Щербюк Х.В., Пядишев В.Г.
Одеський державний університет внутрішніх справ

Особливості вилучення комп'ютерної техніки під час проведення обшуку

Розвиток та розповсюдження сучасних інформаційних технологій сприяли створенню передумов для зростання злочинності, пов'язаної з неправомірним доступом до комп'ютерних мереж, несанкціонованим отриманням або зміною інформації, незаконним використанням та розповсюдженням комп'ютерного програмного забезпечення. У силу своєї специфічності, злочини цього виду мають високий рівень латентності та низький рівень розкриття.

У зв'язку із швидким темпом комп'ютеризації суспільства у працівників Національної поліції виникають труднощі із відсутністю повної обґрунтованої методики розслідування комп'ютерних злочинів та особливостей проведення окремих слідчих дій, зокрема, огляду вилученої комп'ютерної техніки [1].

Коли шукані докази можуть міститися на комп'ютерних носіях, обшук слід проводити забезпечуючи законність та найголовніше доказову базу. Розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій, вимагає спеціальних знань. Залучення фахівців до огляду є обов'язковим. Слідчий, хоч і володіє достатніми навиками і знаннями в області комп'ютерної техніки і інформаційних технологій, але без допомоги фахівця він може припуститись помилок підчас огляду технічної апаратури, зняття необхідної інформації і (або) її вилучення [2].

До комп'ютерних носіїв інформації відносяться магнітні диски, компакт диски (CD), DVD диски, флеш накопичувачі, оптичні диски, магнітні картки, цифрові касети та інші. Такі носії можуть міститися в персональних комп'ютерах, серверах, комунікаційному устаткуванні, комунікаторах, смартфонах, мобільних телефонах, цифрових фотоапаратах і відеокамерах, плеєрах та іншій подібній техніці - вся така техніка з вбудованими носіями вилучається цілком.

Слід пам'ятати, що техніка стрімко розвивається і доступні користувачеві носії можуть завтра з'явитися в складі таких пристроїв, які ще сьогодні їх не мають. В найближчих планах виробників оснастити вбудованими комп'ютерами всю побутову техніку - холодильники, кондиціонери, кавоварки, пральні машини та інше. Комп'ютер в складі побутової техніки, швидше за все, буде включати вбудований або з можливістю трансформування носій і мережевий інтерфейс для віддаленого доступу.

Під час вилучення комп'ютерної техніки не повинна змінюватися жодна інформація яка міститься на носіях які є вилученими. Слідчий повинен довести, що представлена експерту або суду комп'ютерна інформація не змінювалася. Ні в процесі обшуку, ні при подальшому зберіганні [3].

Доступ до інформації та дослідження її «на місці» допустимі

лише в тих випадках, коли неможливо вилучити носій і відправити його на експертизу. Такий доступ повинен проводитися компетентним спеціалістом, який в змозі зрозуміти і дати пояснення кожній своїй дії.

В момент вилучення комп'ютерної техніки слідчий повинен взяти під контроль приміщення, де встановлена техніка, а також електрощит. Не дозволяти нікому, окрім компетентного спеціаліста, доторкатись до техніки і пристроїв електроживлення. Виключені пристрою не варто вмикати. Всю підключену до комп'ютера периферію слід сфотографувати або описати в протоколі, щоб було зрозуміло які були з'єднання. Також варто звернути увагу на місце де знаходиться комп'ютерна техніка, поруч можуть бути записані паролі, мережеві адреси та інші дані, - часто такі записи лежать поруч, приклеєні до монітора, висять на стіні.

Якщо принтер щось друкує, дочекайтеся закінчення друку. Усе, що знаходиться у вихідному лотку принтера, описується і вилучається на ряду з іншими носіями комп'ютерної інформації. Після цього комп'ютери треба вимкнути, це повинен зробити спеціаліст.

Вилучена техніка упаковується згідно з крихкістю і чутливістю до зовнішніх впливів. Особливо чутливі до вібрації жорсткі магнітні диски; їх механічне ушкодження (наприклад, через перевезення в багажнику) призводить до повної недоступності даних.

Крім цього необхідно опитати всіх користувачів на предмет паролів. Варто дізнатися у кожного співробітника всі відомі йому паролі, що мають відношення до вилученої техніки. Паролі не слід сприймати на слух. Їх треба записати по символам, звертаючи увагу на алфавіт і регістр кожного символу і вивірити у джерел. Після виконання всіх необхідних вищевказаних дій в кінці протоколу зазначаються всі заяви присутніх під час огляду та ставляться підписи [4].

Отже, практичне значення вищезазначеного матеріалу є досить вагомим, адже полягає у виокремленні конкретних рекомендації та тактичних дій під час проведення огляду вилученої комп'ютерної техніки під час розслідування комп'ютерних злочинів, що дозволить якісно отримувати доказову базу та ефективно розслідувати кримінальні провадження.

Список використаних джерел

1. *Бутузов В.М Злочини із застосуванням сучасних інформаційних технологій //[Електронний ресурс] – режим доступу// www.catalog.studentochka.ru.*
2. *Касаткин А. В. Тактика сбора и использование компьютерной информации при расследовании преступлений: Дисс. канд. юрид. наук. М., 2010. - 17-18 с.*
3. *Зачек О.І., Навроцька В.В., Федчак І.А. Особливості розкриття та розслідування кіберзлочинів // Методичні рекомендації – Львів: Львівський державний університет внутрішніх справ, 2010. – 60 с.*
4. *Федотов Н.Н. Форензика – компьютерная криминалистика. – М. : Юридический Мир, 2007. – 217 с.*