УДК 343.985

О. В. Захарова,
кандидат юридичних наук, доцент кафедри кримінального процесу
та криміналістки Львівського державного університету
внутрішніх справ

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОГЛЯДУ, ВИЛУЧЕНОЇ КОМП'ЮТЕРНОЇ ТЕХНІКИ ПІД ЧАС РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ.

Розглядаються тактичні особливості проведення слідчої дії, такої як огляд вилученої комп'ютерної техніки під час розслідування комп'ютерних злочинів.
Ключові слова*: слідчий огляд, комп'ютерна техніка, інформаційні технології.*

Рассматриваются тактические особенности проведения следственного действия, такого как обзор изъятой компьютерной техники во время расследования компьютерных преступлений.
Ключевые слова*: следственный обзор, компьютерная техника, информационные технологии.*

The tactical features of leadthrough of investigation action are examined, such as a review of the withdrawn computer technique during investigation of computer crimes.
Keywords: *investigation review, computer technique, information technologies.*

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 [1].

Постановка проблеми. У силу своєї специфічності, злочини цього виду мають високий рівень латентності, низький рівень розкриття та нерідко скоюються для приховування більш тяжких злочинів.

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

Мета цієї статті є удосконалити практичні рекомендації щодо проведення огляду вилученої комп'ютерної техніки під час розслідування комп'ютерних злочинів, на основі аналізу наукових праць, які в подальшому можуть застосовуватись в правоохоронних органах.

Стан дослідження. Окремі питання щодо розслідування комп'ютерних злочинів неодноразово досліджували у своїх працях В.Вєхов, М.Салтевський, В.Бутузов, А.Касаткин, В.Голубєв та інші автори. Але стрімкий зріст злочинності в данному напрямку дає поштовх для глибокого дослідження цієї тематики.

Як визначено у Розділі XVI нового 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), 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)[2,с.200].

Виклад основних положень. З метою виявлення слідів злочину та інших речових доказів, з'ясування обстановки злочину, а також інших обставин, які мають значення для справи, слідчий проводить огляд місцевості, приміщення, предметів та документів. Процесуальний порядок проведення огляду регламентується ст.ст.190-193, 195 Кримінально-процесуальним кодексом України [3, с.232].

Важливим елементом є підбір понятих (на підставі ст.191 КПК України огляд проводиться в присутності не меньше двох понятих), вони мають бути обізнані в комп'ютерній техніці. Поняті повинні володіти мінімально необхідними спеціальними знаннями в сфері обробки комп'ютерної інформації (хоча б на рівні користувачів.

Огляд предметів, вилучених під час огляду місця події, при виїмці або обшуку слідчий проводить на місці події, обшуку або виїмки, а у випадках, коли це неможливо, за місцем провадження у справі.

Комп'ютери які входять до складу інформаційної системи – це складне обладнання, яке потребує обережного поводження з ним під час роботи на місці події. Слід пам'ятати, що комп'ютери можуть містити в собі велику кількість даних, які належать сторонній особі, або організації (наприклад можуть бути об'єктом інтелектуальної власності). Тому обережність при поводженні з комп'ютером необхідна як з точки зору збереження важливої доказової інформації, так і з точки зору запобіганню нанесення матеріальних збитків та збереження власності [4, с.60]. Саме тому розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій, вимагає спеціальних знань. Залучення фахівців до огляду є обов'язковим, на підставі ст.191 КПК України. 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.

Опитування слідчих і фахівців в області обчислювальної техніки показав, що тільки 14% слідчих працюють на комп'ютері на рівні користувача, 56% не знають нічого про принципи його роботи. З іншого боку,

92% з числа опитаних програмістів вважають, що на сучасному рівні розвитку обчислювальної техніки без участі професіонала знайти «заховану» в комп'ютері інформацію без ризику знищення її майже неможливо [5, с.17-18].

Спеціалісти, яких залучають для проведення огляду комп'ютерної техніки, повинні мати відповідні знання, застосування яких забезпечило б виконання зазначених слідчих дій.

Зважаючи на швидкоплинність таких злочинів й складність їх виявлення та розслідування, В.Голубєв зазначає, що бажано мати заздалегідь складений список спеціалістів, які можуть надати слідству реальну допомогу [6].

При розслідуванні кримінальних справ про комп'ютерні злочини можуть залучатися різні спеціалісти, а саме::

- працівників експертних підрозділів усіх рівнів і різних відомств;
- компетентні працівники контролюючих органів;
- представників наукових та педагогічних колективів, які мають відповідні знання у галузі інформаційних технологій;
- приватних осіб, які не перебувають в штаті офіційних структур [7, с.57].

В той же час, привертаючи фахівця, слідчому необхідно переконатися в його компетентності. Річ у тому, що, не дивлячись на поширену протилежну думку, загального поняття «Фахівець з комп'ютерної техніки» не існує. Можна говорити лише про те, що є фахівець, компетентний в конкретних комп'ютерних системах. Так, наприклад, фахівець з операційної системи MS DOS не обов'язково буде знайомий з операційною системою Windows NT, а кваліфікований користувач персонального комп'ютера може не уміти поводитися з великими обчислювальними комплексами [8, с.157].

При огляді комп'ютерів не можна поблизу користуватись радіотелефонами. Оскільки вони шкідливо впливають на комп'ютерну систему [9, с.- 477].

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

Спеціаліст тим часом, зовнішнім оглядом комп'ютерного засобу встановлює наступні обставини, які заносяться до протоколу:

а) склад комп'ютерного засобу: наявність системного блоку, монітора, клавіатури, принтера, модему, безперебійного джерела живлення, колонок та інших периферійних пристроїв;

б) розташування пристроїв на передній панелі системного блоку; наявність та види пристроїв зберігання інформації (дисководи), а також пристроїв зчитування кредитних та парольних карт І т. ін. (особливо відмічається наявність не відомих йому пристроїв, наприклад, для знищення інформації);

в) розташування роз'єднань на задній панелі системного блоку, наявність та види вмонтованих пристроїв, мереженої плати, модему; наявність портів послідовного та паралельного каналів[10, с.35].

Огляд комп'ютера слід почати з системного блока, перш за все зазначається зовнішній вигляд (корпус), а саме: розмір, тип корпуса, з якого матеріалу виготовлений, колір, характерні індивідуальні ознаки (наявність дисководу для гнучких дисків, дисководу для компакт-дисків, їх місце розташування і т.д.), наявність пошкоджень, надписів, гарантійних наліпок. Після чого слід описати комплектацію системного блока, в переважній більшості він складається з: материнської плати, процесора, оперативної пам'яті, блоку живлення, жорсткого об'ємного диска, відео карти, CD-ROMA, флопі диска, картрідера, при описі цих складових необхідно зазначити форму, розмір, матеріал виготовлення, колір, зовнішні ознаки, пошкодження, виробник, модель, марка, серія, ідентифікаційний номер, об'єм, наявність гарантійних наліпки та, що на них зазначено.

Крім цього оглядаються периферійні пристрої (принтер, модем, клавіатура, монітор і т.д), при огляді яких в протоколі зазначається призначення кожного пристрою, назву, кількість, розміри, колір, виготівник, серійний номер, комплектацію.

В протоколі огляду треба відобразити 1) шкідливі програми; 2) програми для ЕОМ, які призводять до дій, несанкціонованих користувачем (які впливають на кінцеві результати технологічного процесу), 3) виявлені спеціальні технічні пристрої негласного отримання та знищення комп'ютерної інформації, 4) показники спеціальних тестових програмно-апаратних засобів, 5) сліди пальців рук на комп'ютерах, охоронних та сигнальних пристроях, на їх клавіатурі, з'єднувальних проводах, 6) залишки з'єднувальних проводів та ізоляційних матеріалів, 7) сліди вдавлювання, проплавлення, надрізу ізоляції з'єднувальних проводів тощо.

Для більш ефективного і якісного отримання доказової інформації при проведенні данної слідчої дії, слід дотримуватися наступних рекомендацій:

- після зовнішнього огляду слід підготувати відповідну комп'ютерну техніку, яка буде використовуватися для зчитування та збереження копій окремих жорстких дисків окремих файлів і папок (крім комп'ютера потрібен кабель та спеціальне програмне забезпечення, яке дозволяє здійснювати копіювання та експрес-аналіз інформації). Для якісного копіювання інформації потрібна відповідність не марок комп'ютерів, а об'ємів використовуваних жорстких дисків: у персонального комп'ютера цей об'єм повинен бути не меншим об'єму диску комп'ютера, що оглядається). Копіювання системи (інформації або даних) яка досліджується повинно бути стандартною

процедурою, а не рекомендацією і всі дослідження проводити з копією, а не з самим оригіналом, крім цього бажано робити декілька копій адже виникають випадки коли при непрофесійному дослідженні може стиратись інформація;

- відшукати і з копіювати данні знищених файлів, адже більшість користувачів не обізнані у комп'ютерних технологіях і не знають, що данні знищених файлів можна відновити, а в них зазвичай міститься цінна інформація;

- перевірка Swap File, данні файли працюють як дискова пам'ять або величезна база даних, фрагменти інформації, або весь текст документу може бути знайдено у цьому Swap файлі;

- порівняння дублікатів 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.

- супровід данної слідчої дії фотографуванням та маркуванням, при фотографуванні необхідно виконати детальну фотозйомку передньої і задньої частин комп'ютерної техніки, а також змін зображень на моніторі. Треба підкреслити, що фотографування та маркування елементів комп'ютерної системи, яка вилучається, дає можливість з точністю відтворити стан комп'ютерної техніки у лабораторних умовах дослідження.

Після виконання всіх необхідних вищевказаних дій в кінці протоколу зазначаються всі заяви присутніх під час огляду та ставляться підписи.

Висновки. Практичне значення данної статті полягає у аналізі наукового матеріалу та виокремлення 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 справи.

Література:

1. *Бутузов В.М Злочини із застосуванням сучасних інформаційних технологій //[Електронний ресурс] – режим доступу//* www.catalog.studentochka.ru.

2. *Кримінальний кодекс України станом на 1 вересня 2010 року. – К.: Атіка, 2010. – 200 с.*

3. *Кримінально-процесуальний кодекс України станом на 1 вересня 2010 року. – К.: Атіка, 2010 – 232 с.*

4. *Зачек О.І. , Захарова О.В., Навроцька В.В. , Федчак І.А. Особливості розкриття та розслідування кіберзлочинів // Методичні рекомендації – Львів: Львівський державний університет внутрішніх справ, 2010. – 60 с.*

5. *Касаткин А. В. Тактика сбора и использование компьютерной информации при расследовании преступлений: Дисс. канд. юрид. наук. М., 1997. - 17-18 с.*

6. *В. Голубев. Деякі особливості тактики окремих слідчих дій при розслідуванні комп'ютерних злочинів // [Електронний ресурс] – режим доступу* http://www.crime-research.org.

7. *Ніколайчук С.І., Никофорчук Д.Й., Семчук А.Г., Шутенко С.В., Липчей.//Протидія злочинам, що вчиняються у сфері використання ЕОМ, систем і компютерних мереж. // Науков-практичний посібник.-К.:КНТ, 2007.-57с.*

8. *Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М., 1998. – 157 с.*

9. *Біленчук П. Д .Криміналістика // Підручник. 2-ге вид., випр. і доп.- К.: Атіка, 2001.- 477с.*

10. *Салтевський М.В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ. // Навч. Посібник. – Харків: Нац. юрид акад. України. 2000. – 35 с.*