

ЗАЛУЧЕННЯ СЛІДЧИМ СПЕЦІАЛІСТІВ ПІД ЧАС РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Охріменко С.С., старший науковий співробітник науково-дослідної лабораторії з проблем експертно-криміналістичного забезпечення ННІ № 2 НАВС, кандидат юридичних наук.

Найважливішим фактором своєчасного встановлення ознак комп'ютерних злочинів є ефективне застосування спеціальних знань в процесі перевірки криміналістично значущої інформації. Єдина кінцева задача перевірочних досліджень – виявлення матеріальних ознак діянь, передбачених в нормах кримінального закону. Перевірочне дослідження може бути виконано як в рамках огляду місця події за участю спеціаліста, так й окремо, після огляду, у лабораторних умовах. Тільки за допомогою досліджень носіїв комп'ютерної інформації буде змога достовірно стверджувати про наявність матеріальних ознак комп'ютерних злочинів.

Предмет перевірочних досліджень повністю поглинається предметом подальшої судової експертизи комп'ютерної техніки та програмних продуктів. Крім того, в процесі досліджень вивчаються відповідні елементи комп'ютерних технологій: технічні засоби, програмне забезпечення, дані тощо.

Так, зокрема, при наявності повідомлення щодо несанкціонованого втручання в роботу ЕОМ (комп'ютерів) чи комп'ютерних мереж перевірочні дослідження за участю спеціаліста здійснюються для встановлення таких необхідних для досудового розслідування відомостей, як:

- ознаки злочину;
- місце несанкціонованого проникнення в комп'ютерну мережу (зсередини організації або ззовні);
- спосіб здійснення несанкціонованого доступу та його результати;

– засоби, використані при вчиненні несанкціонованого доступу (технічні, програмні);

– способи подолання захисту тощо.

Звідси під час проведення досліджень необхідна тісна взаємодія особи, що здійснює перевірку інформації про злочин, та спеціаліста. Це пов'язано з завданням своєчасного вжиття необхідних дій з виявлення, вилучення, закріплення й дослідження слідів комп'ютерних злочинів, що є умовою успішного досудового розслідування. Отже, метою такої взаємодії є негайне отримання орієнтуючої інформації від спеціалістів.

Спеціаліст повинен використати такі засоби, які при пошуці і вилученні слідів не призводили б до знищення і псування цих чи інших слідів, не робили б неможливим подальше їх експертне дослідження. Збереження комп'ютерної інформації в оригінальному вигляді для подальшого проведення експертизи здійснюється її фіксацією.

Переважним прийомом наочної фіксації є вилучення спеціалістом предмету (носія комп'ютерної інформації), тому що:

а) цей прийом зводить до мінімуму втрати доказової інформації, неминучі при копіюванні, вживанні інших прийомів фіксації;

б) забезпечується можливість безпосереднього сприйняття учасниками процесу вилученого предмету, яке виключає сумніви, що можуть виникнути при сприйнятті похідних від нього об'єктів;

в) створюються умови для повного, комплексного дослідження всієї інформації, що міститься в предметі;

г) зберігається можливість отримання копій предмету, якщо характер предмету допускає його багатократне копіювання.

Проте в деяких випадках носії комп'ютерної інформації вилучити неможливо. Це в основному відноситься до вінчестерів (жорстких магнітних дисків), що є головним носієм інформації окремої ЕОМ. Це найчастіше пов'язане з тим, що радикальне вилучення комп'ютерної техніки загрожує подальшими претензіями потерпілих підприємств, установ, організацій. Під час фіксації носіїв, що не можуть бути вилучені, робиться копія носія, відповідність якого оригіналу забезпечується застосуванням вказаних вище спеціальних засобів. З неї

при подальших дослідженнях робляться інші копії, які і досліджуються. Можлива кількість разів такого копіювання відносно необмежена, а тому й досліджувати копію комп'ютерної інформації, що міститься на оригінальному носії, можна необмежену кількість разів навіть руйнуючими методами без ризику втрати важливої інформації на оригіналі. Створення копії і робота з копією рекомендується для безпеки досліджень, щоб не пошкодити вихідний матеріал через можливі помилки з невідомими програмами або пастки, встановлені власником даних. Отже, можливість повного копіювання необмежену кількість разів комп'ютерної інформації, що зберігається в комп'ютерній системі, навіть видаленої, можна вирішити другу проблему, яка обмежує дії спеціаліста – необхідність збереження комп'ютерної інформації в обсязі, що відповідає оригіналу. Така копія буде похідним доказом.

Загалом допомога спеціаліста при проведенні слідчих (розшукових) дій не може обмежуватися тільки виявленням, фіксацією та вилученням потенційних носіїв комп'ютерних слідів злочину. За необхідності слідчий в ході слідчої (розшукової) дії може доручити спеціалісту зібрати сліди саме в комп'ютерній інформації, скопійованій з виявлених носіїв, із занесенням в протокол всіх відомостей про зазначений факт.

Визначальною відносно дослідження комп'ютерної інформації є вимога, що застерігає: слідчий не повинен проводити попередніх (перевірочних) досліджень, якщо є небезпека пошкодження або знищення речових доказів, слідів на них. Якщо ж дослідження необхідні для виявлення ознак об'єкту або для аналізу й оцінки їх, то він повинен призначити експертизу.

Незалежно від того, чи здійснювалося дослідження слідчим самостійно або за допомогою спеціаліста, результати, одержані на підставі спеціальних пізнань й з урахуванням встановлених даних, формулюються у вигляді думки про факти, що мають значення для розслідування злочину. Оскільки ці думки не очевидні для осіб, що беруть участь в проведенні слідчої (розшукової) дії, то вони не можуть бути зафіксовані в протоколі.

Дослідження, які були проведені слідчим самостійно, процесуальне відображення їх результатів тим більше неприпустиме, оскільки від слідчого не можуть виходити доказові факти, бо він не входить до переліку джерел судових доказів.

Отже, можна зробити висновок, що всі дії, що проваджуються із носіями комп'ютерних слідів на місці проведення слідчої (розшукової) дії, як вже було зазначено вище, можуть носити характер попереднього дослідження, але без зміни властивостей комп'ютерних засобів, інформації (методичне обмеження) та без надання письмових висновків у протоколі (процесуальне обмеження). Такими діями є пошук, переглядання та копіювання комп'ютерної інформації.

Найскладнішою при розслідуванні комп'ютерних злочинів є така слідча (розшукова) дія як огляд місця події. Безпосередньо на робочому етапі проведення слідчої (розшукової) дії спеціаліст надає допомогу слідчому:

- у виявленні засобів комп'ютерної техніки, її окремих компонентів, документації, інших об'єктів, які можуть містити сліди несанкціонованого втручання;

- у коректному (з точки зору збереження слідів злочину) відключенні засобів комп'ютерної техніки від енергопостачання;

- в описі засобів комп'ютерних технологій, її окремих компонентів і документації, що вилучаються;

- при вирішенні питання визначення складу комплексу комп'ютерної техніки або окремих її компонентів, що підлягають вилученню або ізолюванню від вільного доступу;

- в підготовці засобів комп'ютерної техніки до транспортування (їх упакувці, опечатуванні) й ін.

Спеціаліст під час проведення слідчих (розшукових) дій також допомагає виявити спеціальні засоби, встановлені власником в комп'ютері для знищення інформації при несанкціонованому доступі до нього; встановити, чи необхідний пароль для доступу до інформації; які правила його використання та чи не призведе порушення цих правил до знищення файлів. Слід передбачити, що інформація може бути

зіпсованою за сигналом від портативного випромінювача на кшталт вимикач автомобільної сигналізації. Звідси варто рекомендувати слідчому забезпечити спостереження за персоналом, який перебуває у приміщенні та знає про проведення слідчої (розшукової) дії, час і мету якої за цих обставин слід зберігати в таємниці. Спеціаліст може захистити системні блоки від зовнішнього випромінювання надійним їх екрануванням або застосуванням пристрою активних радіоперешкод із набору вибухотехніка.