комп'ютерної мультиплікації дозволяє продемонструвати фази розвитку ДТП з різних точок зору, моделювати специфічні дорожні умови, наприклад, туман, снігопад тощо, відтворити які іншими засобами неможливо.

П'ятою підставою, за якою класифікуються моделі, є об'єкт моделювання. Модельованими об'єктами під час проведення автотехнічних експертиз може виступати речова обстановка на місці ДТП, транспортні засоби, тіло людини і механізм ДТП у цілому.

Вибір моделі залежить від завдань дослідження. Якщо графічна модель призначена замінити об'єкт у процесі ідентифікації, то вона повинна відбивати загальні й приватні ознаки в обсязі, достатньому для індивідуалізації об'єкта. Якщо графічне моделювання здійснюється, наприклад, з метою визначення взаємного розташування транспортних засобів, то виготовлення індивідуальних моделей кожного автомобіля відбере багато часу, а для вирішення питання виявиться недоцільним: модель повинна відбивати лише обмежене коло тих загальних ознак, що потрібні в даному конкретному випадку (наприклад, розміри й пропорції автомобіля). Звідси випливає найважливіша вимога до графічної моделі – вона повинна містити доцільний мінімум ознак моделюваного об'єкта.

Список літератури: 1.Словарь основних терминов судебных экспертиз. М., 1980. 2. Аверьянова Т.В. Содержание и характеристика методов судебно-экспертных исследований. Алма-Ата, 1991. 3.Энциклопедия судебной экспертизы/ Под ред. Т.В. Аверьяной, Е.Р. Россинской. М., 1992.

Надійшла до редколегії 25.02.02

В.А. Коршенко

ДЕЯКІ ОСОБЛИВОСТІ ПОВОДЖЕННЯ З КОМП'ЮТЕРНИМИ ЗАСОБАМИ ПІД ЧАС ПРОВЕДЕННЯ СЛІДЧИХ ДІЙ

Останнім часом у вітчизняній юридичній літературі та у публікаціях фахівців близького зарубіжжя, в яких розглядаються проблеми розвитку криміналістики і судової експертизи, почали з'являтись рекомендації для слідчого щодо порядку проведення слідчих дій, пов'язаних з оглядом, вийомкою і підготовкою персональних комп'ютерів, периферійних пристроїв і інших комп'ютерно-технічних засобів до відправлення на експертизу. В основному ці публікації носять однотипний характер і мають, на наш погляд, ряд як дрібних недоліків, так і грубих помилок. Взагалі ж дана тема цілком актуальна, і обумовлюється появою в переліку доказів по кримінальним і цивільним справам документів і інформації на комп'ютерних носіях. Даний факт змушує по-новому глянути на проблему застосування спеціальних знань в галузі комп'ютерно-технічної експертизи (КТЕ) під час розслідування злочинів і здійснення окремих слідчих дій. Це обумовлено тим, що припущення про наявність на комп'ютерному носії (жорсткому магнітному диску (вінчестері), дискеті, CD-диску, оптомагнітному диску і т.п.) інформації, яка має відношення до скоєного злочину, носить вірогідний характер у тих випадках, коли комп'ютер фігурує як елемент об'єктивної сторони злочину. Нерідко, виходячи із слідчих ситуацій, слідчий має підстави припускати, що в будь-якому

комп'ютері міститься така інформація. Для того, щоб зазначена інформація могла перетворитись на докази, необхідно її знайти та процесуальним шляхом виявити. Одним із основних процесуальних способів перетворення комп'ютерної інформації на докази є проведення КТЕ носіїв, на яких вона міститься. Відомо, що успіх будь-якої криміналістичної експертизи багато в чому залежить від того, наскільки вміло були зібрані, зафіксовані, збережені об'єкти дослідження, наскільки вчасно призначена експертиза, наскільки ретельно були підготовлені матеріали для її проведення.

У зв'язку з цим вважається за доцільне розглянути декілька загально розповсюджених помилок, які роблять слідчі, дізнавачі під час проведення слідчих дій, та надати відповідні рекомендації щодо їх уникнення.

На наш погляд, однією із помилок є рекомендація слідчому робити якінебудь дії з комп'ютерною технікою на місці її виявлення з метою пошуку, відновлення і запису інформації [1, с.156–161; 2 с.84–113; 3, с.73-81]. Так, М.О. Селіванов та І.Дворкін вказують на те, що слідчому при пошуку, фіксації і вилученні речових доказів корисно мати при собі дискети для копіювання на них інформації, яка міститься в комп'ютері, а також дискету (чи кілька дискет) з набором сервісних програм, підбор яких може провалитися в ході нагромадження досвіду розслідування кримінальних справ розглянутої категорії і в міру створення нових, більш досконалих програм. Мінімальний набір, що рекомендується, включає сервісні програми, що забезпечують визначення властивостей і якостей комп'ютера (тестові програми), перевірку справності окремих пристроїв і зовнішньої пам'яті. Крім того, для роботи з комп'ютером слідчому рекомендована будь-яка програма, яка дозволяє працювати з інформацією на твердому диску комп'ютера (копіювати і переглядати інформацію, яка міститься у файлах, що зберігаються на комп'ютері) [4, с.412].

Такий підхід визнається нами абсолютно невірним і неприйнятним, тому що властивості найбільш розповсюдженого програмного забезпечення комп'ютерів дозволяють зробити висновок про заборону в категоричній формі будь-яких маніпуляцій з комп'ютерною технікою на місці події. Даний висновок виходить з декількох причин.

1. Операційні системи (ОС) сімейства Microsoft Windows[1] , а також більшість програм, які функціонують під їх управлінням, мають здатність схованих взаємодій з файловою системою комп'ютера (створення файлів підкачки, тимчасових файлів, резервних копій і т.д.), містять різні механізми відстеження станів програм і документів. Запуск комп'ютера з таким програмним забезпеченням сам по собі тягне безумовну і сховану зміну (перекручування) слідової картини.

2. Більшість розповсюджених програм, що функціонують під керуванням ОС MS-DOS, також мають здатність схованих взаємодій з файловою системою комп'ютера, у результаті чого утворюються криміналістично-значимі сліди, які ні яким чином не пов'язані зі скоєним злочином.

3. В результаті створення або копіювання будь-якої інформації на твердий диск (вінчестер) досліджуваного комп'ютера зменшується імовірність відновлення знищеної з нього інформації.

---

1 Windows 3.1x, Windows 9x, Windows NT, Windows XP тощо.

4. Використання програмного забезпечення досліджуваного комп'ютера з метою виявлення інформації, несе загрозу знищення визначеної кількості криміналістично-значимих слідів у файловій системі комп'ютера і настройках програм.

5. Документи й інші сліди злочину, якщо вони розташовуються на машинних магнітних носіях інформації, можуть бути ненавмисно знищені слідчим, дізнавачем без можливості відновлення під час проведення слідчих дій, якщо не дотримується особливий порядок поводження з носієм інформації.

6. На досліджуваному комп'ютері може бути встановлена ОС не сумісна або частково сумісна з Windows[1] , і спроба запуску програмного забезпечення може привести до непередбачених наслідків: від змін даних до повного знищення інформації.

Друга розповсюджена помилка – це рекомендація «коректного» вимикання комп'ютера, який був виявлений на місці проведення слідчої дії у ввімкненому стані. Так, А.Н.Яковлєв стверджує, що фіксація «комп'ютерних» слідів злочину можлива тільки за допомогою коректного завершення функціонуючих програм, вимикання комп'ютера і кваліфікованого рішення завдання щодо визначення комплекту комп'ютерної техніки або окремих компонентів, які підлягають вилученню слідчим [6].

Поняття «коректне вимикання» мінялося в міру удосконалення старих і нових ОС та комп'ютерно-технічних засобів. На початку комп'ютерно-технічного прогресу жорсткі магнітні диски не «вміли» самостійно паркуватись[2] і під поняттям «коректне вимикання» малося на увазі введення команд або запуск відповідних програм, які здійснювали паркування магнітної голівки. Надалі дана функція стала здійснюватися незалежно самим вінчестером, і при використанні ОС MS-DOS про коректне вимикання не згадувалось, або під «коректним завершенням» малося на увазі коректне завершення конкретної запущеної програми і вимикання комп'ютера шляхом натискання клавіші «Живлення» («Power»). Ситуація істотно змінилася з появою на ринку операційних систем Windows. Зазначені ОС на відміну від MS-DOS є багатозадачними й у процесі своєї роботи здійснюють сховані взаємодії з файловою системою комп'ютера. Це виражається в самостійному запуску бібліотек і виконавчих модулів, створення файлів підкачки, тимчасових файлів і т.д. При цьому більшість зазначених дій відбувається без відома користувача і їх зміна вимагає суттєвих знань та досвіду роботи з конкретною операційною системою[3] і, найчастіше, перезапуску системи. У зв'язку з цим по закінченні роботи в ОС Windows рекомендувалося завершити всі запущені програми і вибрати пункт «Завершення роботи» («Shut down the computer)[4] в меню «Пуск» («Start»), що і

---

1 Останнім часом велике розповсюдження отримали операційні системи Linux, Unix, а також альтернативні типу Lindows, BeOS і т.п. [5, с.28-29].

2 Паркування – це встановлення магнітної головки (головок) вінчестера в фіксатори, щоб запобігти пошкодженню самої головки або поверхні магнітного диску при переміщені носія в просторі.

3 Функціонування і принципи роботи ОС сімейства Microsoft суттєво відрізняються один від одного в залежності від призначення: домашній або настільний ПК, робоча станція, сервер и т.п.

4 В деяких версіях Windous цей пункт має назву «Turn Off the computer».

було «коректним завершенням» роботи комп'ютера. При виконанні зазначених дій ОС Windows знищує всі тимчасові файли, вигружає службові модулі і бібліотеки, потім видає повідомлення про дозвіл виключити комп'ютер кнопкою «Живлення». З появою системних блоків форм-фактора «ATX» термін «коректне вимикання» знову став зводиться до натискання кнопки «Живлення», тому що всі інші дії комп'ютер виконує самостійно.

У зв'язку з вище сказаним, при виявленні комп'ютера на місці проведення слідчих дій у включеному стані ми рекомендуємо негайно відключити його і периферійні пристрої від мережі електроживлення. У першу чергу необхідно відключити системний блок. Якщо комп'ютер приєднаний до електромережі через джерело автономного (безперебійного) живлення (UPS), то необхідно спочатку розірвати з'єднання між системним блоком і UPS шляхом витягування шнура живлення з'єднуючого останній з комп'ютером з боку системного блоку. Якщо є підтверджена інформація, що комп'ютери зокрема і все місце, де проводяться слідчої дії (кімната, приміщення тощо) не обладнані UPS, то можливо знеструмити все приміщення[1], але у разі що це не заважатиме її загальному плану проведення.

Варто враховувати, що вимикання комп'ютера шляхом натискання на кнопку «Живлення» є неправильним, тому що в корпусах форм-фактора ATX вона програмована. Користувач (злочинець) може запрограмувати вказану кнопку на виконання будь-якої дії.

Дана рекомендація пропонується в зв'язку з тим, що:

1) користувачем (користувачами) комп'ютера можуть бути запущені програми, що знищують важливу інформацію або передають її на інший комп'ютер;

2) користувачем (користувачами) комп'ютера можуть бути запрограмоване знищення або зміна інформації при здійсненні певної дії (дій), наприклад видалення каталогу з документами при натисканні на клавішу «Живлення» або при прийомі телефонного дзвінка;

3) можливий несанкціонований доступ до інформації комп'ютера через видалений доступ (локальні з'єднання, радіомодеми і т. ін.);

4) на більшості комп'ютерів встановлена операційна система Windows, яка за принципом своєї роботи при аварійному відключенні дозволяє відновити більшість, а найчастіше і всю інформацію як збережену, так і не збережену користувачем, у випадку ж так званого «коректного вимикання» навпаки деяка інформація може бути загублена без можливості її відновлення.

Щоб запобігти зазначених і багатьох інших помилок, в процесі проведення слідчих дій, нами рекомендується залучати фахівця в галузі комп'ютерних технологій (програміста, системного аналітика, інженера по засобах зв'язку та мереженому обслуговуванню тощо) на всіх етапах розслідування злочинів, в яких ПК фігурує як елемент об'єктивної сторони злочину. Профіль фахівців визначається, виходячи зі слідчої ситуації, цілей, завдань слідчої дії, а також

---

[1] Загальне знеструмлення може бути рекомендовано у випадках, коли на місці проведення слідчих дій встановлено багато ПК; коли комп'ютери об'єднані в локальну мережу; коли комп'ютер (комп'ютери) обладнані пристроями віддаленого доступу.

комп'ютерної техніки і встановленого на ній програмного забезпечення (операційної системи, прикладних програм).

Вважається також за доцільне запропонувати за можливістю залучати постійний контингент фахівців. Найкращим варіантом вважається залучення одного або декількох спеціалістів на всіх етапах розслідування однієї справи. Багаторазові взаємодії слідчого і фахівця реалізуються як у процесуальній, так і в непроцесуальній формах, а фахівець може виступати як спеціаліст і експерт. Така форма взаємодії, тобто постійний контакт слідчого з одним фахівцем, є найбільш ефективною. Це обумовлюється тим, що, по-перше, слідчий не має необхідності щоразу шукати відповідного фахівця для своєчасного одержання відповідної довідкової інформації; по-друге, фахівець, починаючи з перших консультацій слідчого і закінчуючи складанням висновку КТЕ знайомий з усіма обставинами справи стосовно речових доказів комп'ютерно-технічних засобів, що дозволяє одержати максимальний обсяг доказової та орієнтуючої інформації [7, с.177–183].

Під час підготовки до огляду потрібно вирішити питання про його матеріально-технічне забезпечення. Слідчий і фахівець можуть застосовувати як традиційні техніко-криміналістичні засоби виявлення, попереднього дослідження, вилучення і фіксації слідів, так і спеціальну техніку, спеціальне програмне забезпечення для доступу, зчитування і збереження комп'ютерної інформації. При застосуванні техніко-криміналістичні засобів слід додержуватись загальних правил поводження з обчислювальною технікою і носіями інформації, зокрема потрібно уникати впучення дрібних часток і магнітних порошків на робочі частини комп'ютерів при виявленні відбитків пальців рук, а застосування магнітних шукачів, ультрафіолетового освітлювача, інфрачервоного перетворювача тощо, повинне бути погоджене зі спеціалістом, щоб уникнути руйнування носіїв інформації і мікросхем пам'яті ЕОМ [8, с.81].

Список літератури: 1. Вехов В.Б. Компьютерные преступления: способы осуществления и раскрытия. М., 1996. 2. Касаткин А.В. Тактика собирания и использование компьютерной информации при расследовании преступлений: Дис.... канд. юрид. наук. М., 1997. 3. Крылов В.В. Информационные компьютерные преступления. М., 1997. 4. Селиванов В.А., Дворкин И. Пособие для следователей. М., 1998. 5. Мазепа В. Осиный рой: Всеукраинский еженедельник «Мой компьютер». 2001. №46. 6. Яковлев А.Н. Использование специальных познаний при расследовании «компьютерных» преступлений. Конфидент. 2000. № 6. 7. Коршенко В.А. Взаємодія слідчого з фахівцем під час огляду комп'ютерних засобів та призначенні КТЕ // Актуальні проблеми криміналістики: Матеріали НПК студентів, курсантів і слухачів. Донецьк, 2001. 8. Коршенко В.А. Особливості підготовки матеріалів для проведення комп'ютерно-технічної експертизи// Вісник Наш. ун-ту внутр. справ (спецвипуск). 2001.

Надійшла до редколегії 12.02.02

Т.І. Возна

ДО ПРОБЛЕМИ ПОПЕРЕДЖЕННЯ НАСИЛЬСТВА У СІМ'Ї

Проблема насильства в сім'ї та його попередження є надзвичайно актуальною проблемою для сучасного українського суспільства, оскільки саме родинні стосунки впливають на розвиток чи занепад нації.