБА_1, реалізовуючи свій злочинний умисел, перебуваючи у м. Умань на вулиці Радянській, приблизно о 16 годині, незаконно збула шкідливий програмний засіб «KGB Keylogger 4.2» ОСОБА_3. При цьому, ОСОБА_1 особисто скопіювала зазначений програмний засіб із вказаного флеш-накопичувача на оптичний диск CD-R фірми «PATRON», серійний номер C0102R_MB1_80UG, продемонструвавши при цьому ОСОБА_3 на комп'ютері типу «ноутбук» hp Pavillion dv6 принцип роботи шкідливого програмного засобу «KGB Keylogger 4.2».

Разом з тим, під **використанням шкідливих програмних засобів** слід розуміти реалізацію будь-яких шкідливих функцій (наприклад, активування та початок функціонування вірусу відповідно до своїх властивостей) щодо здатності даного пристрою впливати на встановлений процес обробки інформації в ЕОМ, АС, комп'ютерних мережах чи мережах електрозв'язку.

Під **використанням шкідливого технічного засобу** слід розуміти реалізацію будь-яких шкідливих функцій щодо здатності даного пристрою впливати на встановлений процес обробки інформації в ЕОМ, АС, комп'ютерних мережах чи мережах електрозв'язку.

Використання шкідливого технічного засобу слід вважати закінченим з моменту надання доступу такого засобу до ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку іншим особам, або ж дій, після яких починається його автоматичне відтворення і поширення.

Так, гр-н Д., використовуючи технічний пристрій, що емулює (імітує) роботу єдиної таксофонної карти ВАТ «Укртелеком», здійснив 579 незаконних безоплатних телефонних дзвінків, чим спричинив ВАТ «Укртелеком» збитки на суму 12 525 грн. Злочин було кваліфіковано судом за ч. 1 ст. 361 КК України. А гр-н Л. за допомогою шкідливих програмних засобів вчинив втручання в роботу комп'ютерної мережі Інтернет-провайдера ТОВ «Вокар-Телеком», що призвело до блокування інформації і порушення встановленого порядку її маршрутизації. У результаті даного втручання гр-н Л. підробив «агр» таблицю на шлюзі

сервера компанії ТОВ «Вокар-Телеком», у зв'язку з чим у нього з'явилася можливість сканувати і контролювати інформацію в локальній та Інтернет-мережі, керувати вилученими комп'ютерами, контролювати комп'ютери інших користувачів, здійснювати збір IP і MAC адрес комп'ютерів інших користувачів, що було кваліфіковано за сукупністю ст.ст. 361, 361-1 КК України.

Злочин вважається вчиненим у разі здійснення хоча б одного діяння, вказаного у ст. 361-1 КК України. Причому настання шкідливих наслідків не впливає на кваліфікацію, але повинно братися до уваги під час призначення покарання.

1.2 Суб'єкт та суб'єктивна сторона

Суб'єкт цього злочину загальний, ним є фізична, осудна особа, що досягла 16-річного віку.

Злочини вказаної категорії вчиняються представниками найширших верств суспільства, причому вік правопорушників становить від 10 до 60 років, а їх рівень підготовки – від новачка до професіонала. Особи, які вчиняють комп'ютерні злочини, можуть бути об'єднані в три великі групи:

• особи, які не мають права доступу до певної інформації, що обробляється, не пов'язані трудовими відносинами з організацією чи фізичною особою – жертвою, але, можливо, мають деякі зв'язки з нею;

• співробітники організації, які мають право доступу до інформації, що обробляється у зв'язку із займаною посадою або спеціальними повноваженнями;

• співробітники організації (не посадові особи), які є користувачами та відносяться до персоналу, перебувають у трудових відносинах з власником технічних засобів (уповноваженою ним особою чи розпорядником) і визначені для здійснення функцій управління та обслуговування ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

У силу своїх професійних і посадових обов'язків окремі співробітники (працівники) організацій, установ та підприємств можуть відіграти певну роль у вчиненні комп'ютерних злочинів:

- оператори ЕОМ, периферійних пристроїв введення інформації в ЕОМ і обслуговуючі лінії телекомунікації;

- особи, в чиєму віданні перебувають бібліотеки програм; системні програмісти;

- системні інженери, інженери з термінальних пристроїв, інженери-зв'язківці, інженери-електронщики;

- управлінці комп'ютерною мережею, керівництво операторів; управлінці баз даних; керівники роботою з програмного забезпечення;

- працівники служби безпеки, працівники, які контролюють функціонування ЕОМ або мережі ЕОМ, тощо.

Суб'єктивна сторона. Вина по відношенню до створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів може спостерігатися виключно у формі умислу. На це вказує безпосереднє посилання на мету такого створення, бо за наявності чітко встановленої мети діяння може вчинятися тільки у формі прямого умислу, який виражається у тому, що особа не лише усвідомлювала шкідливість написаної нею програми або виготовленого технічного пристрою, не тільки розуміла їх здатність впливати на встановлений порядок роботи електронно-обчислювальних машин, автоматизованих систем чи комп'ютерних мереж та порушувати його, а й свідомо бажала набуття програмними або технічними засобами ознак шкідливості, створювала їх саме такими. Перелічені ознаки у своїй сукупності вказують на наявність у діях особи виключно прямого умислу (причому завжди визначеного, оскільки особа, прописуючи шкідливі функції програми для ЕОМ, тим самим конкретизує і настання індивідуально визначеного результату). З огляду на це, такий умисел може бути лише заздалегідь обдуманим.

Стосовно збуту шкідливих програмних чи технічних засобів можна зробити аналогічний висновок. При збуті шкідливих програм для ЕОМ або шкідливих технічних засобів особа повинна усвідомлювати їх здатність негативно впливати на встановлений процес обробки інформації в ЕОМ, АС чи комп'ютерних мережах, оскільки здійснювати збут шкідливих програмних та технічних засобів може як особа, що їх створила, так і інші особи. *Так, у 2007 році в м. Одесі було розглянуто кримінальну справу проти чоловіка, який на електронному ринку поряд з іншими компакт-дисками продавав набір шкідливих програм для ЕОМ під назвою «Все для хакера».* Цілком очевидно, що навіть не розуміючись на мовах програмування, виходячи з назви диску, не можна не усвідомлювати шкідливий зміст записаних на ньому програм. Отже, збут шкідливих програмних і технічних засобів характеризується лише прямим умислом.

Щодо його диференціації, то можна констатувати, що збут шкідливих програмних чи технічних засобів особою, яка їх створила, може характеризуватися тільки визначеним, заздалегідь обдуманим умислом. Якщо ж особа вчиняє лише збут, без попереднього створення програми чи пристрою, то в її діях може спостерігатися як визначений умисел, так і невизначений (коли особа усвідомлює шкідливість програми чи пристрою лише в загальних рисах), але у кожному з цих випадків умисел буде заздалегідь обдуманим.

По відношенню до розповсюдження шкідливих програмних чи технічних засобів форма вини не є настільки однозначною, хоча існують точки зору щодо безумовної наявності лише прямого умислу. В разі, якщо особа, яка здійснювала розповсюдження шкідливих програм для ЕОМ, отримала за це матеріальну винагороду в будь-якій формі (наприклад, продаж шкідливих програмних засобів на спеціалізованих сайтах), у її діях також чітко прослідковується наявність прямого умислу. Дуже часто і

безоплатні дії можуть вчинятися умисно, наприклад, з бажанням помститися, пожартувати, або через хуліганські мотиви. Тобто, у більшості випадків розповсюдження шкідливих програмних засобів вчиняється з прямим умислом, також це завжди стосується розповсюдження шкідливих технічних засобів.

Дослідимо й інші випадки. Наприклад, коли особа не знає про наявність шкідливої програми в ЕОМ, АС, мережі або фізичних носіях інформації. Очевидно, що в таких випадках мова не може йти про вчинення протиправного посягання. Але часто трапляються ситуації, коли електронною поштою надходять листи, які за своїм змістом відрізняються від того, що зазначено в назві. Таким чином нерідко поширюються саме шкідливі програми, причому в самому листі можуть надаватися коментарі, кому та навіщо слід далі переслати даний лист (наприклад, «для рекламного відділу» або «надійшли анекдоти всім друзям»). І якщо недосвідченому користувачу розширення файлу може ні про що не сказати, то для особи, яка знається на комп'ютерах, має спеціальну освіту або працює на відповідній посаді, існує велика різниця між розширенням текстового файлу та виконуваної програми, яка цілком може виявитися шкідливою. Отже, коли в листі значиться, що додаток до листа представляє собою графічний або текстовий файл (тобто будь-який текст, фотографії тощо), а розширення файлу цьому не відповідає, то для особи, яка хоч незначною мірою знається на комп'ютерах, це може слугувати сигналом для того, що даний файл нікому пересилати не можна.

Так, питання про форму вини щодо розповсюдження шкідливих програмних засобів для ЕОМ необхідно вирішувати в кожному конкретному випадку, залежно від місця роботи особи та наявності в неї спеціальних знань. Якщо такі знання відсутні, то очевидно, що в діях особи відсутній і склад злочину, оскільки вини в діях не спостерігається. Якщо ж ми маємо справу з особою, в якої є спеціальна освіта, або вона взагалі працює у сфері, що будь-яким чином пов'язана з інформаційними системами, та особа при цьому проігнорувала очевидні дані щодо змісту листа й доданого до нього файлу та дійсно розіслала такі «анекдоти всім друзям», то в діях особи вже спостерігається вина у формі необережності. Якщо ж таку необережність класифікувати, то вбачається її відношення до злочинної самовпевненості, коли особа внаслідок наявності в неї спеціальних знань могла передбачити настання суспільно шкідливих наслідків, але легковажно сподівалась на їх відвернення. Таким чином, у даному випадку прослідковується наявність технічної або професійної необережності.

На підставі викладеного можна зробити висновок, що розповсюдження шкідливих технічних засобів завжди вчиняється у формі прямого умислу, при цьому розповсюдження шкідливих програмних засобів може вчинятися як у формі прямого умислу, так інколи й у вигляді необережності (а саме, злочинної самовпевненості).

Слід зауважити, що для кваліфікації діяння за ст. 361-1 КК України не завжди має значення здатність програми чи технічного засобу заподіювати реальну шкоду. Адже у разі, коли особа впевнена, що створила шкідливу програму або засіб, а насправді помилилася, її дії слід кваліфікувати як закінчений замах на вчинення цього злочину – ч. 2 ст. 15 ст. 361-1 КК України), а якщо особа вчинила поряд з цим інші протиправні дії – залежно від характеру і змісту вчиненого – додатково за відповідною статтею КК України.

1.3 Кваліфікуючі ознаки

Кваліфікуючими ознаками даного злочину є вчинення його:
- повторно;
- за попередньою змовою групою осіб;
- заподіяння значної шкоди.

Повторність. Повторністю злочинів визнається вчинення двох або більше злочинів, передбачених тією самою статтею або частиною статті Особливої частини КК України. Отже, повторність щодо створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут матимуть місце лише у разі вчинення двох чи більше злочинів, передбачених ст. 361-1 КК України, оскільки самою нормою не передбачено інше.

При цьому для встановлення повторності необхідно відокремити одиничні продовжувані злочини від повторних простих (непродовжуваних) злочинів. Повторність відсутня при вчиненні продовжуваного злочину, який складається з двох або більше тотожних діянь, об'єднаних єдиним злочинним наміром (ст. 32 КК України), з тієї причини, що така ситуація є досить типовою для діяння, передбаченого ст. 361-1 КК України. Так, одиничне діяння по умисному розповсюдженню шкідливих комп'ютерних програм може спричинити наслідки у вигляді поступового перекручення, руйнування комп'ютерної інформації на всіх електронно-обчислювальних машинах, які були вражені шкідливою програмою. Наприклад, якщо суб'єкт направляє вірус кільком особам у прикріпленні до листа електронної пошти, крім того, що при розкритті такого прикріплення можуть бути уражені всі комп'ютерні системи, на яких прикріплення було розкрите, в разі несвоєчасного виявлення наявності шкідливої програми, така програма буде поступово змінювати або знищувати інформацію в цій електронно-обчислювальній машині або мережі, до якої ця електронно-обчислювальна машина приєднана.

За попередньою змовою групою осіб. Згідно з частиною другою ст. 28 КК України злочин визнається вчиненим за попередньою змовою групою осіб, якщо його спільно вчинили декілька осіб (дві або більше), які заздалегідь, тобто до початку злочину, домовилися про спільне його вчинення. Разом з тим, вказані злочини можуть вчинятись групою осіб

спонтанно, без попереднього їх узгодження. Також може мати місце цілеспрямоване колективне розсилання шкідливих програм для ЕОМ, наприклад, на адресу певної компанії для виведення з ладу її інформаційної мережі. В такому разі мова може йти лише про заздалегідь обумовлену співпрацю для досягнення спільного злочинного результату. Проте, якщо до початку цієї акції або інших незаконних дій в інформаційному середовищі мала місце попередня домовленість (особиста чи шляхом електронного листування) про спільне вчинення такої атаки задля підвищення її ефективності, то діяння набуває ознак вчиненого за попередньою змовою групою осіб.

Заподіяння значної шкоди. У примітці до ст. 361 КК України встановлюється, що значною шкодою у статтях 361-363[1], яка полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян, а, отже – розуміється виключно у матеріальному виразі.

Згідно з положеннями підпункту 169.1.1 пункту 169.1 статті 169 розділу IV Податкового кодексу України, неоподаткований мінімум доходів громадян, на який є посилання в примітці до ст. 361 КК України щодо визначення значної шкоди, встановлюється на рівні податкової соціальної пільги, яка з 01 січня 2016 року буде рівною 100 відсоткам розміру прожиткового мінімуму для працездатної особи, встановленої законом на 01 січня звітного податкового року.

Статтею сьомою проекту Закону України «Про державний бюджет України на 2016 рік», схваленого Кабінетом Міністрів України постановою від 14 вересня 2015 року № 677 «Про схвалення проекту Закону України «Про Державний бюджет України на 2016 рік», з 01 січня 2016 року прожитковий мінімум працездатних осіб встановлено в розмірі 1 378 гривень. З урахуванням Прикінцевих положень Податкового кодексу України податкова соціальна пільга в частині кваліфікації злочинів може становити у 2016 році 1 378 гривень. Відповідно до цього значна шкода, яка в сто і більше разів перевищує неоподаткований мінімум доходів громадян, становитиме 137 800 гривень.

Для вирішення цієї проблеми виділяють три способи оцінки інформації: 1) затратний підхід – підраховуються витрати, які поніс створювач інформації на етапі її збирання, обробки, розробки, підготовки та введення; додаткові витрати на доопрацювання до необхідного стану, на реєстрацію та ін.; 2) за аналогією – виявляється ціна, за якою аналогічні об'єкти продаються на відкритому, легальному (не «чорному») ринку; 3) через оцінку майбутніх доходів, пов'язаних з експлуатацією цього інформаційного ресурсу.

Також необхідно звернути увагу, що відповідно до п. 6, ч. 2 ст. 242 КПК України слідчий **зобов'язаний звернутися** до експерта для проведення експертизи з визначення розміру матеріальних збитків, шкоди немайнового характеру заподіяної кримінальним правопорушенням. Відповідь на

поставлені експерту запитання можна отримати шляхом проведення комплексної експертизи із застосуванням спеціальних знань у галузі інформатизації, засобів обчислювальної техніки та зв'язку, економіки, фінансової діяльності. Таку експертизу проводить **Науково-дослідний центр судової експертизи з питань інтелектуальної власності,** поштова адреса: 01133, м. Київ, бульвар Лесі Українки, 26. Телефон: (044) 272-44-15, адреса сайту: http://www.intelect.org.ua.

РОЗДІЛ 2
Особливості здійснення окремих слідчих (розшукових) дій під час досудового розслідування злочинів, що вчиняються з використанням шкідливих програмних чи технічних засобів

2.1 Алгоритм розслідування

Аналіз вітчизняного та зарубіжного досвіду свідчить, що можна виділити три типові слідчі ситуації, пов'язані із вчиненням злочинів з використанням шкідливих програмних чи технічних засобів:

- власник інформаційної системи (комп'ютера) власними силами виявив порушення цілісності/конфіденційності інформації в системі, виявив винну особу і заявив про це в правоохоронні органи;
- власник інформаційної системи (комп'ютера) власними силами виявив порушення цілісності/конфіденційності інформації в системі, не зміг виявити винну особу і заявив про це в правоохоронні органи;
- дані про порушення цілісності/конфіденційності інформації в інформаційній системі та винну особу стали загальновідомими або безпосередньо виявлені працівниками правоохоронних органів (наприклад, у ході проведення оперативно-розшукових заходів чи здійснення кримінального провадження по іншій справі).

При розслідуванні злочину, пов'язаного із створенням, збутом чи розповсюдженням шкідливих програмних або технічних засобів для ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку представляється найдоцільнішою наступна послідовність встановлення основних завдань:

1. Факту злочину – створення, збут, розповсюдження шкідливих програмних чи технічних засобів для ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку.
2. Місця вчинення злочину.
3. Часу вчинення злочину.
4. Надійності засобів захисту комп'ютерної інформації.
5. Способу вчинення злочину.
6. Осіб, які вчинили злочин.
7. Винності й мотивів правопорушників.

8. Обставин, що впливають на ступінь тяжкості злочину, а також обставин, що характеризують особу підозрюваного, пом'якшують та обтяжують покарання.

9. Характеру та розміру шкоди, завданої злочином.

10. Виявлення обставин, що сприяли злочину.

Загальний порядок проведення слідчих (розшукових) дій за фактом розповсюдження шкідливих програмних чи технічних засобів може складатись з наступного алгоритму:

1. Отримання та внесення до Єдиного реєстру досудових розслідувань (ст. 214 КПК України) заяв від фізичних осіб та повідомлення від юридичних осіб про вчинення кримінального правопорушення, пов'язаного з виявленням шкідливих програмних і технічних засобів, які незаконно втручаються в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку. Початок досудового розслідування та направлення письмового повідомлення про це прокурору (ст. 214 КПК України).

2. Розгорнутий допит заявника про відомі йому ознаки протиправного діяння.

3. Витребують та вивчають матеріали потерпілої сторони, що свідчать про вчинення протиправного впливу на її програмно-технічні засоби.

4. Створення слідчо-оперативної групи (далі - СОГ) для проведення обшуку *(вважається, що саме цією дією необхідно проводити огляд місця вчинення злочину) у* потерпілої особи, із визначенням включення в її склад залежно від обставин відповідних спеціалістів і працівників підрозділу протидії кіберзлочинності. Отримання відповідного рішення слідчого судді, суду на здійснення обшуку за місцем вчинення злочину, в якому безпосередньо зазначаються електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку (ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку тощо), які можуть бути тимчасово вилучені для вивчення фізичних властивостей, що мають значення для кримінального провадження. Виїзд СОГ на місце вчинення злочину та проведення там обшуку.

Під час обшуку здійснюється:

а) огляд комп'ютерного обладнання, інших електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку на яких був виявлений шкідливих програмний чи технічний засіб. Огляду підлягає також навколишня обстановка;

б) вилучаються для вивчення фізичних властивостей, що мають значення для кримінального провадження, зазначені в ухвалі суду електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку, якщо їх вилучення неможливе за певних причин – з них знімаються необхідні копії інформації.

Якщо виникла потреба здійснити тимчасове вилучення інших електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, що не зазначені в ухвалі слідчого судді, то такі дії здійснюються лише в порядку, передбаченому главою 16 КПК України,

тобто береться нова ухвала слідчого судді, в якій зазначаються електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку, що потребують додаткового вилучення;

в) у *потерпілої сторони* витребовуються та вивчаються (якщо такі є в наявності) наступні матеріали:

− журнал нештатних ситуацій обчислювального центру збоїв у роботі комп'ютерної мережі, виходу з ладу окремого комп'ютера або технічного пристрою. Журнал може вестися як на самому підприємстві, так і в сервісному центрі, який надає технічне обслуговування;

− журнал передачі змін операторами ЕОМ;

− документи про проведені протягом доби операції (банківські розрахунки, результати антивірусних перевірок тощо);

− копія файлу адміністратора мережі, в якому фіксується робота мережі (моменти вмикання і вимикання, результати тестування, протоколи позаштатних ситуацій);

− копія файлів зафіксованих спроб протиправного використання комп'ютера або підключення до мережі;

− акти про результати проведення аудиту системних журналів (LOG-файлів), сервера аутентифікації, авторизації та обліку, HTTP- та FTP-серверів;

− роздруківки та електронні копії з системних журналів (LOG-файлів доступу та помилок) сервера аутентифікації, авторизації та обліку, HTTP- та FTP-серверів й інша документальна інформація, яка підтверджує факт втручання в автоматизовану систему організації;

− копія договору на надання послуг зв'язку між оператором зв'язку, на мережі якого проводився моніторинг, і правопорушником;

− копія договору на надання послуг доступу до мережі Інтернет з провайдером;

− копія договору на реєстрацію доменного імені;

− копії довідок, що підтверджують сплату за користування мобільним сервісом, сервісом доступу до мережі Інтернет;

– копія договору щодо надання зазначеної послуги, система сплати, можливі контактні дані особи, якою укладалась угода (у випадку орендування серверу «Колокейшен[2]»).

При цьому слідчий за порадою спеціаліста вирішує, які саме копії чи оригінали документів необхідно вилучати, а які ні.

5. Допит осіб, які можуть бути свідками або очевидцями.

6. У рамках кримінального провадження здійснюються слідчі (розшукові) та негласні слідчі (розшукові) дії, направлені на встановлення місця створення, розповсюдження чи збуту шкідливих програмних або технічних засобів, а також осіб, які причетні до вчинення злочинних діянь.

[2] Послуга мережі Інтернет (різновид хостингу), що передбачає фізичне розміщення клієнтського сервера на технічному майданчику провайдера, або надання провайдером в оренду користувачеві власного сервера.

Напрямками здійснення таких дій можуть бути:

а) направлення на експертизу вилучених під час обшуку предметів, пристроїв, програмних продуктів, речовин і слідів;

б) встановлення IP-адреси, комп'ютерної техніки та засобів комунікації, з яких здійснювалося розповсюдження шкідливих програмних засобів;

в) направлення запитів до Інтернет-провайдерів стосовно надання інформації про користувачів Інтернет-сайтів і власників поштових скриньок щодо яких здійснювалося розповсюдження шкідливих програмних засобів:

– про реєстрацію доменного імені та хостінгу для розміщення сайту, з якого здійснювалось розповсюдження шкідливих програмних засобів;

– про реєстрацію IP-адреси чи поштової скриньки користувача Інтернет-мережі (підозрюваного);

– про адміністрування Інтернет-форуму або чату, через який здійснювалося розповсюдження шкідливих програмних засобів;

г) направлення запитів до банківських установ щодо надання інформації про рахунки, що належать юридичним та фізичним особам, які їх використовували для отримання коштів за збут шкідливих програмних засобів, а також про рух коштів по таких рахунках;

д) проведення обшуку або здійснення тимчасового доступу до речей і документів за місцем:

– встановлення комп'ютерної техніки та засобів комунікації, з яких здійснювалося розповсюдження шкідливих програмних засобів;

– створення чи зберігання (знаходження) шкідливих комп'ютерних чи технічних засобів;

– проживання осіб, які можуть бути причетні до обігу шкідливих комп'ютерних чи технічних засобів;

– ймовірного перебування підозрюваного під час виходу в мережу Інтернет;

е) у порядку, передбаченому главою 15 КПК України, здійснюється тимчасовий доступ до:

− матеріалів (інформації) провайдера та оператора зв'язку, які обслуговують програмно-технічні засоби, що зазнали протиправного впливу;

− комп'ютерного обладнання та засобів комунікації, на яких створювалися та оброблялися шкідливі програмні й технічні засоби;

− комп'ютерного обладнання та засобів комунікації, через які здійснювалось Інтернет-спілкування підозрюваного;

− камер спостереження, в яких зафіксовано перебування підозрюваного у приміщеннях чи інших місцях, де він виходив у мережу Інтернет чи здійснював фінансові операції (наприклад, місце встановлення банкоматів);

ж) огляд предметів, що мають відношення до кримінального правопорушення;

з) допит:

− свідків, яким відомі обставини вчиненого кримінального правопорушення, а також які знають підозрюваного або мають інформацію

про факти вчинення ним аналогічних чи інших протиправних діянь. Наприклад, якщо електронна поштова адреса створена навмисно для протиправних дій, правопорушник може користуватися нею з комп'ютерних мереж, що належать Інтернет-клубам, кафе, орендованих квартир, готелів тощо, тому необхідно допитати адміністратора закладу, який був на зміні під час виходу правопорушника до мережі Інтернет; осіб з числа інших клієнтів, які в той час знаходилися поблизу комп'ютера правопорушника; інший обслуговуючий персонал клубу (кафе, готелю тощо), який міг запам'ятати правопорушника (охоронець, бармен, прибиральниця тощо);

- спеціалістів провайдера чи оператора зв'язку, які забезпечують доступ програмно-технічних засобів потерпілого до мереж;

- спеціалістів, які безпосередньо обслуговують програмно-технічні засоби потерпілої сторони.

За результатами допиту можливо встановити особу (або скласти фоторобот) правопорушника;

і) затримання та допит підозрюваного;

и) призначення судових експертиз вилученого в результаті слідчих (розшукових) дій комп'ютерного обладнання, програмного забезпечення та засобів комунікації (комп'ютерно-технічна), слідів рук (дактилоскопічна) та інших речових доказів;

к) призначення експертиз щодо інших предметів, вилучених у рамках кримінального провадження;

л) в разі необхідності – проведення слідчим негласних слідчих (розшукових) дій або надання доручення на проведення таких дій уповноваженим оперативним підрозділам Національної поліції і приєднання до кримінального провадження отриманих документів та протоколів з відповідними додатками.

Вину осіб, причетних до розповсюдження забороненого контенту, може бути також доведено:

– результатами дослідження способів передавання контенту (електронною поштою, записами на диски чи флеш-картки пам'яті тощо);

– результатами відстеження обміну інформацією через мережу Інтернет, які здійснював підозрюваний;

– зв'язком підозрюваного з роботою на певному комп'ютері, на якому створювався чи розповсюджувався шкідливий програмний;

– результатами дослідження змісту жорсткого диску з комп'ютера підозрюваного та потерпілого зі слідами журналів роботи в мережі Інтернет (закладки, пошукові запити), тимчасових файлів (кеш, Cookie-файли, буфер друку, місце зберігання інформації, записаної на комп'ютер веб-сайтом), змісту своп-файлу «вільне місце», списків друзів + особистих профілів + записів чат-кімнат + інших збережень «області»; відстеженням дат збереження файлів (у файлі Windows зберігаються дати створення (коли файл було створено), останнього запису (коли файл востаннє було змінено) та останнього доступу до файлу (коли файл востаннє було відкрито);

– іншими документами, що свідчать про протиправну діяльність особи.

При огляді комп'ютерів, допиту свідків чи потерпілих також рекомендується звертати увагу на відвідування користувачем веб-ресурсів мережі Інтернет, а саме:

Яндекс (http://www.yandex.ru/),
ВКонтакте (http://vk.com/),
Одноклассники (http://www.odnoklassniki.ru/),
Фотострана (http://fotostrana.ru/),
Привет.ру (http://privet.ru/),
LiveIntemet (http://www.liveintemet.ru/),
Toodoo (http://toodoo.ru/),
LJ.Rossia.org (http://lj.rossia.org/),
Блоги@Mail.Ru (http://blogs.mail.ru/),
Моя живая страница (http://www.mylivepage.ru/),
MirTesen.ru (http://mirtesen.ru/),
Дневник на TKS.RU (http://blogs.tks.ru/portal.php),
Клерк.ru (http://www.klerk.ru/),
Beon.ru (http://beon.ru/),
БебиБлог (http://www.babyblog.ru/),
Блогус (http://www.blogus.ru/blog.php),
ITBlogs (http://itblogs.ru/),
Рыболовний клуб (http://www.fion.ru/),
RuSpace (http://www.ruspace.ru/),
Re:vision (http://www.revision.ru/),
Diary.Ru (http://www.diary.ru/),
LiveLib (http://www.livelib.ru/),
Карта для любителей рыбалки (http://www.fishingmap.ru/),
Сообщество влюбленных в кино (http://www.ilovecinema.ru/),
100 Друзей (http://www.100druzei.ru/),
Dogster (http://www.dogster.ru/),
Факультет.ру (http://www.facultet.ru/),
Тейст (http://www.mmm-tasty.ru/).
Вебкруг (http://www.webkrug.ru/),
VeniVidi(http://www.mmm-tasty.ru/),
Вебкруг (http://www.webkrug.ru/),
VeniVidi (http://venividi.ru/),
Я талант (http://yatalant.ru/),
Мой мир (http://my.maiJ.ru/),
ЛИМП (http://www.limpa.ru/),
Spaces.ru (http://spaces.ru),
Мой Круг (http://moikxug.ru/),
Соседи-Онлайн (http://sosedi-online.ru/),
За Баранкой (http://zabarankoi.ru/),
Юмами (http://www.u-mama.ru/),

Автокадабру (http://autokadabra.ru/),
Отдохнули.ру (http://www.otdohnuli.ru/),
Telefoner.ru (http://www.telefoner.ru/),
Одноклассники.КМ.РУ (http://vkrugudruzei.ru),
Mail.ru (https://mail.ru/),
Rambler.ru (http://www.rambler.ru/),
Mamba.ru (http://wwAv.mamba.ru/),
а також інших Інтернет-ресурсів російського походження.

Наявність відомостей про відвідування користувачем зазначених сайтів може свідчити про можливе знаходження в операційній системі цього комп'ютера шкідливих програмних засобів, які сприяють витоку інформації.

2.2 Особливості проведення обшуку

Сліди вчинення злочинів, пов'язаних із створенням, використанням та розповсюдженням шкідливих програмних чи технічних засобів, можна розділити на:

- сліди доступу до засобів комп'ютерної техніки;
- сліди доступу до комп'ютерної інформації та впровадження шкідливих програмних чи технічних засобів;
- сліди функціонування і впливу шкідливих програмних чи технічних засобів.

Найбільш специфічними залишаються сліди на машинних носіях у результаті впровадження, функціонування та впливу шкідливих програмних засобів, які можна розділити на кілька підгруп:

1. Сліди зміни файлової структури, системних областей машинних носіїв інформації та постійної незалежної пам'яті.
2. Сліди зміни налаштувань ЕОМ і окремих програм.
3. Сліди порушення роботи ЕОМ і окремих програм.
4. Сліди впливу на системи захисту і конфіденційність інформації.
5. Інші прояви впливу і функціонування шкідливих програмних та технічних засобів, включаючи відеоефекти, повідомлення, що виводяться на пристрій для друку, аудіоефекти.

Враховуючи викладене, особливу увагу необхідно приділити належному огляду та вилученню ЕОМ, АС, комп'ютерних мереж та мереж електрозв'язку, які були предметом посягання.

Обшук доцільно розділити на три етапи: підготовчий (до виїзду на місцевість), робочий (дослідний) та заключний (фіксація результатів).

Підготовчий етап. До обшуку в кримінальних провадженнях у злочинах, пов'язаних з обігом шкідливих програмних чи технічних засобів, слідчий обов'язково повинен зосередити увагу на оптимальному варіанті створення СОГ, рекомендується включити до неї відповідних спеціалістів, а також працівника (-ів) підрозділу боротьби з кіберзлочинністю.

Залежно від конкретної слідчої ситуації до проведення обшуку (тимчасового доступу до речей та документів) можуть залучатися спеціалісти:

- спеціаліст із мережевих технологій (у випадку можливої наявності на місці проведення обшуку периферійного обладнання віддаленого доступу або локальної мережі);

- спеціаліст із системи зв'язку (при використанні для дистанційної передачі даних каналів електрозв'язку);

- інженери електрики, спеціалісти супутникових систем зв'язку, оператори комп'ютерних систем і мереж (стільникових, Інтернет тощо).

При необхідності для участі в обшуку можуть бути запрошені й інші незацікавлені в провадженні спеціалісти, які знають специфіку роботи об'єкта, що оглядається.

Місцем проведення обшуку у вказаних злочинах можуть бути: приміщення підприємств, установ, організацій, житлові будинки, квартири, дачі, кімнати, класи, зали, клуби, іноді нежитлові приміщення (кімнати в цокольних будовах, підвали, напівпідвали, гаражі, сараї, інші приміщення). Залежно від конкретного місця, території, кількості приміщень, засобів охорони, об'єму комп'ютерного оснащення, різновидів і технічних характеристик тощо, слідчий разом із спеціалістом чи працівником підрозділу боротьби з кіберзлочинністю розробляє план з організації та ефективного проведення обшуку.

Робочий етап. Особливої уваги вимагає робочий етап проведення обшуку. Він включає в себе:

- заходи щодо відсторонення осіб від працюючих технічних засобів, за умови проведення обшуку в робочий час;

- персонального встановлення осіб, які працюють з комп'ютерними системами та їх обслуговують, при виявленні сторонніх суб'єктів, установлення мети їх перебування у цьому місті;

- складання планів і схем приміщення та розташування в ньому технічних засобів;

- проведення фотографічної і відеофіксації розташування ЕОМ, АС, комп'ютерних мереж та мереж електрозв'язку;

- детальний опис зображення на моніторах кожного з працюючих комп'ютерів (фіксація конкретної програми на момент проведення слідчої дії) та ін.;

- огляд ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку, що передбачає як огляд безпосередньо фізичного стану вказаних предметів, так і програмних продуктів, які уражені вірусом. Проводиться, як правило, спеціалістом чи працівником підрозділу протидії кіберзлочинності.

Після прибуття на місце проведення обшуку слід відразу ж вжити заходів щодо забезпечення збереження на ЕОМ, АС, комп'ютерних мережах та мережах електрозв'язку наявних на них даних. Для цього необхідно:

1. Встановити місцезнаходження ЕОМ, АС, комп'ютерних мереж та мереж електрозв'язку, які стали об'єктом посягання, їх кількість, а також програмне забезпечення, комп'ютерної інформації та документів, що використовувалися під час підготовки, здійснення і можливого приховування злочину, а також інших криміналістично-значущих даних, які мали відношення до вчинення протиправної дії.

2. Визначити зміст комп'ютерної інформації, яка могла була бути об'єктом посягання.

3. Визначити схематичний план місць проведення огляду, при цьому додатково можуть бути оглянуті інші ЕОМ, АС, комп'ютерні мережі та мережі електрозв'язку на предмет наявності у них (впливу на них) шкідливих програмних та технічних засобів.

4. Встановити власника чи користувача, а також осіб, які мають відповідний допуск до ЕОМ, АС, комп'ютерних мереж, мереж електрозв'язку та носіїв електронних даних, а також осіб, які перебувають на об'єкті, незалежно від їх пояснень мети перебування.

5. З'ясувати режим роботи установи, в якій було вчинено злочин, кількісний та персональний склад працюючих з комп'ютерним програмним забезпеченням, осіб, які обслуговують (програмують, діагностують, здійснюють захист) автоматизованих комп'ютерних систем, мереж та мереж електрозв'язку тощо.

6. Не дозволяти нікому з осіб, які працюють на місці вчинення злочину, або перебувають тут з інших причин (персоналу), торкатися до ЕОМ, АС, комп'ютерних мереж та мереж електрозв'язку з будь-якою метою.

7. Ні в якому разі не вимикати електропостачання об'єкта, хто б не просив за це (крім компетентних фахівців зі складу СОГ).

8. У разі, якщо на момент початку проведення обшуку електропостачання об'єкта вимкнено, то підключення/відключення до/від електромережі ЕОМ чи АС здійснюється за погодженням із спеціалістом чи працівником підрозділу боротьби з кіберзлочинністю.

9. Самому не вчиняти ніяких маніпуляцій із ЕОМ, АС, комп'ютерними мережами та мережами електрозв'язку, якщо результат цих маніпуляцій заздалегідь невідомий.

Одночасно керівник СОГ має вжити заходів щодо охорони та забезпечення цілісності електронної інформації на основних та периферійних запам'ятовуючих пристроях. З цією метою необхідно:

1. За сприяння керівника чи представника організації, підприємства, установи тощо, або ж без їх допомоги, пояснити працюючому з комп'ютерним обладнанням персоналу мету цього заходу, щоб уникнути непорозумінь під час проведення обшуку.

2. Заборонити присутнім на місці проведення обшуку подальше ведення операцій з використанням автоматизованих систем, а також самостійне здійснення відключення ЕОМ (комп'ютерів) від АС, комп'ютерних мереж та мереж електрозв'язку.

3. Вжити заходів щодо тимчасового відсторонення працюючого персоналу від їхніх робочих місць і виконання дій, пов'язаних з використанням ЕОМ (комп'ютерів), АС та комп'ютерних мереж чи мереж електрозв'язку. Бажано позбавити їх можливості користатися також і телефоном, а при гострій необхідності робити це тільки з дозволу слідчого.

4. Визначити, чи з'єднані комп'ютери, що знаходяться в приміщенні, у локальну обчислювальну мережу. За наявності локальної комп'ютерної мережі найбільший інтерес представляє центральний комп'ютер, так званий сервер, на якому зберігається велика частина інформації й до якого мають доступ всі ЕОМ. Цей комп'ютер необхідно обстежувати більш ретельно та обережно.

5. Встановити, чи існують з'єднання комп'ютера з устаткуванням або комп'ютерною технікою поза приміщенням, що оглядається.

6. На випадок, якщо перед початком огляду комп'ютерне обладнання або його частина були в неробочому режимі, не поспішати його вмикати та запускати в дію операційну систему, а з'ясувати причину відключення її від мережі.

7. При наявності у приміщенні, де проводитиметься огляд, сторонніх предметів, електромагнітних, вибухових, токсичних та інших речовин, забезпечити їх негайне видалення з метою запобігання непередбачуваних наслідків.

8. Враховувати наступні фактори: а) можливі спроби з боку персоналу пошкодити ЕОМ з метою знищення інформації та інших даних; б) наявність на ЕОМ спеціальних засобів захисту від несанкціонованого доступу, які, не отримавши у встановлений час спеціальний код, автоматично знищать всю інформацію; в) наявність на ЕОМ інших засобів захисту від несанкціонованого доступу.

9. Дотримуватись заходів безпеки: а) у скрутних випадках не звертатися за консультацією (допомогою) до персоналу, а викликати спеціаліста, який не зацікавлений у результаті справи; б) не підносити ближче, ніж на 1 м до ЕОМ металошукачі та інші джерела магнітного поля, в т.ч. сильні освітлювальні прилади й деяку спеціальну апаратуру.

Враховуючи, що основним об'єктом обшуку є ЕОМ, АС, комп'ютерні мережі чи мережі електрозв'язку та навколишня обстановка, слідчий, приступаючи до їх огляду, повинен з'ясувати наступні питання:

- що відбулося на комп'ютері?
- коли це сталося?
- як це сталося?
- де це сталося?
- хто виявив це?
- хто ще був присутній при цьому?

Огляд необхідно починати з обстеження серверів, комп'ютерів, засобів комунікації, мережевих кабельних з'єднань на предмет відповідності встановленим технічним параметрам, правильному послідовному

сполученню з іншими операційними системами та відсутності слідів несанкціонованого підключення сторонніх улаштувань. Також звертається увага на наявність (відсутність) фізичних ушкоджень комп'ютерної техніки, порушень її пломбування.

У подальшому залежно від кількості ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку та характеру вчинення злочину вирішується питання про вибір першочергового об'єкта огляду. Ним може бути центральний сервер, який уражений вірусом, чи комп'ютер, або місце виявлення шкідливого технічного засобу тощо.

Якщо комп'ютер, в якому містяться шкідливі програмні засоби, працює, він підлягає огляду спеціалістами за місцем перебування. Залежно від ситуації, під час огляду можливе від'єднання однієї комп'ютерної системи від іншої, що сполучені між собою в локальну мережу, на випадок уникнення ризиків самостійного обміну чи знищення інформації поза волею спеціалістів.

Якщо комп'ютер, в якому містяться шкідливі програмні засоби, вимкнений, то його включення можливе лише після дозволу спеціаліста (працівника підрозділу боротьби з кіберзлочинністю), який ґрунтується на поясненнях потерпілої сторони щодо характеристик шкідливого програмного продукту, який вразив ЕОМ.

Під час обшуку доцільно перевірити облікові документи підприємства, де зазначаються дані про осіб, що працюють з ЕОМ та їх програмними забезпеченнями, перелік яких зазначений на сторінці 23 цих рекомендацій.

Під час проведення обшуку центральне місце посідає виявлення слідів злочинної діяльності:

1. Різнотипні зміни у будові комп'ютерного устаткування (наявність шкідливих технічних засобів чи іншого позаштатного обладнання, пристроїв розширення оперативної пам'яті, програми для зчитування оптичних дисків, заміна або відсутність мікросхем чи інших комплектуючих).

2. Наявність шкідливих програмних засобів, що спричиняють копіювання, блокування, модифікацію чи знищення інформації; файлове програмне забезпечення підбору паролів до несанкціонованого доступу до мережі Інтернет тощо.

3. Будь-який вплив вказаних вище засобів на саму електронну інформацію, що знаходиться всередині машинних носіїв (зміни у файловій системі; шкідливі та небезпечні файлові програми).

Окрім зазначеного, під час обшуку необхідно переглянути й інші носії електронної інформації.

Також огляду можуть піддаватись різні ніші у стінах, підлозі, вентиляційних отворах; окремі речі й предмети з подвійним дном (підвіконня, столи, стільці тощо). Виявлені підозрілі предмети, які можуть мати відношення до кримінального провадження, з дотриманням установленого процесуального порядку вилучаються.

Завершальний етап включає складання протоколу та додатків до

нього, виготовляються плани і схеми, до яких додаються матеріали фіксації процесу (відеокасети, флеш-карти, звукозапис, зліпки), зняття копій інформації та вилучення предметів, які мають значення для кримінального провадження.

Залежно від властивостей шкідливого програмного засобу, можливостей його дослідження на місці чи в експертних установах слідчий за погодженням із спеціалістом може:

- зняти копію інформації, що міститься на ЕОМ, АС, інших електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку;

- вилучити ЕОМ, АС, інші електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку, якщо вони безпосередньо зазначені в ухвалі суду на проведення обшуку;

- вилучити у порядку, визначеному главою 16 КПК України, ЕОМ, АС, інші електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку, якщо вони безпосередньо не зазначені в ухвалі суду на проведення обшуку. Тобто, береться нова ухвала слідчого судді, в якій зазначаються електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку, що потребують додаткового вилучення.

При цьому необхідно враховувати вимоги частини першої ст. 159 КПК України в тій частині, що тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення, а також побажання потерпілої сторони, що відсутність ЕОМ, АС не нанесе суттєвої шкоди підприємству, установі чи організації або фізичній особі.

У протоколі необхідно вказати всі дії щодо виявлення слідів і предметів огляду в тій послідовності, в якій він проводився, і в тому вигляді, в якому виявлене спостерігалося:

- загальний вигляд місця вчинення злочину і процес поетапного його огляду та результатів кожної дії слідчого;

- місце розташування об'єкта дослідження відносно інших комп'ютерних устаткувань та приміщення в цілому;

- відобразити, в якому стані перебувало устаткування чи інша комп'ютерна система до початку проведення огляду. Якщо ж технічне устаткування мало робочий режим, то слід у процесуальному документі зафіксувати, яку саме операцію воно здійснювало. Має бути проведена фото-, відеозйомка чи цифровий запис інформації, яка є на екрані монітора, та прилеглих до нього програмних засобів, а паралельно з тим обов'язково здійснена графічна фіксація детального дослідження баченого. У випадку виявлення непрацюючого комп'ютерного забезпечення, не слід самостійно здійснювати будь-які операції до з'ясування обставин провадження по даному устаткуванню;

- виявляються та фіксуються сліди пальців рук на комп'ютерах, охоронних і сигнальних пристроях, на їх клавіатурі, з'єднувальних проводах. Так, сліди можуть бути виявлені при наявності спеціальних засобів розпізнавання користувача персонального комп'ютера. До таких засобів відносяться: а) спеціальні електронні картки, в які записується спеціальна інформація про власників, їх паролі та ведеться облік усіх операцій, виконуваних користувачем; б) електронні ключі доступу до комп'ютера, у запам'ятовуючий пристрій якого заноситься унікальна для кожного користувача інформація; в) пристрій ідентифікації користувачів за відбитками пальців, за геометричними ознаками руки; за почерком чи за голосом;

- зазначаються показники спеціальних тестових програмно-апаратних засобів (антивірусів);

- фіксуються сліди впливу шкідливих програмних засобів, стан яких відображений на моніторі на момент огляду. Для цього необхідно детально вивчити та описати існуюче на екрані монітора комп'ютера зображення, всі функціонуючі при цьому периферійні пристрої і результат їхньої діяльності. Багато сервісних програмних засобів дозволяють визначити і переглянути найменування усіх програм, які раніше викликалися, та останню виконану;

- опис комп'ютера слід почати із системного блока, перш за все, зазначається назва предмету дослідження, марка, модель, серія, заводський та інвентарний номер, його зовнішній вигляд (корпус), а саме розмір, тип корпусу, з якого матеріалу виготовлений, колір, характерні індивідуальні ознаки (наявність дисководу для гнучких дисків, дисководу для компакт-дисків, їх місце розташування і т. ін.), наявність пошкоджень, надписів, гарантійних наліпок і пломбування чи інших позначень. Якщо на його корпусі чи інших деталях виявлено сліди (дактилоскопічні, одорологічні, трасологічні тощо), здійснювати опис за встановленою для такого виду слідів формою;

- після цього слід описати комплектацію системного блока, в переважній більшості він складається з материнської плати, процесора, оперативної пам'яті, блоку живлення, жорсткого об'ємного диска, відеокарти, CD-ROM, флопі диска, картрідера. При описі цих складових необхідно зазначити тип, вид, модель, марку або назву, серію, заводський або реєстраційний (інвентарний) номер виробу, виробника, пошкодження, ідентифікаційний номер, наявність гарантійних наліпок і пломб. Крім цього, оглядаються периферійні пристрої (принтер, модем, клавіатура, монітор і т. ін.), при огляді яких у протоколі зазначається призначення кожного пристрою, назва, кількість, розмір, колір, виробник, серійний номер, комплектація;

- порядок з'єднання між собою всіх пристроїв із зазначенням особливостей. Відсутність або наявність комп'ютерної мережі, використання каналу (каналів) зв'язку і телекомунікацій. В останньому випадку

встановлюється тип зв'язку, апаратура, абонентський номер, позивний або робоча частота;

- якщо виявлено шкідливі (несанкціоновані) технічні засоби чи пристрої – вказати, де вони виявлені, як та до чого вони підключені, їх форму, розмір, матеріал виготовлення, колір, зовнішні ознаки, пошкодження, виробника, модель, марку, серію, ідентифікаційний номер, об'єм, наявність гарантійних наліпок і пломб, а також докладно описати сліди й об'єкти, на яких знаходяться ці сліди, у статиці щодо місць їх виявлення; умови та порядок їх вилучення й упакування;

- при наявності відбираються залишки з'єднувальних проводів та ізоляційних матеріалів, фіксуються сліди вдавлювання, проплавлення, надрізу ізоляції з'єднувальних проводів тощо;

- вилучаються та упаковуються предмети, які будуть доказами у кримінальному провадженні в установленому порядку.

Описуються всі маніпуляції із засобами комп'ютерної техніки (включаючи натискання на клавіші клавіатури), зроблені в процесі проведення слідчої дії, та їх результат (наприклад, при копіюванні програм і файлів, визначенні їх атрибутів, дати, часу створення і запису, а також при включенні та вимиканні апаратури, від'єднанні її частин). Також описується процес роз'єднання (з дотриманням усіх необхідних запобіжних заходів) апаратних частин (пристроїв) з одночасним пломбуванням їх технічних входів і виходів.

Проведення обшуку має супроводжуватися фотографуванням. Перш за все, в протоколі обшуку обов'язково треба зазначити характер упаковки комп'ютера та його комплектуючих, чи опечатаний він шляхом наклеювання на місця з'єднань аркушу паперу із закріпленням їхніх країв на бокових стінках комп'ютера клеєм або клейкою стрічкою, чи опечатана безпосередньо коробка, контейнер, де міститься вилучений предмет. Крім цього, зазначається дата, якою печаткою опечатано, підписи слідчого та понятих.

За результатами обшуку, якщо немає можливості зняти копію інформації, потребують вилучення для подальшого направлення на дослідження:

– комп'ютерне обладнання та засоби комунікації (системні блоки комп'ютерів, ноутбуки, айпади, сервери тощо), на яких були виявлені або можуть знаходитись шкідливі програмні засоби;

– модеми та інші пристрої провідного та безпровідного Інтернет-зв'язку;

– програмне забезпечення, яке встановлене на комп'ютері, на якому було виявлено шкідливі програмні чи технічні засоби;

– файл адміністратора мережі, в якому фіксується вся робота мережі (моменти включення і вимикання, результати тестування, протоколи збійних ситуацій);

– сліди пальців рук на комп'ютерах, охоронних і сигнальних пристроях, на їх клавіатурі, з'єднувальних проводах.

- носії інформації, які могли вставлятися чи зчитуватись на комп'ютері (флеш-картки, HDD, дискети, DVD, CD, касети стрічкових стримерів тощо);

- антивірусні програми, які встановлені на комп'ютері;

- технічні засоби розпізнання користувачів (магнітні карти, ключі блокування та ін.) з метою запобігання доступу користувачів до комп'ютерів у період проведення перевірки;

- роздруківки проведених на даному комп'ютері операцій при їх наявності в даному обчислювальному центрі;

- аркуші з нотатками правопорушника (імена, паролі, адреси тощо), які можуть бути прикріплені до монітору, на столі, під клавіатурою, у смітті тощо;

- ділові щоденники із записами;

- службова документація:

а) журнал аварійних ситуацій обчислювального центру, збоїв у роботі комп'ютерної мережі, виходу окремих комп'ютерів або технічних пристроїв з ладу (він може вестися як у конкретному підприємстві, організації, установі, фірмі, компанії, де могло бути вчинено злочин, так і в обслуговуючому даний підрозділ сервісному центрі (обчислювальному центрі);

б) журнал обліку робочого часу операторів ЕОМ;

в) журнал передачі змін операторами доступу до ЕОМ чи його користувачів;

г) копії проведених протягом дня операцій, наприклад, банківських, результати антивірусних перевірок і перевірок контрольних сум файлів;

д) список осіб, які мають право доступу до тієї чи іншої комп'ютерної інформації, список паролів, під якими вони ідентифіковані в комп'ютері;

е) ліцензійні угоди та договори на користування програмними продуктами;

ж) проектна документацію і відповідні інструкції з експлуатації даної системи;

з) накази та інші документи, які регламентують роботу установи.

Усі речі та документи, які підлягають тимчасовому вилученню, слідчий повинен пред'явити понятим та іншим присутнім особам і перелічити їх у протоколі обшуку чи в доданому до нього опису із зазначенням їхніх назв, кількості, міри, ваги, матеріалу, з кого вони виготовлені, та індивідуальних ознак.

Після тимчасового вилучення майна слідчий зобов'язаний забезпечити схоронність такого майна.

2.3 Підготовка запитів щодо надання інформації про користувачів Інтернет-сайтів і власників поштових скриньок

Якщо розповсюдження шкідливим програмним засобом сталося через мережу Інтернет, вживаються заходи щодо встановлення IP-адреси користувача, причетного до розповсюдження в мережі Інтернет вірусу, а у подальшому слідчий вживає заходів щодо ідентифікації особи користувача й встановлення місцезнаходження відповідного комп'ютерного обладнання та засобів комунікації.

У даному випадку встановлення місцезнаходження комп'ютерної техніки відбувається за допомогою технічних особливостей функціонування Інтернет-мережі. Отже, задача встановлення особи правопорушника напряму пов'язана із встановленням IP-адреси, під якою його комп'ютер виходив у мережу Інтернет. Встановлення IP-адреси може здійснити як безпосередньо слідчий, так, за його дорученням, і оперативний працівник підрозділу по боротьбі з кіберзлочинністю.

Кожен комп'ютер у мережі Інтернет має свою унікальну адресу, яка складається з чотирьох чисел, що знаходяться в діапазоні від 0 до 255, розділених крапками. Приклад такої адреси: 192.254.55.232. Такі адреси називаються *IP-адресами* (адресами Інтернет Протоколу).

Ця система адресації базується на мережевій програмі IP версії 4 (IP v4), що використовує 32-бітову адресацію. Слід зауважити, що сьогодні проходить експлуатаційні випробування нова версія програми Internet Protocol Next Generation (IP v6), яка використовує 128-бітну адресацію.

IP-адреса складається з *двох частин*.

Перша частина має від одного до трьох чисел, розташованих ліворуч – вона позначає мережу, в якій знаходиться комп'ютер, і називається ідентифікатором мережі. Інтернет складається з безлічі мереж, кожна з яких має власну адресу.

Друга частина має від трьох до одного чисел, розташованих праворуч – вона позначає конкретний комп'ютер у мережі й має назву ідентифікатор вузла.

Таким чином, ієрархія IP-адрес читається зліва направо, тобто ліворуч розташовуються старші біти, праворуч – молодші (як-то поштова адреса: країна, місто, вулиця, будинок).

Коли особа підключається до мережі Інтернет, її комп'ютер стає частиною мережі, тому йому має бути привласнена унікальна IP-адреса. Отримання IP-адреси здійснюється при кожному підключенні, але ця адреса щораз має нове значення з діапазону динамічних IP-адрес провайдера, через якого здійснюється підключення.

Статичні IP-адреси, як правило, закріплені за тими вузлами Інтернет, що повинні бути присутніми у мережі постійно. Це сервери, призначення яких полягає в тому, щоб обробляти запити користувачів мережі Інтернет.

Щоб встановити IP-адресу Інтернет-ресурсу (порталу, сайту, веб-сторінки), який містить заборонений контент, слід використовувати певні програмні продукти й утиліти (ping, Trace, Figner LookUp тощо). Найбільш простішим є використання команди ping.

Наприклад, нам необхідно встановити IP-адресу сайту *privet.ru* та місцезнаходження Інтернет-провайдера, який надає послуги хостингу для цього сайту. Спочатку встановлюємо IP-адресу сайту privet.ru. З цією метою необхідно у головному меню системи Windows, натиснувши кнопку «Пуск», обрати пункт меню «Выполнить». У вікні «Запуск программы», яке з'явиться, набрати рядок: ping privet.ru, натиснути кнопку «ОК». За результатами виконання програми отримуємо інформацію про IP-адресу сайту privet.ru 64.34.89.162. Команда ping може бути також виконана і на інших сайтах, що надають таку можливість (як правило, це сайти, що надають сервіс Whois).

Знаючи IP-адресу сайту, подальшим кроком буде встановлення компанії Інтернет-провайдера, яка надає послуги хостингу для цього сайту, за допомогою сервісу Whois або RIPEi, відповідно, володіє інформацією про місце встановлення користувача.

Реєстрація доменного імені здійснюється реєстратором у домні GOV.UA та у разі потреби у домені .УКР відповідно до правил реєстрації та використання доменних імен, установлених адміністраторами зазначених доменів.

Відомості про осіб, які здійснюють адміністративний та технічний супровід доменного імені (назва посади, прізвище, ім'я, по батькові, номер службового телефону та адреса електронної пошти), є відкритими. Адреса електронної пошти, яка використовується у контактних даних осіб, містить офіційне доменне ім'я реєстратора.

Програмно-технічні засоби, на яких розміщуються державні електронні інформаційні ресурси, для яких здійснюється реєстрація доменного імені повинні розташовуватися на території України.

З цією метою слідчий має отримати відповідні ухвали слідчого судді на тимчасовий доступ до комп'ютерних систем на адресу встановлених Інтернет-провайдерів, у яких:

а) зареєстровано доменне ім'я сайту та які здійснюють хостінг для розміщення сайту, з якого здійснювалось розповсюдження шкідливого програмного засобу.

Метою направлення ухвали є отримання інформації, що має відношення до справи, зокрема:

– коли та протягом якого часу був створений даний обліковий запис протиправного характеру;

– з якої IP-адреси було створено обліковий запис користувача, який створив Інтернет-ресурс із шкідливим програмним засобом;

– на кого зареєстрований обліковий запис (повні анкетні дані власників сайту, інформація з панелі адміністрування, IP-адреси, номери телефонів тощо);

– деталізація всіх IP-адрес та часу виходу в даний обліковий запис користувача;

– як здійснювався перегляд даного облікового запису та його наповнення (IP-адреса, установчі дані та час входу);

– яким чином оплачуються послуги за зазначене доменне ім'я (вид платіжної системи, яка використовувалась при поповненні балансу облікового запису користувача даної системи (гаманці, ідентифікатори, види оплат), банківські установи, рахунки тощо;

б) зареєстровано IP-адресу чи поштову скриньку правопорушника-користувача мережі Інтернет, який здійснював спілкування з невстановленого комп'ютерного обладнання:

– якими є реквізити абонента, який здійснював доступ до мережі Інтернет під певною IP-адресою у певний час доби;

– які IP-адреси використовувалися для створення певного облікового запису;

– які IP-адреси використовуються для з'єднання з цим обліковим записом;

– якими є реєстраційні дані (logs) та абонентська інформація про користувача певного облікового запису (електронної поштової адреси) (наприклад, roma_narkoman@ukr.net);

– якими є відомості про певний обліковий запис (електронну поштову адресу), на який пересилається повідомлення після його отримання;

– яким є зміст адресної книги електронної поштової скриньки;

– яким є зміст усіх вхідних і вихідних повідомлень.

в) є права на адміністрування Інтернет-форумом або чатом, через який здійснювалося протиправне спілкування (з метою встановлення IP-адреси правопорушника):

– час реєстрації даної поштової скриньки і IP-адреси, якими користувався правопорушник;

– установчі дані користувача поштової скриньки;

– через який телефонний номер здійснювалась активація облікового запису;

– якими є деталі всіх сеансів входу до даного облікового запису із зазначенням IP-адрес та часу.

З метою отримання даних переписки (спілкування) в Інтернет-форумі або чаті, яку здійснював розповсюджувач шкідливих програмних засобів з їх покупцем, доцільно запросити історію повідомлень на певному Інтернет-форумі певного користувача під певним ніком (мережевим ім'ям). У цьому випадку доцільно, щоб провайдер до відповіді додав інформацію в електронному вигляді.

Для спрямування запитів закордонним хостінг-провайдерам слід використовувати можливості НЦБ Інтерполу з метою зв'язатися з правоохоронними органами тієї держави, де розташовано головний офіс провайдера.

Слід пам'ятати, що стаціонарний комп'ютер, підключений до мережі Інтернет, має в базі Інтернет-провайдера облікові записи імені користувача, його реквізити, адресу встановлення комп'ютерної техніки та засобів комунікації, інші дані (наприклад, технічний телефонний номер). Вказане надає слідчому можливість проведення подальших слідчих розшукових дій, направлених на встановлення особи користувача комп'ютерного обладнання та засобів комунікації, який, можливо, причетний до використання шкідливих програмних засобів.

Якщо з'єднання комп'ютера з Інтернетом відбувається через провідний *модем*, слідчий має витребувати інформацію в Інтернет-провайдера про номер стаціонарного телефону, через який підтримувався зв'язок користувача з провайдером. У подальшому слідчий за визначеним телефонним номером вживає заходів щодо тимчасового доступу до місць, де встановлено модем і підключеного до нього комп'ютерного обладнання та засобів комунікації, а також відпрацьовує їхніх користувачів на причетність до розповсюдження шкідливих програмних засобів.

Якщо з'єднання з Інтернетом відбувається через підключення за допомогою звичайних *мережевих карт* (LAN) та мережевого кабелю, то слідчий витребує в Інтернет-провайдера інформацію про адресу встановлення комп'ютерної техніки та засобів комунікації, а також особу, яка заключила абонентський договір з провайдером. У подальшому слідчий вживає необхідних заходів щодо тимчасового доступу до комп'ютерної техніки чи засобів комунікацій за визначеною адресою, а також відпрацьовує її користувачів на причетність до шкідливих програмних засобів.

Якщо електронну поштову адресу створено навмисно для вчинення протиправних дій, правопорушник може користуватися нею з робочих місць у комп'ютерних Інтернет-клубах, кафе, орендованих квартирах, готелях тощо. В цьому випадку слід встановити наступне:

– конкретний комп'ютер у внутрішній локальній мережі Інтернет-клубу, кафе або іншого місця, де правопорушник анонімно здійснював свою діяльність;

– який адміністратор, офіціанти та інші працівники закладу були на зміні під час виходу правопорушника до мережі Інтернет;

– осіб з числа інших клієнтів, які в той час перебували поблизу комп'ютера правопорушника;

– інший обслуговуючий персонал Інтернет-клубу, кафе, готелю тощо, який міг запам'ятати правопорушника (охоронець, бармен, офіціант, прибиральниця та ін.).

Встановлених осіб необхідно опитати та встановити особу (або скласти фоторобот) правопорушника.

Особливу увагу варто звертати на наявність камер відеоспостереження, які могли зафіксувати правопорушника під час перебування у певному приміщенні, звідки він здійснював вихід у мережу Інтернет. У подальшому здійснюють тимчасовий доступ і перегляд відеоматеріалів, отриманих камерами стеження у місцях появи правопорушника.

Здійснення аналізу отриманих відеоматеріалів дозволить встановити певні ознаки правопорушника (стать, вік, зовнішній вигляд, одяг, атрибути, інші індивідуальні ознаки тощо), встановити транспортний засіб, яким він користується, а також інших осіб, які володіють відомостями про особу правопорушника (оскільки вони були свідками чи спільниками його протиправних дій, або бачили марку чи реєстраційні номери машини, яка його підвозила, тощо).

Для технічної фіксації надання послуг міжнародного телефонного зв'язку спільно з працівниками Державної інспекції електрозв'язку від оператора зв'язку, на мережі якого проводився моніторинг, необхідно отримати:

− роздруківку витягу викликів або дзвінків, знятих за допомогою приладу АСТС за певний період часу з визначеного цифрового потоку;

− роздруківку витягу з білінгової системи АТС оператора зв'язку, на мережі якого проводився моніторинг, викликів або дзвінків правопорушника;

− копію акту технічної комісії про включення з'єднувальних ліній між оператором зв'язку, на мережі якого проводився моніторинг, та правопорушника;

− копію договору на виконання робіт по організації зв'язку між оператором зв'язку, на мережі якого проводився моніторинг, та правопорушником;

− копію договору на надання послуг зв'язку між оператором зв'язку, на мережі якого проводився моніторинг, та правопорушником;

− довідку про надання у користування правопорушнику телефонних номерів, для якої мети;

− схему підключення правопорушника до телефонної мережі;

− схему проходження телефонних викликів або дзвінків.

2.4 Допит

2.4.1 Допит підозрюваного

Допит підозрюваного і потерпілого, мабуть, одна з найбільш поширених слідчих дій. Він є способом отримання, закріплення та перевірки такого виду доказів, як показання названих осіб. Найважливішою умовою цінності свідчень будь-якої особи є її правдивість, яка забезпечується, насамперед, добровільністю і моральним обов'язком давати правдиві показання.

Існують загальні правилами, напрацьовані практикою і закріплені у чинному законодавстві для даної слідчої дії. Допит як потерпілого, так і

підозрюваного необхідно починати із вільного оповідання про все, що їм відомо по суті справи. Вислухавши вільну розповідь, слідчий може поставити питання.

Однак, враховуючи, що практичного досвіду слідчого, як правило, недостатньо для розслідування злочинів у віртуальному світі, що особа злочинця відрізняється цілим рядом особливостей:

- чітко формулює будь-яку професійну задачу, але часто характеризується хаотичною поведінкою у побуті;

- володіє розвиненим формально-логічним мисленням, яке часто підводить у реальному житті;

- прагне до точності, чіткості та однозначності в мові, постійно ставить уточнюючі питання і перепитує, що викликає роздратування співрозмовника;

- постійно використовує комп'ютерний жаргон, малозрозумілий непосвяченим. При проведенні слідчих дій необхідно скористатися допомогою спеціаліста, який би володів спеціальними знаннями в галузі інформатики, телекомунікаційних технологій, мережевих технологій, програмування та обчислювальної техніки, з метою отримання фактичних даних, що містяться в пам'яті комп'ютера, на носіях інформації, комп'ютерної документації та ін., а при необхідності запросити його для участі в допиті (що має бути процесуально оформлено), а також скласти детальний план допиту.

За загальними правилами допит підозрюваного треба починати з питання чи визнає він себе винним. Потім підозрюваному пропонується дати показання по суті.

Предметом проведення допиту в зв'язку з використанням комп'ютерної техніки, програмного забезпечення, шкідливих програмних та технічних засобів є з'ясування:

на початковій стадії – це обставини загального характеру, які цікавлять слідство:

- які навички користування комп'ютером і програмування має підозрюваний, де, коли і за яких обставин він освоїв роботу з комп'ютерною технікою, із конкретним програмним забезпеченням і методами проникнення;

- місце його роботи і посада, чи працює він на комп'ютері за місцем роботи, чи має правомірний доступ до комп'ютерної техніки та до яких видів програмного забезпечення;

- які операції з інформацією за допомогою комп'ютерної техніки виконує на робочому місці;

- чи має доступ до глобальної мережі Інтернет, чи працює в Інтернеті, як часто, де виходить у мережу;

- чи закріплені за ним за місцем роботи логіни та паролі для роботи в комп'ютерній мережі чи з комп'ютерною технікою, що не має доступу до мережі;

- якщо не працює, то які операції виконує на своєму особистому

комп'ютері або особистих комп'ютерах інших осіб зі свого оточення (якщо працює в Інтернет-клубі чи кафе), де і у кого придбав програми для свого комп'ютера;

- які обставини передували вчиненню злочину, а саме :

коли у нього виник намір вчинити злочин у сфері комп'ютерної інформації, хто або що вплинуло на прийняття такого рішення;

чому даний об'єкт обраний ним для злочинного посягання (організація, структура, де сам працював, або стороння установа, підприємство);

яка мета вчинення злочину (чи лише настання таких наслідків, як копіювання, знищення, блокування, модифікація інформації, порушення роботи комп'ютера, системи, мережі або комп'ютерна техніка були засобом і способом вчинення інших традиційних злочинів, наприклад, розкрадання, ухилення від сплати податків, промислове шпигунство і т. ін.);

При проведенні допиту підозрюваного під час досудового розслідування злочинів, що вчиняються з використанням шкідливих програмних чи технічних засобів, слід також враховувати й основні мотиви і цілі скоєння останніх, серед яких можна виділити:

- корисливі (привласнення грошових коштів і майна);
- політичні (шпигунство, діяння, спрямовані на підрив фінансової та грошово-кредитної політики, валютної системи країни, чорний піар);
- дослідницький інтерес;
- хуліганські спонукання і пустощі;
- помсту;
- заздрість;
- перевірку своїх здібностей та ін.

З'ясувати конкретні злочинні дії, вчинені з використанням комп'ютерних технологій (неправомірний доступ до інформаційних баз даних, персональних даних, створення, використання і поширення шкідливих програм, шахрайські дії з використанням інформаційних технологій, порушення правил експлуатації комп'ютерної техніки, системи або їх мережі).

Аналіз практики свідчить про те, що на зміну «хакерам-одинакам» приходять організовані злочинні групи і спільноти, для яких характерним є чіткий розподіл ролей у вчиненому злочині (причому «хакери» нерідко використовуються за наймом).

З огляду на це, в ході допитів підозрюваних необхідно встановити:

- наявність змови з іншими особами на вчинення злочину, хто ці особи;
- хто є ініціатором вчинення злочину;
- час, місце та інші деталі злочинної домовленості;
- розподіл ролей між учасниками злочину (злочинів);
- конкретні дії з підготовки злочину (попереднє вивчення об'єкта злочинного посягання, підтвердження наявності співучасників, вжиття заходів щодо нелегального отримання логінів, паролів для доступу в мережу, відкриття псевдопідприємства, або рахунків у існуючих банках, отримання

кредитних/платіжних карток або ідентифікаційних даних про кредитні/платіжні картки для переказу викрадених грошових коштів і т. ін.);

- частку кожного із співучасників, яку він повинен був отримати в результаті вчинення злочину (злочинів).

Використовуючи сучасні телекомунікаційні мережі, в тому числі глобальну мережу Інтернет, зловмисники отримали можливість чинити злочини буквально «не виходячи з дому», зі свого робочого місця в офісі або з квартири. Об'єкт злочинного впливу може перебувати далеко від місця скоєння злочину, в іншому кінці міста, іншій області й навіть в іншій державі. Такі вторгнення «ззовні» в комп'ютерні мережі потерпілих організацій становлять майже половину всіх учинених комп'ютерних злочинів.

Виходячи з цього, при допитах підозрюваного дуже важливо детально уточнити «технологію» вчинення злочину або злочинів, отримати відомості про те, які електронні й речові докази скоєного є (або могли зберегтися), де можна виявити цікаву інформацію.

Оскільки ця частина допиту вимагає спеціальних знань у комп'ютерній та/або телекомунікаційній техніці, рясніє спеціальною термінологією і специфічною лексикою, допит підозрюваного, як зазначалося вище, слід проводити за участю спеціаліста в цій галузі.

На даній стадії допиту фіксуються (відображаються в протоколі допиту) конкретні деталі, способи і засоби вчинення злочину.

При неправомірному доступі до комп'ютерної інформації, підозрюваний допитується з наступних питань:

- про місце неправомірного проникнення в комп'ютерну систему (мережу), тобто всередині потерпілої організації (шляхом видачі відповідних команд з комп'ютера, на якому знаходиться інформація, і т. ін.) або ззовні;

- яким чином сталося проникнення в приміщення, де встановлено комп'ютерну техніку (якщо не мав до неї доступу або не працював у цій організації), якщо таке проникнення мало місце;

- як здійснено неправомірний доступ до комп'ютерної мережі, які способи подолання інформаційного захисту:

шляхом підбору ключів і паролів (вхід у систему, мережу під ім'ям і паролем одного з легальних користувачів, присвоєння імені іншого користувача за допомогою програми, яка змінює дані, й користувач отримує інше ім'я і т. ін.);

шляхом розкрадання ключів і паролів (візуальне перехоплення інформації, виведеної на екран дисплея, або введення з клавіатури, про паролі, ідентифікатори і процедури доступу; перехоплення паролів при підключенні до каналу під час сеансу зв'язку; електронне перехоплення в результаті електромагнітного випромінювання; збір та аналіз використаних роздруківок, документів та інших матеріалів, що містять відомості про паролі і процедури доступу, тощо);

шляхом відключення засобів захисту;

шляхом руйнування засобів захисту;

шляхом використання недосконалості засобів захисту;

- від кого ним отримано дані про використовувані в потерпілій організації заходи захисту інформації та способи її подолання;

- які засоби використано при вчиненні злочину: а) технічні; б) програмні; в) комбіновані (тобто використання двох або всіх трьох зазначених вище);

- про інші технічні хитрощі, використовувані для неправомірного доступу:

зчитування інформації при підключенні до кабелю локальної мережі при прийомі електромагнітного випромінювання мережевого адаптера;

перехоплення електромагнітного випромінювання від дисплеїв серверів або робочих станцій локальної мережі для зчитування та копіювання інформації;

копіювання даних з машинних носіїв інформації, залишених без нагляду або викрадених з місць їх зберігання;

зчитування інформації з носіїв;

- про способи приховування неправомірного доступу (програмних, помилкових даних про особу, що вчинила неправомірний доступ, та ін.);

- про обставини та кількість фактів незаконного вторгнення до інформаційних баз даних;

- про використання для неправомірного доступу свого службового, посадового становища і в чому це конкретно виразилося.

При створенні, використанні та поширенні шкідливих програм для ЕОМ слідчому в ході допиту підозрюваного необхідно з'ясувати:

1. Обставини створення таких програм, у тому числі:

- на якому комп'ютерному обладнанні, коли і де розроблялася програма;

- чи є дана програма оригінальною розробкою або модифікацією ліцензійної програми зі зміною її первісних функцій і для чого вона призначена;

- яке програмне забезпечення використовувалося при створенні програми;

- чи можливе мимовільне поширення даної програми (тобто, чи є вона вірусом).

2. Яким чином використовувалася шкідлива програма:

- зараження програмного забезпечення комп'ютерів третіх осіб;

- завантаження шкідливої програми в комп'ютер (комп'ютери) за допомогою локальної мережі або глобальної мережі Інтернет і т. ін.

3. До якого виду належать створені та використані нею (співучасниками) шкідливі програми («логічні бомби», «троянські коні», «загарбники паролів», «черв'яки» та ін.), який алгоритм їх функціонування, на яку інформацію вони впливають і т. ін.

4. Способи поширення шкідливих програм:

- продаж через торговельну мережу;
- збут неофіційним шляхом, у тому числі в порядку обміну;
- здача в прокат, передача в позику, тимчасове користування;
- дарування та ін.

5. Відношення підозрюваного до наслідків, які неминучі при виготовленні, використанні та поширенні шкідливих (вірусних) програм.

6. Корислива зацікавленість у створенні, використанні та поширенні шкідливих програм, розміри отриманої наживи.

7. Способи приховування злочину і своєї участі в ньому.

При незаконному втручанні в роботу комп'ютера, систем та комп'ютерних мереж та мереж електрозв'язку, порушенні правил експлуатації комп'ютерів, їх системи, мережі в ході допитів підозрюваних, а такими можуть бути тільки особи, які мають правомірний доступ до комп'ютерного обладнання та мережі, комп'ютерної інформації (оператори, програмісти, техніки-наладчики та ін.), необхідно акцентувати увагу на наступних моментах:

1. Чи був ознайомлений підозрюваний з установленим режимом і правилами; в якому документі таке ознайомлення відображено, в якому підрозділі за місцем роботи підозрюваного він знаходиться.

2. Місце і час (період часу) факту порушення правил експлуатації.

3. В чому конкретно полягало порушення правил експлуатації, які технічні аспекти способу і механізму порушення правил (виконання непередбачених операцій або, навпаки, невиконання запропонованих дій, порушення технології обробки інформації і т. ін.).

4. Які наслідки допущених порушень (нестандартна або нештатна ситуація з комп'ютером і його пристроями призвела до знищення, модифікації або копіювання інформації; виведення з ладу комп'ютерної системи, що викликало блокування інформації і порушення роботи організації, установи, підприємства, систем управління і зв'язку та ін.).

5. Місце настання шкідливих наслідків (далеко не завжди збігається з місцем порушення правил, тобто порушення може статися на робочій станції локальної мережі, а знищення інформації - в сервері та ін.).

Також під час допиту підозрюваного про обставини скоєння комп'ютерних злочинів необхідно встановлювати форми і ступінь провини та відношення до шкідливих наслідків.

При цьому в ході допитів підозрюваних установлюються обставини скоєння ними не тільки комп'ютерних злочинів (тобто використання комп'ютерної техніки як знаряддя або засобу вчинення традиційних злочинів), а й відповідних «традиційних» злочинів.

При скоєнні шахрайства в ході допитів з'ясовується:

1. Яким чином (з використанням свого службового становища, правомірного доступу або шляхом несанкціонованого проникнення в мережу) і з якою метою та в які саме інформаційні бази даних підозрюваний вніс зміни:

- для підробки та фальсифікації бухгалтерських і фінансових документів;

- для зміни розрахункової програми та перерахування, зарахування грошей і цінних паперів на певний рахунок (рахунки) в іншій кредитно-фінансовій установі;

- для порушення правильності обробки первинних бухгалтерських документів, що відображають касові операції, рух товарно-матеріальних цінностей;

- для спотворення вихідних даних, необхідних для прийняття управлінських рішень по товарообігу, виробництву платежів і т. ін.

2. Подробиці використання глобальної мережі Інтернет для доступу до чужих банківських рахунків, даних кредитних карток, а також махінацій, що здійснюються через Інтернет-магазини та сфери послуг («розкручування» фінансових пірамід, азартних ігор, лотерей, шахрайства на Інтернет-аукціонах і дошках оголошень, наприклад, olx.ua, за допомогою сторінок Інтернету).

3. Способи переведення в готівку створеного неврахованого резерву «електронних грошей», цінних паперів і товарно-матеріальних цінностей, їх вилучення в кредитно-фінансових і торгових організаціях й розкрадання.

4. Способи завалювання здійснюваних розкрадань з використанням комп'ютерних даних, канали збуту і місця зберігання викраденого майна і цінностей.

5. Інші обставини скоєних розкрадань, роль співучасників та ін.

Аналогічні питання задаються і при здійсненні інших видів злочинів з використанням комп'ютерних технологій, шкідливих програмних або технічних засобів та при допиті потерпілої сторони від даного виду правопорушень.

2.4.2 Допит потерпілого та свідків

При допиті потерпілої сторони слід врахувати її умовний поділ на наступні три групи: власники комп'ютерної системи; клієнти, що користуються їхніми послугами; інші особи, та обов'язково з'ясувати наступне:

- установчі дані, посада та функціональні обов'язки на робочому місці;

- яка інформація піддавалася неправомірному впливу;

- призначення і зміст інформації, що піддалася неправомірному втручанню;

- як здійснюється доступ до комп'ютерних ресурсів, систем, мереж, кодів, паролів та іншої комп'ютерної інформації;

- як організовано противірусний захист;

- яким чином ведеться облік користувачів комп'ютерної системи;

- хто і як виявив шкідливий програмний чи технічний засіб;

- коли та за яких умов це сталося.

При допиті *заявника* додатково висвітлюються питання щодо:

− документального підтвердження шкоди, завданої несанкціонованим втручанням у роботу ЕОМ, АС або мережі;

− Інтернет-провайдера, який забезпечує доступ до мережі Інтернет потерпілої сторони (технічне обслуговування, технічну підтримку сайту тощо), та угоди з провайдером щодо надання їм послуг;

− Інтернет-технологій та програмних засобів, що використовуються при обліку фінансової діяльності: чи є ресурс оригінальною розробкою;

− кола осіб, які мають доступ до паролів адміністративного інтерфейсу та доступ до ЕОМ;

− обсягу конфіденційної інформації, яка міститься у ЕОМ (мережі), можливості доступу до неї;

− останніх відомих випадків протиправного впливу на роботу ЕОМ, АС чи мережі, зміни, знищення або блокування інформації, яка міститься на зазначеній системі;

− чи збережені дані про вчинення протиправного впливу (в комп'ютері, сервері мережі тощо);

− чи був такий вплив єдиним або він має системний характер;

− які організаційні, програмні та технічні засоби використовуються для забезпечення безпеки мережі.

Під час допиту *провайдера або оператора зв'язку*, необхідно встановити відомості про:

− наявність інформації про здійснення доступу до ЕОМ, АС (мережі) потерпілого;

− IP-адреси користувача мережі Інтернет, яким здійснювався вплив на роботу програмно-технічних засобів потерпілого, ім'я, яке ним використовувалося під час роботи в мережі;

− дані щодо реєстратора доменного імені правопорушника;

− наявність даних щодо користувача IP-адреси, з якої було здійснено протиправний вплив;

− номер телефону (стаціонарного, мобільного), з якого було здійснено доступ до мережі Інтернет, а також дані про його власника;

− місцезнаходження телефону (в тому числі мобільного);

− внесення будь-яких змін або здійснення несанкціонованих дій з інформацією, що міститься на сервері провайдера;

− системність вчинення протиправного впливу з певних IP-адрес мережі;

− минулі спроби протиправного впливу на роботу певної ЕОМ, АС (мережі);

− програмні й технічні засоби, що були використані при здійсненні протиправного впливу.

2.5 Призначення експертиз

Згідно з частиною першою ст. 242 КПК України експертиза проводиться експертом за зверненням сторони кримінального провадження або за дорученням слідчого судді чи суду, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання.

Експертиза комп'ютерної техніки і програмних продуктів призначається у тих випадках, коли необхідно встановити фактичні дані, що мають значення для кримінального провадження і пов'язані із застосуванням комп'ютерної техніки, та вчинені за її допомогою певні дії, які встановлюються на основі спеціальних знань у галузях обчислювальної техніки та програмування.

Об'єктами експертизи комп'ютерної техніки і програмних продуктів є:

– комп'ютерна техніка (системні блоки комп'ютерів, ноутбуки, сервери тощо та їх комплектуючі);

– периферійні пристрої (принтери, сканери, дисководи, звукові карти модеми тощо), комунікаційні пристрої комп'ютерів і обчислювальних мереж;

– носії інформації (накопичувачі на жорстких магнітних дисках, комп'ютерні дискети, оптичні компакт-диски, флеш-карти пам'яті тощо);

– електронні записні книжки, айпеди, айподи, смартфони, мобільні телефони та інші електронні носії текстової або цифрової інформації;

– технічні засоби.

При призначенні та проведенні експертизи комп'ютерної техніки і програмних продуктів необхідно дотримуватися вимог Кримінального процесуального кодексу України, Закону України «Про судову експертизу», Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України 08 січня 1998 р. № 53/5.

Для дослідження робочого стану комп'ютерно-технічних засобів експерту надають ці засоби, а також технічну документацію до них; для встановлення відповідності програмних продуктів певним параметрам – надають носій з копією досліджуваного програмного продукту або програмного коду.

Для дослідження інформації, що міститься на комп'ютерному носієві, експерту надається цей носій, а за потреби – комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій інформації.

З метою визначення, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта або спеціаліста в галузі комп'ютерної техніки.

До об'єктів, які направляються на експертизу комп'ютерної техніки і програмних продуктів, встановлено такі вимоги:

– для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях;

– системний блок комп'ютера та інші пристрої мають бути упаковані й опечатані в такий спосіб, що унеможливлює їх пошкодження, безпосередній доступ до носіїв інформації та підключення системного блоку до мережі електроживлення;

– у постанові про призначення експертизи повинні бути точно вказані місце, час вилучення, а також зовнішній вигляд пристроїв і програмних продуктів, які направляються на експертизу;

– при вилученні комп'ютерів та електронних носіїв інформації їх варто упаковувати в поліетиленовий (або полотняний) пакет, який опечатують. Носії інформації можна упакувати в картонну чи пластмасову коробку та опечатати її. Варто зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їх кількість). Коробку з носіями та опис поміщають до поліетиленового пакету, який заклеюють;

– під час перевезення комп'ютерних засобів вживають заходів щодо запобігання їх механічного пошкодження і взаємодії з хімічно активними речовинами.

Завданням експертизи комп'ютерної техніки і програмних продуктів є:

- встановлення робочого стану комп'ютерно-технічних засобів;

- встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;

- виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

- встановлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Орієнтовний перелік питань, які вирішує експертиза комп'ютерної техніки і програмних продуктів:

1. Які інформаційні ресурси знаходяться в даному комп'ютері?
2. Які технічні несправності має даний комп'ютер або його окремі блоки та пристрої і як ці несправності впливають на роботу комп'ютера (блоку, пристрою)?
3. Чи міститься на даному носії інформація стосовно (зазначити, яка інформація цікавить); якщо так, то у якому вигляді?
4. Яка конфігурація та склад комп'ютерних засобів та чи можливо за їх допомогою здійснити дії, які інкримінуються підозрюваному?
5. Чи заражені надані файли з програмами вірусом, якщо так, то яким саме?
6. Чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача?
7. Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення, копіювання, спотворення, модифікації інформації?
8. Чи є на носії інформація, що була знищена, і чи можна її відновити?

9. Чи могла бути створена зазначена інформація на цьому комп'ютері, чи вона перенесена з іншого носія?

10. Який час створення певної інформації (зазначається яка) на цьому комп'ютері?

11.Чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме – встановлене, невстановлене) програмне забезпечення?

12.Яким чином інформацію (зазначити, яку саме) перенесено до досліджуваного комп'ютера (носія)?

13.Чи можна за допомогою даного програмного продукту реалізувати функції, передбачені технічним завданням на його розробку?

14.Які функціональні несправності має дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому?

15.Чи можливе виконання певних дій за допомогою даного програмного продукту?

16.Чи можливе вирішення певного завдання за допомогою даного програмного продукту?

17.Чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

18.Які правила експлуатації ЕОМ існують у даній інформаційній системі та чи було порушено ці правила?

19. Чи знаходяться порушення правил експлуатації в даній інформаційній системі у причинному зв'язку із знищенням, копіюванням, модифікацією?

20.Чи містять надані файли з програмами шкідливі програмні засоби, якщо так, то які саме?

21.Яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст)?

22.Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно (зазначити зміст)?

23.Чи відповідає стиль програмування досліджуваного програмного продукту стилю програмування певної особи?

24.Чи відповідають прийоми і засоби програмування, що використовувалися при створенні досліджуваного програмного продукту, прийомам і засобам, які властиві даному програмісту?

25.Чи є надані тексти на паперовому носієві записами коду до програми?

26.Яка вартість програмного забезпечення (на час його придбання, вилучення, проведення експертизи)?

27.Яка вартість окремих модулів, що входять до складу програмного продукту?

28.Яка вартість комп'ютерної техніки (окремих комплектуючих) на час придбання (вилучення, проведення експертизи)?

Експертиза телекомунікаційних систем і засобів

Об’єктами експертизи телекомунікаційних систем і засобів є телекомунікаційні системи, засоби, мережі і їх складові частини та інформація, що ними передається, приймається та обробляється.

Основними завданнями експертизи телекомунікаційних систем і засобів є:

– визначення характеристик і параметрів телекомунікаційних систем та засобів;

– встановлення фактів і способів передачі (отримання) інформації в телекомунікаційних системах;

– встановлення фактів і способів доступу до систем, ресурсів та інформації у сфері телекомунікацій;

– визначення якості надання телекомунікаційних послуг на рівні їх споживання;

– встановлення конфігурації та робочого стану телекомунікаційних систем і засобів;

– встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем і засобів;

– дослідження алгоритмів обробки інформації та її захисту в сфері телекомунікацій.

Орієнтовний перелік вирішуваних експертизою телекомунікаційних систем і засобів питань:

1. Які тип, марка, модель телекомунікаційного засобу (системи)?
2. Чи в робочому стані знаходиться телекомунікаційний засіб (об’єкт)?
3. Які характеристики підключень до мережі має телекомунікаційний засіб?
4. Чи змінювались користувачем телекомунікаційної мережі налаштування окремих пристроїв, у який час, які їх значення?
5. Який загальний характер підключень до телекомунікаційної мережі виконував об’єкт (телекомунікаційна система, засіб)?
6. За допомогою яких програмних засобів здійснювалось підключення до телекомунікаційної мережі?
7. Яка топологія апаратних засобів, об’єднаних у телекомунікаційну систему?
8. Чи відповідає функціонування телекомунікаційного засобу (системи) технічній документації?
9. Які технічні характеристики (параметри) має телекомунікаційний засіб (система)?
10. Чи мав місце факт доступу до телекомунікаційної системи та в який спосіб?
11. Чи мало місце використання ресурсів та інформації в телекомунікаційній системі та в який спосіб?

12. Чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі та в який спосіб?

13. Чи є ознаки втручання в роботу телекомунікаційної системи?

14. Чи могли апаратні засоби об'єднуватись у телекомунікаційну мережу та за якими ознаками?

15. Які шляхи маршрутизації даних у телекомунікаційній системі?

16. Чи можливе використання телекомунікаційного засобу (обладнання) для вказаних цілей?

Експертиза слідів рук (дактилоскопічна експертиза)

Головним завданням дактилоскопічної експертизи є ідентифікація особи за слідами її рук, що залишені на місці вчинення злочину на комп'ютерному обладнанні, засобах комунікації, предметах, заборонених для вільного обігу, та інших предметах, яких могли торкатися підозрювані. Якщо версія про особу, яка залишила слід, ще не висунута, а також якщо слідчий вважає за потрібне встановити, чи є на предметах невидимі або слабовидимі сліди, перед експертом варто поставити питання про наявність такого роду слідів і їх придатність для ідентифікації особи.

Об'єктами дактилоскопічної експертизи є речові докази, на яких знайдено сліди рук або припускається їх наявність. Експертиза може бути проведена також шляхом дослідження копії сліду на слідокопіювальній плівці, зліпку об'ємного сліду або масштабного фотознімку сліду.

Як порівняльні зразки надаються відбитки нігтьових фаланг пальців або відбитки долонь осіб, які підлягають перевірці.

Орієнтовний перелік вирішуваних дактилоскопічною експертизою питань:

1. Чи є на об'єкті сліди рук?

2. Чи придатні дані сліди для ідентифікації особи?

3. Чи залишені сліди рук конкретною (однією) особою?

4. Чи однією особою залишено сліди рук, вилучені в різних місцях?

5. Чи є на даному предметі сліди рук і якщо так, то чи придатні вони для ідентифікації?

6. Якою рукою і якими пальцями руки залишено сліди?

7. Які особливості мають руки людини, що залишила сліди (відсутність пальців, наявність шрамів тощо)?

8. Якими ділянками поверхні долоні залишено сліди?

9. У результаті якої дії залишено слід (захват, торкання тощо)?

10. Чи були сліди до вилучення на поверхні конкретного об'єкта?

11. Чи є ознаки переносу вилучених слідів з однієї поверхні на іншу?

Об'єкти дактилоскопічної експертизи мають надсилатися експерту в якомога коротші строки.

До кола осіб, що підлягають дактилоскопіюванню, слід включати і тих, що не причетні до вчинення кримінального правопорушення, якщо вони могли залишити сліди на місці вчинення злочину. Встановлення того факту, що слід залишила певна особа, виключить пошук нових підозрюваних і призначення зайвих експертиз.

Якщо в процесі слідчого огляду не було встановлено, якою частиною руки залишено слід, слідчий направляє експерту як порівняльні зразки відбитки всіх трьох фаланг пальців рук підозрюваної особи, а також відбитки долонь.

Якщо сліди рук після проведення дактилоскопічної експертизи мають бути направлені на судово-медичну експертизу (для встановлення групи крові тощо), слідчий зазначає про це в постанові про призначення дактилоскопічної експертизи з метою забезпечення збереження біологічної ідентичності слідів.

ВИКОРИСТАНІ ТА РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Конституція України, прийнята на п'ятій сесії Верховної Ради України 28 черв. 1996 р. / Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. Кримінальний кодекс України від 05 квітня 2001 р. (зі змінами та доповненнями на сьогоднішній час) // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131.
3. Кримінальний процесуальний кодекс України від 13 квітня 2012 р. (зі змінами та доповненнями на сьогоднішній час) // Відомості Верховної Ради України. – 2013. – № 9–13. – Ст. 88.
4. Деякі питання використання доменних імен державними органами в українському сегменті Інтернету : Постанова Кабінету Міністрів України від 21 жовт. 2015 р. № 851 / [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/851-2015-%D0%BF.

Про запобігання негативним наслідкам використання Інтернет-ресурсів російських провайдерів : Наказ Міністерства внутрішніх справ України від 07 груд. 2015 р. № 146 / [Електронний ресурс]. - Режим доступу: http://www.mvs.gov.ua/mvs/control/main/uk/index.

5. Інструкція про призначення та проведення судових експертиз: затв. наказом М-ва юстиції України від 08 жовт. 1998 р. № 53/5 // Офіц. вісник України. – 1998. – № 46.
6. Бутузов В. М. Злочини із застосуванням сучасних інформаційних технологій / В. М. Бутузов // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2003. – № 7. – С. 84–88.
7. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій : посібник // Б. В. Романюк,

М. І. Камлик, В. Д. Гавловський та ін.; [за ред. Я. Ю. Кондратьева]. – К: НАВСУ, 2000. – 64 с.

8. Волков О. О. Особливості документування злочинів при організації розслідування кримінальних справ, пов'язаних зі створенням, використанням та поширенням шкідливих програмних засобів: (ст. 361-1 Кримінального кодексу України) : метод. рек. / О. О. Волков. – К., 2011. – 48 с. – Бібліогр. : с. 48. Термін. сл. : с. 25-47. – Б.ц.

9. Волков О. О. Особливості проведення допиту підозрюваних та обвинувачених при розслідуванні злочинів, пов'язаних з незаконним створенням, розповсюдженням або збутом шкідливих програмних засобів / О. О. Волков // Вісник Луган. держ. ун-ту внутр. справ ім. Е. О. Дідоренка. – 2008. – Вип. 4. – С. 196-205.

10. Волков О. О. Виявлення доказової інформації при розслідуванні створення, використання, розповсюдження і збуту шкідливих програмних засобів / О. О. Волков // Інформаційне забезпечення розкриття та розслідування злочинів : [у 3-х ч.]. – Луганськ : РВВ ЛДУВС, 2008. – Спец. вип. № 5. – Ч. 3. – С. 158-165.

11. Волков О. О. Особливості проведення допиту свідків при розслідуванні злочинів, пов'язаних з незаконним створенням, розповсюдженням або збутом шкідливих програмних засобів / О. О. Волков // Південноукраїнський правничий часопис. - 2008. - № 1. - С. 137-141.

12. Волков О. О. Об'єктивна сторона складу злочину, передбаченого ст. 361-1 КК України: кримінально-правові, процесуальні та криміналістичні аспекти / О. О. Волков // Кримінальна юстиція в Україні: сучасний стан та перспективи розвитку. – Луганськ : РВВ ЛДУВС, 2010. – Ч. 3. – С. 258-265.

13. Волков О. О. Знаряддя вчинення злочину при розслідуванні злочинів, пов'язаних з створенням, використанням, розповсюдженням і збутом шкідливих програмних засобів / О. О. Волков // Розвиток України в XXI столітті: економічні, соціальні, екологічні, гуманітарні та правові проблеми : зб. тез доп. III Міжнар. наук.-практ. Інтернет-конф. (Тернопіль, 15 жовт. 2008 р.). – Тернопіль : Тернопіль. нац. економіч. ун-т. 2008. – С. 43-46.

14. Климчук О. Б. Юридичний аналіз складу злочину, передбаченого ст. 361-1 Кримінального кодексу України «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» / О. Б. Климчук // Юрид. радник : журнал юристів України. – 2006 . – № 2 . – С. 102-105.

15. Кримінальний процесуальний кодекс України. Науково-практичний коментар / за заг. ред. В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. – К. : ЮСТІНІАН, 2012. – 1 224 с.

16. Міхайліна Т. В. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут : дис. ... канд. юрид. наук : 12.00.08 / Т. В. Міхайліна. – К., 2011. – 240 с.

17. Мотлях О. І. Методика розслідування комп'ютерних злочинів. Монографія / О. І. Мотлях. – К. : Вид-во «Освіта України», 2010. – 236 с.

18. Настільна книга слідчого (наук.-практ. видання для слідчих і дізнавачів) / М. І. Панов, В. Ю. Шепітько, В. О. Коновалова [та ін.]. – К. : Видав. дім «Ін ЮРЄ», 2003. – С. 566–567.

19. Особливості проведення огляду, вилученої комп'ютерної техніки під час розслідування комп'ютерних злочинів / [Електронний ресурс]. – Режим доступу:
http://nbuv.gov.ua/j-pdf/Nzlubp_2011_7_53.pdf.

20. Тактичні особливості проведення огляду місця події при розслідуванні злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій / [Електронний ресурс]. – Режим доступу:
http://web.znu.edu.ua/herald/issues/2011/ur_2011_1/243-248.pdf.

Навчальне видання

РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, УЧИНЕНИХ З ВИКОРИСТАННЯМ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ

Методичні рекомендації

Підписано до друку 20.01.2014. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 3,28. Ум. друк. арк. 3,26. Тираж 40 прим.

Редакційно-видавничий центр
Національної академії внутрішніх справ
03035, Київ-35, пл. Солом'янська, 1

Друк: ФО-П Поліщук О.В.
Свідоцтво суб'єкта видавничої справи ДК №2142 від 31.03.2005
07400, м. Бровари, вул. Незалежності, 2, кв. 148
тел. (044) 592-13-49