УДК 343.985:004 (045)

В.П. Верченко,
старший викладач

ОСОБЛИВОСТІ ПРОВЕДЕННЯ СЛІДЧИХ ДІЙ НА ПОЧАТКОВОМУ ЕТАПІ РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

У статті розглядаються деякі типові помилки, які часто вчиняються при проведенні слідчих дій у відношенні до комп'ютерної інформації або самих комп'ютерів та надаються рекомендації щодо їх усунення.

Ключові слова: слідча дія, комп'ютерні злочини, комп'ютерна інформація, докази.

Як визначено у Розділі XVI чинного Кримінального кодексу України комп'ютерний злочин — це протиправне використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, незаконне втручання в їх роботу (Ст. 361), операції зі шкідливими програмами чи технічними засобами (Ст. 361-1), збут чи розповсюдження електронної інформації з обмеженим доступом (Ст. 361-2), викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (Ст. 362), порушення правил експлуатації автоматизованих електронно-обчислювальних систем (Ст. 363), умисне масове розповсюдження повідомлень електрозв'язку, що призвело до порушення чи припинення роботи комп'ютерних систем (Ст. 363-1) [1].

Але як відомо, у кримінальному праві та криміналістиці вид злочину називають не за засобом (знаряддям) вчинення злочину, а за видом злочинної діяльності (вбивство, крадіжка, шахрайство). Отже для назви комп'ютерних злочинів більш коректним буде термін — злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

Тому подальше вживання для спрощення терміну «комп'ютерний злочин» та «комп'ютерна злочинність» треба розглядати з урахуванням роз'яснення даної дефініції з точки зору кримінального права.

Дослідниками даної теми є: В.О.Маркусь, О.І.Мотлях, А.П.Шеремет та ін. Результати аналізу практичної діяльності правоохоронних органів щодо розслідування комп'ютерних злочинів свідчать про те, що дослідження комп'ютерної техніки доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконують фахівці з необхідною професійною підготовкою.

Докази, що пов'язані з комп'ютерним технічним обладнанням та програмним забезпеченням, які вилучені з місця події, можуть бути легко змінені, як у результаті помилок при їх вилученні, так і в процесі самого їх дослідження. Представлення таких доказів для використання в судовому процесі вимагають спеціальних знань і відповідної підготовки. Тут не можна недооцінювати роль експертизи, що могла б дати кваліфікований висновок щодо поставлених слідством питань.

Однак експертиза вимагає деякого часу не тільки на її процесуальне проведення, але і на пошук відповідних фахівців, а при вилученні комп'ютерної техніки часто важливим фактором, що дозволяє зберегти необхідну доказову інформацію, є раптовість та оперативність. Саме тому вилучення комп'ютерів і інформації доводиться проводити тими силами, що у даний момент проводять слідчі дії. У цьому випадку слідчий саме і не застрахований від помилок, обумовлених недостатністю знань, що пізніше спритно використовується захистом у суді.

Постановка завдання: Поставлена проблема має два аспекти: загальні помилки, що допускаються співробітниками правоохоронних органів при розслідуванні злочинів, пов'язаних з комп'ютерами, і захист інформації, встановлюваний на комп'ютерах їх безпосередніми користувачами.

Метою дослідження є встановлення переліку поширених помилок при проведенні слідчих дій та надання основних рекомендацій щодо їх усунення.

Як відомо виявлення, огляд і вилучення комп'ютерної інформації, як і самих комп'ютерів у ході слідчих дій можуть здійснюватися не тільки при слідчому огляді (Ст. 190 КПК), але і при проведенні інших слідчих дій: обшуку (Ст. 177 КПК), виїмки (Ст. 178 КПК), відтворенні обстановки та обставин події (Ст. 194 КПК) [2].

Розглянемо деякі типові помилки, які часто вчиняються при проведенні слідчих дій у відношенні до комп'ютерної інформації або самих комп'ютерів. Можна виділити деякі правила роботи з комп'ютерами, вилученими при розслідуванні злочинів у сфері комп'ютерної інформації, а також запропонувати загальні рекомендації, що можуть бути корисні при обробці комп'ютерних доказів, працюючи в операційних системах DOS чи Windows.

Помилка 1. Помилкова робота з комп'ютером.

Перше та основне правило, що неухильно повинне виконуватись, полягає в наступному: ніколи і ні при яких умовах не працювати на вилученому комп'ютері. Це правило припускає, що вилучений комп'ютер - насамперед об'єкт дослідження фахівців. Тому його бажано навіть не включати до передачі експертам, оскільки категорично заборонено використовувати будь-які програми на вилученому комп'ютері без вживання необхідних заходів безпеки (наприклад, захисту від модифікації або створення резервної копії). Якщо на комп'ютері встановлена система захисту на вході в нього (наприклад — пароль), то його включення може викликати знищення інформації, що знаходиться на жорсткому диску. Не допускається завантаження такого комп'ютера з використанням його власної операційної системи.

Така міра пояснюється досить просто: злочинцю не складає особливих труднощів установити на своєму комп'ютері програму для знищення інформації на жорсткому чи гнучкому магнітному диску, записавши такі «пастки» через модифікацію операційної системи. Наприклад, проста команда DIR, яка використовується для відображення каталогу диска, може легко бути змінена, щоб відформатувати жорсткий диск.

Після того як дані і сама руйнуюча програма, знищені, ніхто не зможе вірогідно сказати, чи був «підозрюваний» комп'ютер спеціально оснащений такими програмами, чи це результат недбалості при дослідженні комп'ютерних доказів?

Помилка 2. Допуск до комп'ютера власника (користувача) комп'ютера.

Серйозною помилкою є допуск до досліджуваного комп'ютера власника для допомоги при його експлуатації. У багатьох зарубіжних літературних джерелах описуються випадки, коли підозрюваному на допиті пов'язаному з комп'ютерними доказами, було надано доступ до вилученого комп'ютера. Пізніше вони розповідали своїм знайомим, як шифрували файли «прямо під носом у поліцейських», а ті при цьому навіть не здогадувалися. Враховуючи такі наслідки, дуже швидко комп'ютерні фахівці стали робити резервні копії комп'ютерної інформації перш, ніж надавати доступ до них.

Інша проблема пов'язана з можливістю спростувати у суді ідентичність пред'явленого у процесі програмного забезпечення полягає у тому, що знаходилося в даному комп'ютері на момент вилучення. Щоб уникнути таких ситуацій, комп'ютер треба не включаючи опечатати у присутності понятих. Якщо ж співробітник правоохоронних органів приймає рішення оглянути комп'ютер на місці, перше, що варто зробити це зняти копію з жорсткого магнітного диску і будь-якої дискети, що буде вилучатися як речовий доказ. Це означає, що до проведення будь-яких операцій з комп'ютером необхідно зафіксувати його стан на момент проведення слідчих дій.

Помилка 3. Відсутність перевірки комп'ютера на наявність вірусів і програмних закладок.

Для перевірки комп'ютера на наявність вірусів і програмних закладок, необхідно завантаження комп'ютера не з операційної системи, яка знаходиться на ньому, а з своєї заздалегідь підготовленої дискети, або зі стендового жорсткого диску. Перевірці підлягають усі носії інформації — дискети, жорсткий диск та інші носії. Цю роботу варто робити залученому для участі в слідчих діях фахівцю, за допомогою спеціального програмного забезпечення.

Не можна допустити, щоб у суді з'явилася можливість обвинуватити слідство у навмисному зараженні комп'ютера вірусами, чи у некомпетентності при проведенні слідчих дій або просто в недбалості, оскільки довести, що вірус був у комп'ютері до початку дослідження, навряд чи можливо, а подібне обвинувачення поставить під сумніви всю працю експерта та вірогідність його висновків.

Такі найбільш типові помилки, що часто зустрічаються при дослідженні комп'ютерів у справах пов'язаних з розслідуванням комп'ютерних злочинів. Однак розглянутий перелік не охоплює всіх помилок, що виникають у процесі вилучення і дослідження комп'ютерної інформації. Цьому легко знайти пояснення: відсутність достатнього досвіду в подібних справах у нашій країні. У той же час у країнах Західної Європи і, особливо, США є вже досить багатий досвід щодо розслідування складних комп'ютерних злочинів. Варто більш ретельно його вивчати, що дозволить уникнути багатьох помилок.

Для запобігання помилок при проведенні слідчих дій на початковому етапі розслідування, які можуть привести до втрати чи руйнування комп'ютерної інформації, погрібно дотримуватися деяких запобіжних заходів:

Рекомендація 1. У першу чергу треба виконати резервне копіювання інформації.

При обшуках і виїмках, пов'язаних з вилученням комп'ютера, магнітних носіїв і інформа-

ції виникає ряд загальних проблем, пов'язаних зі специфікою технічних засобів, що вилучаються. Так, необхідно передбачати заходи безпеки, що здійснюються злочинцями з метою знищення комп'ютерної інформації. Наприклад, вони можуть використати спеціальне обладнання яке, в критичних випадках утворює сильне магнітне поле, що стирає магнітні записи.

Протягом обшуку усі електронні докази, які знаходяться у комп'ютері чи комп'ютерній системі повинні бути зібрані таким шляхом, щоб вони потім були визнані судом. Світова практика свідчить, що у великій кількості випадків під тиском представників захисту у суді електронні докази не приймаються до уваги. Для того, щоб гарантувати їх визнання як доказів, необхідно суворо дотримуватися вимог кримінально-процесуального законодавства, а також стандартизованих прийомів та методик їх вилучення.

Звичайно, комп'ютерні докази зберігаються шляхом створення точної копії з оригіналу (первісного доказу), перш ніж виконується будь-який їх аналіз. Але робити копії комп'ютерних файлів, використовуючи тільки стандартні програми резервного копіювання, недостатньо. Речові докази можуть існувати у формі знищених або прихованих файлів, а дані, зв'язані з цими файлами, можна зберегти тільки за допомогою спеціального програмного забезпечення, у найпростішому виді це можуть бути програми типу - SafeBack; а для гнучких дискет буває досить програми DOS Diskcopy.

Магнітні носії, на які передбачається копіювати інформацію, повинні бути зазделегідь підготовлені (необхідно впевнитись, що на них нема ніякої інформації). Носії потрібно зберігати у спеціальних упаковках або загортати у чистий папір. Слід пам'ятати, що інформація може бути зіпсована вологістю, температурним впливом або електростатичними (магнітними) полями.

Рекомендація 2. Знайти і виконати копіювання тимчасових файлів.

Багато текстових редакторів і програм управління базами даних створюють тимчасові файли як побічний продукт нормальної роботи програмного забезпечення. Більшість користувачів комп'ютера не усвідомлюють важливості створення цих файлів, тому що вони звичайно знищуються програмою наприкінці сеансу роботи. Однак дані, що містяться усередині цих знищених файлів, можуть виявитися найбільш корисними. Особливо якщо вихідний файл був шифрований чи документ підготовки текстів був надрукований, але ніколи не зберігався на диску, такі файли можуть бути відновлені.

Рекомендація 3. Треба обов'язково перевірити Swap File.

Популярність Microsoft Windows принесла деякі додаткові засоби, щодо дослідження комп'ютерної інформації. Swap File працюють як дискова пам'ять або величезна база даних, і багато різних тимчасових фрагментів інформації, або навіть весь текст документу може бути знайдено у цьому Swap файлі.

Рекомендація 4. Необхідно порівнювати дублі текстових документів.

Часто дублі текстових файлів можна знайти на жорсткому або гнучкому магнітному диску. Це можуть бути незначні зміни між версіями одного документу, які можуть мати доказову цінність. Ці розходження можна легко ідентифікувати за допомогою найбільш сучасних текстових редакторів.

На закінчення хотілося б виділити загальні рекомендації, які необхідно враховувати при дослідженні комп'ютерної техніки на місці події.

Приступаючи до огляду комп'ютера, слідчий і фахівець, що безпосередньо робить усі дії на ЕОМ, повинні дотримувати наступного:

– перед вимиканням комп'ютера потрібно по можливості закрити усі використовувані на комп'ютері програми. Треба пам'ятати, що некоректний вихід з деяких програм може викликати знищення інформації або зіпсувати саму програму;

– необхідно прийняти заходи щодо встановлення пароля доступу у захищені програми;

– при активному втручанні співробітників підприємства, які намагаються протидіяти слідчій групі, потрібно відключити електроживлення всіх комп'ютерів на об'єкті, опечатати їх і вилучити разом з магнітними носіями для дослідження інформації в лабораторних умовах;

– при необхідності отримання консультацій у персонала підприємства, варто одержувати їх у різних осіб шляхом опитування чи допиту. Такий метод дозволить одержати максимально правдиву інформацію та уникнути навмисної шкоди;

– при вилученні технічних засобів, доцільно вилучати не тільки системні блоки, але й додаткові периферійні пристрої (принтери, стрімери, модеми, сканери тощо);

– при наявності локальної обчислювальної мережі необхідно мати потрібну кількість фахівців для додаткового дослідження інформаційної мережі;

– вилучати усі комп'ютери (системні блоки) і магнітні носії;

– потрібен ретельний огляд документації, звертаючи особливу увагу на робочі записи операторів ЕОМ, тому що часто саме в цих записах недосвідчених користувачів можна знайти коди, паролі й іншу дуже корисну інформацію;

– варто скласти список усіх позаштатних і тимчасово працюючих фахівців організації (підприємства) з метою виявлення програмістів і інших фахівців у галузі інформаційних технологій, що працюють у даній установі. Бажано встановити їх паспортні дані, адреси і місце постійної роботи;

– потрібно записати дані всіх людей, що знаходяться у приміщенні в момент приходу слідчої групи, незалежно від пояснення причини перебування їх у даному приміщенні;

– варто скласти список усіх співробітників підприємства, що мають доступ до комп'ютерної техніки або часто перебувають у приміщеннях, де знаходяться ЕОМ.

Якщо безпосередній доступ до комп'ютера можливий і всі небажані ситуації виключені, приступають до огляду, причому слідчий і фахівець повинні чітко пояснювати всі свої дії понятим.

При огляді повинні бути встановлені:

– конфігурація комп'ютера з чітким описом усіх пристроїв;

– номера моделей і серійні номери кожного з пристроїв;

– інвентарні номери, що привласнюються бухгалтерією при постановці обладнання на баланс підприємства;

– інша інформація з фабричних ярликів (на клавіатурі ярлик звичайно знаходиться на зворотній стороні, а на моніторі і процесорі — на задній). Така інформація, заноситься до протоколу огляду обчислювальної техніки і може виявитися важливої для слідства.

Рекомендація 5. Треба перевірити і проаналізувати роботу комп'ютерної мережі.

Комп'ютери можуть бути зв'язані між собою в комп'ютерну мережу (наприклад, локальну), котрі в свою чергу можуть бути з'єднані через глобальну комп'ютерну мережу Internet. Тому не виключена ситуація, коли певна інформація (яка може бути використана як доказ) буде передана через мережу в інше місце. Не виключений також випадок, що це місце буде знаходитись за кордоном або на території декількох країн. У такому випадку необхідно використати всі можливості (документацію, опитування, технічні можливості системи) для встановлення місцезнаходження іншої комп'ютерної системи, куди була передана інформація. Як тільки це буде зроблено, необхідно терміново надіслати запит, з виконанням встановлених вимог, про надання допомоги (або правової допомоги, якщо така необхідна для виконання поставлених у запиті питань) у компетентний правоохоронний орган відповідної країни (по встановленим офіційним каналам, наприклад Інтерпол). Саме на цьому етапі виникають найбільші труднощі в організації роботи щодо розслідування злочину, який вчиняється за допомогою комп'ютерних технологій та кримінального переслідування злочинців.

Особливу цінність при розслідуванні у комп'ютерних мережах відіграють так звані «логі», інформація яка міститься в лог- файлах (текстові файли). За допомогою отримання цієї інформації можливо визначити рахунок користувача, його ідентифікатор, час транзакції, мережну адресу, телефонний номер, а також з'ясувати, що саме трапилось в системі, що було знищено, змінено, скопійовано, які ресурси були задіяні для цього [3, с. 198].

«Логі» можуть збиратися в комп'ютерних системах на різному рівні: операційній системі, спеціально встановленому програмному забезпеченні (наприклад, програмний аудит безпеки), окремих модулях баз даних і навіть у деяких прикладних програмах. Фізично ця інформація може знаходиться в різних місцях: від робочої станції і серверу мережі до віддаленого серверу.

Висновки.

Як висновок, треба підкреслити, що будь-які дії, пов'язані з розслідуванням злочинів у сфері використання комп'ютерних технологій (особливо вилучення інформації і комп'ютерного обладнання), доцільно з самого початку залучення фахівця у галузі інформаційних технологій. До початку слідчих дій необхідно також мати певну інформацію щодо: марки, моделі комп'ютеру, операційної системи, периферійних пристроїв, засобів зв'язку та будь-які інші відомості про систему, котра є об'єктом розслідування.

Широке впровадження комп'ютерних технологій вимагає також певних змін у кримінально-процесуальних нормах, що регламентують процедури в частині використання нових джерел доказів. У той же час перед правоохоронними органами відкриваються нові можливості використання інформаційних технологій, як технологічного приладдя у розслідуванні комп'ютерних злочинів.

Література

1. *Кримінальний* кодекс України (прийнятий сьомою сесією Верховної Ради України 5 квітня 2001 р.) зі змінами та доповненнями №2756-VI від 02.12.2010 року. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?user=a&find=1&typ=21

2. *Кримінально*-процесуальний кодекс України зі змінами та доповненнями №1071-V від

24.05.2007 року. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?user=a&find=1&typ=21

3. *Голубєв В.О.* Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В.Д. Гавловський, В.С. Цимбалюк. — Запоріжжя: Просвіта, 2001. — 201 с.

В.П. Верченко

Особенности проведения следственных действий на начальном этапе расследования компьютерных преступлений.

В статье рассматриваются некоторые типичные ошибки, которые часто совершаются при проведении следственных действий по отношению к компьютерной информации или компьютерной технике и даются рекомендации по их устранению.

V.P. Verchenko

Features the in investigation initially investigating computer crimes.

This article discusses some common mistakes that are often made while carrying out investigations in relation to computer data and computers themselves and recommendations for their elimination.