Ученые записки Таврического национального университета им. В. И. Вернадского
Серия «Юридические науки». Том 19 (58), № 2. 2006 г. С. 296-296.

УДК 343.98:004.056.53

Пашнєв Д. В.

ВЛАСТИВОСТІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ ТА ОСОБЛИВОСТІ ЗБИРАННЯ КОМП'ЮТЕРНИХ СЛІДІВ

Комп'ютерні сліди являють собою якісні та кількісні зміни комп'ютерної інформації, пов'язані зі злочином. Якісні: зміни вмісту або атрибутів комп'ютерної інформації. Кількісні: зміни відповідно кількості одиниць або розміру одиниць комп'ютерної інформації [1]. Виходячи з цього, існує нерозривний зв'язок комп'ютерної інформації і комп'ютерних слідів. Отже, для повнішого розуміння суті комп'ютерного сліду в цій статті ми звернемося до сутності комп'ютерної інформації, виявимо, як властивості комп'ютерної інформації впливають на властивості комп'ютерних слідів і особливості їх збирання та дослідження.

Розглянемо властивості комп'ютерної інформації як доказу по аналогії з запропонованими С.А.Россовим взагалі щодо інформації в світлі доказування [2]:

1. Фіксованість інформації. Це ключова властивість інформації. Оскільки «інформація є інформація, а не матерія і не енергія» (Н. Вінер) вона мислима тільки в зафіксованому вигляді. Потенційним носієм інформації може бути будь-який феномен оточуючого нас світу, наявність або відсутність якого можна регулювати довільним чином. Далі С.А. Россов, вказує, що „слід відрізняти потенційні носії інформації від її реальних носіїв. Якщо перші можуть містити інформацію, а можуть і не містити, то другі завжди її містять. Власне носієм інформації є речення, що складене тією чи іншою мовою, тобто з використанням системи знаків (звуків, сигналів тощо), що передають інформацію". На нашу думку, важливо додати, що варто розрізняти сигнали, що є тільки засобом передачі інформації, і феномен дійсності, що є саме носієм інформації. Важливу роль тут відіграє фактор часу, адже сигнал існує тільки в певний момент часу і тільки в цей момент він є носієм інформації, потім він зникає передаючи свої властивості більш постійному носієві. У випадку вербальної передачі інформації слова є сигналами, що складаються в речення та існують тільки в момент їх висловлення. Далі ж вони фіксуються в більш постійному носієві – пам'яті людини.

З використанням комп'ютерних технологій інформація може бути зафіксована переведенням її з семантичного вигляду в матеріальний сигнал і записом цього сигналу на фізичний об'єкт за допомогою відповідних програмно-технічних засобів. Таким чином, засобом передачі інформації в комп'ютерних технологіях є матеріальний сигнал, а безпосереднім носієм інформації є феномен дійсності, що виникає внаслідок впливу цього сигналу. Використовуючи новітній термін, можна казати про комп'ютерну технологію передачі та фіксації інформації. Найбільш розповсюдженим зараз є електричний сигнал (носієм є магнітне поле), але розповсюджуються оптичні, радіо- та інші фізичні сигнали та явища. З розвитком біо- та інших технологій з'являться інші носії. Зі всього цього витікають властивості саме комп'ютерної інформації: неможливість вочевидь, без застосування спеціальних знань, визначити наявність інформації на носії, чи є він реальним чи потенційним, скласти сигнали в речення і зрозуміти зміст інформації.

2. Інваріантність інформації по відношенню до її фізичних носіїв. Ця властивість інформації безпосередньо пов'язана з попередньою. Вона означає, що одну і ту ж інформацію, незалежно від її семантики, можна зафіксувати (записати) будь-якою мовою, використовуючи будь-яку систему знаків, що наносяться будь-яким способом на будь-які носії.

В комп'ютерних технологіях обробки інформації ця властивість породжує наявність ймовірності неправильного розуміння змісту комп'ютерної інформації та помилкової її оцінки як доказу.

3. Тлінність інформації. Оскільки кожна дана інформація (точніше, кожний її екземпляр) у будь-якому випадку зафіксована на тому або іншому фізичному носії, збереження і саме існування інформації цілком визначається долею її носія. Поки носій недеформований, зберігається і сама інформація. Відбувається це незалежно від того, використовувалася інформація для яких-небудь цілей чи ні. Деформація носія спричиняє за собою зміну зафіксованої на ньому інформації. При цьому вона перекручується або руйнується – зникає. Образно кажучи, інформація гине разом зі своїми носіями.

Відносно комп'ютерного носія інформації вважаємо потрібним додати, що інформація на ньому може бути знищена і без його пошкодження під впливом явищ, які знищують сам феномен дійсності, що є носієм інформації. Наприклад, сильне магнітне поле може знищити інформацію на магнітному носії інформації, але сам носій при подальшому форматуванні зберігає можливість зберігати інформацію. Крім того, при використанні програмних засобів інформацію можна просто перекрутити аж до втрати нею первинного змісту, що також можна вважати її втратою. Таким чином, щодо комп'ютерної інформації властивість тлінності зростає, адже можливостей її знищити виявляється більше. Але наряду з цим, варто відмітити, що існує більше можливостей відновлення інформації на комп'ютерному носії. Поки що вони недоступні рядовому спеціалісту через велику кількість технологічних затрат, але вони існують і досить ефективні.

4. Трансльованість, розмножуваність і мультиплікативність інформації. Згубних наслідків, пов'язаних з проявами тлінності інформації, дозволяють уникнути деякі інші її властивості. Трансльованість — можливість бути переданою з одного носія на інший тієї ж або іншої фізичної природи, в тій же або іншій системі запису. Якщо швидкість трансльованості перевершує швидкість руйнування і загибелі інформації, остання розмножується. Звідси наступна властивість — мультиплікативність інформації (можливість одночасного існування однієї і тієї ж інформації у вигляді ідентичних копій на однакових або різних носіях).

Якщо перші дві властивості інформації працювали так би мовити проти використання її як доказу, то ця властивість - навпаки. Тим більше, комп'ютерні технології створили можливість необмеженого копіювання (розмножування) інформації без втрати будь яких її властивостей і зміни змісту. А отже відносно комп'ютерної інформації можливо практично зі 100 % вірогідністю уникнути згубних наслідків прояву перших властивостей інформації, якщо правильно використовувати розмножуваність комп'ютерної інформації.

5. Мінливість інформації. Під змінами інформації прийнято розуміти такі її зміни, які (на відміну від її руйнування і зникнення) хоча і зачіпають її кількість і семантику, але не позбавляють її значення.

Комп'ютерні технології дозволяють в короткі строки змінити інформацію на іншу:

1. без присутності на місті знаходження носія (з віддаленого доступу);

2. за допомогою спеціально створеної програми, тобто навіть зовсім без участі людини.
3. Ці властивості вказують на наступні особливості збирання та дослідження комп'ютерних слідів.

А. Негативні:

1. Виключна необхідність застосування спеціальних знань.
2. Відповідність науково-технічних засобів збирання та дослідження комп'ютерних слідів деяким спеціальним вимогам.
3. Необхідність скорочення до мінімуму проміжку часу між вчиненням злочину (виникненням слідів) та моментом їх збирання.

Б. Позитивні:

Можливість необмеженого у кількості копіювання комп'ютерної інформації без втрати змісту і властивостей.

Наявність доволі ефективних способів відновлення втраченої комп'ютерної інформації.

У зв'язку з цими особливостями збирання та дослідження комп'ютерних слідів хотілося б звернути увагу на наступну проблему. Іноді носії комп'ютерної інформації вилучити в натурі неможливо. Це в основному відноситься до вінчестерів (жорстких магнітних дисків), які є головним носієм інформації окремої ЕОМ. Це найчастіше пов'язано з економічними причинами. Наприклад, у разі виходу з ладу ЕОМ банк, як правило, може пропрацювати без шкоди для себе не більше двох днів, оптова фірма – 3-5, промислова компанія – 4-8, страхова компанія – 5-6 днів [3]. У зв'язку з цим радикальне вилучення комп'ютерної техніки загрожує подальшими претензіями потерпілих організацій. Проведення ж експертизи прямо на місці знаходження засобів комп'ютерних технологій також іноді неможливе у зв'язку з наступними причинами:

- при цьому засіб комп'ютерних технологій, що є об'єктом дослідження, повинен бути відімкнений від мережі і весь час експертизи не працюватиме в системі;
- на режимних об'єктах, якими найчастіше і є приміщення з комп'ютерною технікою, присутність сторонніх осіб, якими є експерт та інші присутні при експертизі особи, суворо обмежується;
- під час проведення експертизи може бути виявлена активна протидія з боку заінтересованих осіб.

В цьому випадку у зв'язку з можливістю розмноження комп'ютерної інформації без втрати властивостей робиться повна дзеркальна (покластерна) копія (образ) носія з використанням спеціальних засобів. Але іноді виникають ситуації, при яких і копію неможливо зробити, адже є підприємства, установи, організації з безперервним циклом роботи, і вимкнення хоча б однієї робочої станції може призвести до значних збитків, а наявні засоби не забезпечують копіювання при увімкненому комп'ютері. Прикладом може слугувати кримінальна справа відносно посадових осіб Кримської регіональної митниці. Було встановлено, що в певний період співробітники пункту пропуску «Феодосійський морський порт» ТП «Феодосія», використовуючи комп'ютерну техніку, увійшли до електронної автоматичної інформаційної системи ДМС України і дали помилкові підтвердження про те, що вантаж цукру покинув митну територію України. При огляді терміналу, з якого ймовірно були вчинені ці дії, спеціаліст стикнувся з вказаними проблемами. Єдиним виходом було виявлення в ході слідчої дії – виїмки – необхідної для експертизи інформації та проведення дослідження в лабораторних умовах вже саме

її. Що було успішно зроблено і стало запорукою успішного закінчення розслідування злочину.

З приводу допустимості таких дій наведемо наступні міркування. Відносно документів є поняття оригінал, дублікат, копія. Ці поняття, на наш погляд, можна перенести і на комп'ютерні носії інформації. Під час фіксації носіїв, що не можуть бути вилучені в натурі, робиться дублікат носія, ідентичність якого оригіналу забезпечується застосуванням спеціальних засобів. З нього при подальших дослідженнях робляться копії, які і досліджуються. Можлива кількість разів такого копіювання відносно необмежена, а тому і досліджувати комп'ютерну інформацію, що міститься на оригінальному носії можна необмежену кількість разів навіть руйнуючими методами без ризику втрати важливої інформації на оригіналі.

Але у зв'язку з цим М.Г. Щербаковський ставить справедливе питання: яке доказове значення копій комп'ютерної інформації, одержаних спеціалістом, до якого виду доказів вони можуть бути віднесені, чи є вони первинними чи похідними речовими доказами. На його думку неочевидність процедури копіювання і копійованої інформації, можливість навіть помилково або з недосвідченості спеціаліста внести в копію зміни, відсутні в оригіналі, дають мотив взагалі засумніватися в залученні копій як доказів [4].

Що стосується первинних та похідних доказів - чи є значення і взагалі чи можна говорити по відношенню до комп'ютерної інформації про такий поділ?

Комп'ютерна інформація представлена на трьох рівнях (фізичному, логічному та семантичному – загальнозрозумілому), на кожному з них представлена одна і та ж інформація (краще сказати відомості), але в різних видах представлення [5, с. 55]. Чи можна вважати процес отримання загальнозрозумілої форми представлення з фізичної отриманням похідного доказу? На думку автора, можна, якщо прийняти логічний рівень представлення опосередковуючою ланкою, тими «другими руками», про які завжди йдеться при поясненні суті похідних доказів.

Проте що тоді буде первинним доказом? Фізичний рівень представлення комп'ютерної інформації? І що повинні зробити суб'єкти доказування, щоб оцінити ці первинні докази? І взагалі чи можна говорити про отримання похідних доказів або просто про перекодування сигналу?

На нашу думку, говорити про отримання похідних доказів можна при здійсненні огляду носіїв комп'ютерної інформації поза рамками експертизи. Про перекодування сигналу можна говорити при здійсненні експертного дослідження.

У першому випадку інформація знаходиться на носії вже у загальнозрозумілій формі. Це може бути звичайна інформація, зрозуміла неспеціалісту (текст, символи, зображення), або спеціальна інформація (файли настройок, журналів, звітів програм тощо), зрозуміла особі, що володіє спеціальними знаннями. В другому – це захищена або зашифрована інформація, окремий випадок – програма, яка представлена в машинних кодах (при перекодуванні у вихідний код для вивчення функцій).

По цій ознаці можна розділити дії, які можна проводити на місці огляду, і лише ті які здійснюються при експертизі.

Що ж стосується визнання копії як доказу, то сучасні спеціальні програмно-технічні засоби [6] дозволяють створити повний образ-дублікат початкового носія, що вміщує не тільки область даних, але і всі інші області носія, включаючи ділянки видалених даних і вільний простір носія [7] - покластерну копію (образ). Створення

копії і робота з копією рекомендується для безпеки досліджень, щоб не пошкодити висхідний матеріал через можливі помилки з невідомими програмами або пастки, встановлені власником даних. Крім того, вище доведена крайня необхідність такого копіювання в деяких випадках. Сумніви ж у тотожності копії та оригіналу можуть бути відкинуті при необхідності за допомогою алгоритму MD5: md5sum – це вільно доступна утиліта для порівняння оригінального диска і копії, що може використовуватися в комп'ютерному експертному дослідженні для доказу, що зроблений образ є точною копією оригіналу [8].

Більшість опитаних автором експертів визнають допустимим покластерне або побітне копіювання вінчестера комп'ютера при слідчому огляді для експертного дослідження копії.

Отже можливістю повного копіювання необмежену кількість разів комп'ютерної інформації, навіть видаленої, знімається проблема, що обмежує дії спеціаліста при проведенні слідчих дій у комп′ютерних злочинах – необхідність збереження комп′ютерної інформації в оригіналі.

З цього можна зробити висновок, що допомога спеціаліста при проведенні слідчих дій при розслідуванні комп'ютерних злочинів не повинна обмежуватися тільки виявленням, фіксацією та вилученням потенційних носіїв комп'ютерних слідів злочину. При необхідності слідчий в ході слідчої дії має право доручити спеціалісту зібрати сліди саме в комп'ютерній інформації на виявлених носіях із занесенням в протокол всіх відомостей про це. І при цьому слідчий та спеціаліст, як ми вже з'ясували, будуть діяти в рамках діючих процесуальних вимог.

Література:

1. Пашнєв Д.В. Поняття та сутність комп'ютерних слідів. // Актуальні проблеми сучасної науки в дослідженнях молодих учених. – Сімферополь. 2006. – Вип. 9. - с. 74-77.
2. Россов С.А. Информация и судебные доказательства. // Российский следователь. - № 3. – 2004. – с. 39-40.
3. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной информации. // Законность. – 1999. - №3. – с. 12-15.
4. Щербаковський М.Г. Формы применения специальных знаний при исследовании компьютерных средств на месте проведения следственных действий. //
5. Толеубекова Б.Х. Криминалистическая характеристика компьютерных преступлений (по материалам зарубежной печати). - Караганда: ВШ МВД РК, 1993. - с.55.
6. Пашнєв Д.В. Спеціальні засоби збирання та дослідження слідів злочинів, вчинених з використанням комп'ютерних технологій. // Вісник Луганської академії внутрішніх справ. - 2005. – Спецвипуск. – с. 137-139.
7. Комиссаров В., Гаврилов М., Иванов А. Назначение компьютерно-технических экспертиз. // Законность. – 2000. – №1. – с. 31-33.
8. Михаил Разумов. Компьютерная экспертиза на платформах Windows, часть 2 - http://securitylab.ru/default.asp?ID=36707.

Пост упила в редакцию: 02.11.2006 г.