КРИМІНАЛІСТИЧНА ТЕХНІКА ТА МЕТОДИКА

УДК 621.3

М.М. Зацеркляний,
доктор технічних наук, професор
О.В. Струкова

СЛІДОУТВОРЕННЯ В ІНФОРМАЦІЙНИХ КОМПОНЕНТАХ КОМП'ЮТЕРНИХ СИСТЕМ

Авторами досліджується природа слідів в інформаційному середовищі комп'ютерних систем. Розглядаються деякі властивості комп'ютерних пристроїв та особливості процесів перетворення інформації в комп'ютерних системах, що зумовлюють "віртуальність" слідів, які утворюються в інформаційному середовищі комп'ютерних систем.

Ключові слова: *інформація, криміналістика, слід, програма, віртуальне середовище.*

Авторами исследуется природа следов в информационной среде компьютерных систем. Рассматриваются некоторые свойства компьютерных устройств и особенности процессов преобразования информации в компьютерных системах, обуславливающие "виртуальность" следов, образующихся в информационной среде компьютерных систем.

Ключевые слова: *информация, криминалистика, след, программа, виртуальная среда, виртуальный след.*

The authors investigate the traces' nature in the information environment of computer systems. Several properties of computer devices as well as some features of the information transforming processes in computer systems are considered, that causes the "virtual" nature of traces, formed in the environment of computer information systems.

Keywords: *information, criminalistics, track, program, virtual environment, virtual track.*

Існуюча в криміналістиці традиційна класифікація слідів скоєння тих чи інших злочинів практично не охоплює ті її види, які виникли при появі нових видів злочинів. Важливу роль у цьому відіграють способи вчинення злочинів у сфері інформаційних технологій, кількість яких постійно збільшується.

Виділення комп'ютерних злочинів в окрему групу передбачає активізацію пошуку, спрямованого на дослідження раніше невідомих криміналістиці і теорії оперативно-розшукової діяльності слідів. Цілісне уявлення про слідові картини, що виникають при приготуванні, здійсненні, приховуванні комп'ютерних злочинів, дозволяє розробляти і впроваджувати нові методи, або запозичувати їх із суміжних областей діяльності (наприклад, діяльності із забезпечення комп'ютерної безпеки). Відкриваються також перспективи вдосконалення основних положень тактики використання спеціальних знань для виявлення, фіксації, вилучення і дослідження слідів

комп'ютерних злочинів при провадженні слідчих дій та проведенні оперативно-розшукових заходів.

В науках кримінально-процесуального циклу термін "слід" вживається в двох значеннях – процесуальному і криміналістичному [1]. Процесуальне значення сліду полягає в тому, що інформація, одержана за його допомогою, використовується для формування доказової бази з кримінальної справи і знаходить своє відображення у процесуальних документах. Криміналістичне розуміння сліду більш широке і охоплює всю сукупність одержуваної інформації, яка використовується для розшукових дій, висунення пошукових та інших версій, визначення напрямку дій слідчого.

Розглянемо природу слідів в інформаційному середовищі комп'ютерних систем. Безсумнівно, вона матеріальна, оскільки дані, які є безпосереднім об'єктом криміналістичного дослідження, завжди мають матеріальну основу. Основою технології обробки комп'ютерної інформації є властивість комп'ютерних систем зчитувати інформацію з матеріальних носіїв і перетворювати її у цифрову форму. Слідоутворюючим об'єктом у цих умовах є виконавчий елемент пристрою запису, слідосприймаючим – досліджуваний носій інформації [2].

Інформація в комп'ютерні системи передається та обробляється шляхом електромагнітної взаємодії. Електромагнітне поле, як особливий вид матерії, звичайно ж, залишає фізичні сліди, але цей факт може бути корисним тільки в ситуаціях з магнітними та оптичними змінними носіями, ера яких закінчується. Найбільш численним класом знімних носіїв сьогодні стають електронні флешкарти, втім, сукупність їх ознак носить досить бідний трасологічний характер. Тому система матеріальних слідоутворюючих і слідосприймаючих об'єктів може виступати як об'єкт аналізу щодо обставин впливу на комп'ютерну інформацію досить рідко. Крім того, інформаційні сигнали в процесі передачі від одного комп'ютерного пристрою до іншого контролюються на цілісність і в разі необхідності коректуються, тобто здійснюється регенерація переданих даних, а не проста трансляція від одного вузла до іншого. Отже, процес слідоутворення в ході інформаційних процесів побудований таким чином, аби знищувати в слідах будь-які фізичні особливості передавального пристрою, які можуть вплинути на цілісність переданої інформації.

Комп'ютерним пристроям пам'яті притаманна важлива властивість – зберігати комп'ютерну інформацію у вигляді, характерному саме для цього пристрою, повністю зберігаючи її семантику. Отже, суто трасологічні ознаки, в традиційному розумінні цього слова, як основа слідоутворення в комп'ютерних системах криміналіста цікавити не можуть. Аналіз взаєморозташування елементарних одиниць інформації, звичайно, дозволяє розшифрувати зміст повідомлення, але такий шлях не може бути визнаний ефективним і необхідним. Адже для того, аби передати людині семантику повідомлення, зафіксована на комп'ютерному носії інформація повинна пройти ряд перетворень, абсолютно звичайних для інформаційних систем. При цьому вона поступово перетворюється у більш загальні структури: від біта – до байту, від байта – до блоку, від блоку – до файлу, від файлу – до форматованого запису і від запису – відповідним поданням на пристрій виведення. Все це виконує комп'ютерна система без участі людини (за винятком вольового початкового впливу). В результаті, дослідник одержує інформацію не в тому вигляді, в якому вона існує на слідосприймаючому об'єкті, і не може судити про фізичні властивості слідоутворюючого об'єкта.

Враховуючи це, сліди, що утворюються в інформаційному середовищі комп'ютерних систем в ході інформаційних процесів, можна назвати віртуальними, оскільки вони є перетвореними, тобто спостережуваними не в тому вигляді, в якому існують. Крім того, починаючи з етапу семантичного визначення стає можливою участь у перетворенні даних людиною (звичайним користувачем).

"Віртуальність" слідів у комп'ютерній системі зумовлена ще однією причиною. Сам процес зміни стану носія інформації пов'язаний із функціонуванням конкретного програмного забезпечення комп'ютерної системи. Отже, сліди залежать від того, які програми працювали в комп'ютерній системі на момент розслідуваної події. Тому, якщо при одній і тій же події використовувалися різні програми, то і сліди ці будуть різними.

Внаслідок цього можна зробити висновок, що основою процесу слідоутворення в комп'ютерній системі та головним слідоутворюючим фактором є сукупність взаємодіючих програм і їх налаштувань, що існували на момент скоєння розслідуваної події. Будь-яка програма залишає сліди тільки тоді, коли вона знаходиться в активному стані, тобто виконується в оперативній пам'яті комп'ютера. Адже тільки в процесі виконання програми проявляються її властивості, які знаходять своє відображення в її ознаках, а надалі – в слідах. З іншого боку, не можна сказати, що програма, яка знаходиться в неактивному стані, не має жодних ознак програми, що виконується в пам'яті, адже вона містить той же програмний код. А отже, програма може вважатися слідоутворюючим об'єктом, незалежно від того, в якому стані вона знаходиться.

Усі комп'ютерні дані, які можуть бути слідами, містяться на носіях пристроїв комп'ютерної пам'яті. Варто вказати, що серед існуючих видів пам'яті - оперативна, зовнішня і постійна – лише зовнішня може вважатися основним об'єктом уваги криміналіста, оскільки в оперативній пам'яті дані знищуються відразу після вимкнення живлення (виняток становлять пристрої пам'яті комп'ютерних пристроїв, які мають мобільні джерела живлення – КПК, смартфони, стільникові телефони тощо), а постійна пам'ять доступна лише для зчитування.

Носії пристроїв зовнішньої пам'яті характеризуються тим, що мають особливу логічну організацію, яка називається файловою системою. Саме файлова система визначає, як одна і та ж програма запише дані на накопичувач. На цій підставі можна вважати, що слідосприймаючим об'єктом в інформаційному середовищі комп'ютерної системи є файлова система. Крім цього, до факторів, що впливають на формування слідів у файловій системі, належать:

– інші програми, присутні в оперативній пам'яті, які є активними (які одержали управління) і які взаємодіють із тією, що здійснює запис;

– дані, розташовані у зовнішній пам'яті, які можуть використовуватись цією програмою для повноцінного функціонування.

Таким чином, важливим, а може і найважливішим з точки зору можливості ідентифікації слідоутворюючим фактором є інформаційне середовище комп'ютерної системи в цілому: активні програми і дані, попередньо зчитані слідоутворюючою програмою. Це інформаційне середовище можна вважати середовищем слідоутворення.

Фізичні особливості носіїв інформації не можуть відіграти скільки-небудь помітної ролі в процесах слідоутворення в інформаційному середовищі комп'ютерних систем. Сама по собі інформація не може мати тих ознак, які б відрізняли одне повідомлення від іншого, якщо ці повідомлення мають абсолютно однакову

синтаксичну структуру. Тому, відриваючись від несуттєвих фізичних особливостей носіїв інформації, ми не можемо замикатися тільки на особливостях синтаксичної будови об'єкта слідчих інтересів, оскільки в цих рамках в інформаційному середовищі можлива наявність множини абсолютно однакових об'єктів. Таким чином, порушується одна з філософських основ криміналістичної ідентифікації – неповторність матеріальних об'єктів. Інформаційні об'єкти – це синтаксичні структури, які містять одне і те ж повідомлення, можуть бути абсолютно однаковими, і тому на їх основі не можна робити диференціацію фізичних об'єктів – носіїв інформації. Внаслідок цього необхідно вийти за рамки дослідження системи "повідомлення – синтаксична структура" та включити сюди спосіб зберігання даних.

Теорія інформації говорить про те, що в понятті інформації доцільно розрізняти ядро повідомлення (смисловий зміст) і атрибутику (як цей зміст подається). Оскільки важливою властивістю інформації є атрибутивність, тобто неможливість існування інформації без носія з одного боку і обов'язкове кодування з іншого, то всяке повідомлення супроводжує щось, що характерно саме для джерела цього повідомлення. Відповідно до даної теорії, будь-яке повідомлення "незримо пов'язане" з іншими відомостями, які можуть бути ідентифікаційними ознаками, що вказують на джерело інформації. Отже, слід у комп'ютерній системі несе ознаки програмного середовища, яке існувало на момент процесу слідоутворення, і тієї програми, яка цей слід залишила. У сукупності ці ознаки в достатній кількості повинні утворювати ідентифікаційне поле. Таким чином, можна говорити про те, що атрибутивна складова будь-якої інформаційної структури в інформаційному середовищі комп'ютерних систем несе відомості про події, які відбувалися на момент створення (зміни) цієї структури.

Інформаційне середовище кожної комп'ютерної системи є унікальним. Тому і сліди в їх файлових системах будуть формуватися на основі унікальних факторів і самі будуть унікальними. Це зумовлює можливість ідентифікації інформаційного середовища комп'ютерної системи. Апаратне забезпечення комп'ютера пов'язане з його інформаційним середовищем на основі логічних імен або ідентифікаторів. Ці імена або ідентифікатори пов'язані з властивостями відповідних апаратних об'єктів мати власне інформаційне середовище – пам'ять, в якій записані деякі дані, і які можуть бути одержані основним середовищем комп'ютерної системи і зафіксовані в його пам'яті. За цими даними можна відновити прив'язку інформаційного середовища до апаратного і, отже, ідентифікувати комп'ютер в цілому. Це можливо, звичайно, за умови, що однотипні апаратні пристрої мають унікальне власне інформаційне середовище.

Розглянемо, що є атрибутикою інформації, яка міститься на комп'ютерному носії. Програми здатні інтерпретувати дані тільки тоді, коли ці дані подаються у встановлених для цих програм форматах. Формат даних є описом правил декодування деякої сукупності даних. Сучасні складні форми подання даних не можуть бути реалізовані на комп'ютерній техніці без додаткової (службової) інформації. Службова інформація забезпечує можливість розпізнавання і інтерпретацію програмами корисної інформації, яка для них завжди є даними. Ця інформація виникає поза волею суб'єкта внаслідок "природних" властивостей слідоутворюючого і слідосприймаючого об'єктів. У комп'ютерних системах ці властивості визначені розробниками програмного середовища, в якому відбувається обробка інформації користувачів. У сучасних системах, націлених на автоматичну обробку інформації, практично будь-яка корисна інформація супроводжується службовою. Ряд

програмних продуктів з різних причин змушені стежити за своїм станом для його відновлення після деактивації, адже при вимкненні комп'ютера інформація з оперативної пам'яті втрачається, та створювати додаткові інформаційні об'єкти в зовнішній пам'яті для подальшого коректного відновлення своєї роботи.

Треба сказати, що виникнення категорій "службова інформація для корисних даних" та "службова інформація для програм" з точки зору розвитку інформаційних систем є цілком об'єктивним процесом, спрямованим на збільшення міри автоматизації процесів обробки інформації та позбавлення користувача від необхідності витрачати час на узгодження наявної і знову виниклої інформації. Варто зауважити, що цей процес реалізується кожним розробником суб'єктивно. Розробники, в свою чергу, користуються готовими модулями – бібліотеками підпрограм, які прискорюють розробку їх власних програмних продуктів. Ці бібліотеки є ще одним об'єктивним фактором, який значною мірою обмежує суб'єктивізм розробника і дозволяє об'єктивно існувати вище розглянутим ознакам інформаційних об'єктів.

Службова інформація виникає незалежно від бажання суб'єкта діяння на основі обставин, які передбачені розробником програмного забезпечення і які пов'язані певними рамками вимог нижчестоящих програм. Службова інформація – це те, з чим працює криміналіст, оскільки корисна інформація повністю контролюється суб'єктом – користувачем. Тут доречна аналогія: текст листа – прояв волі суб'єкта, а почерк автора в основному є проявом об'єктивних обставин, які не залежать від волі суб'єкта. Вміст листа – предмет дослідження слідчого, почерк – криміналіста. В результаті їх спільної роботи встановлюється зв'язок між волею суб'єкта, викладеної в тексті листа, і самим суб'єктом, тобто, проводиться криміналістична ідентифікація.

Оскільки в ході інформаційних процесів відбувається доповнення корисної інформації службовою, тобто відбувається фіксація прояву властивостей програми і стану активного програмного середовища комп'ютера в цілому у файловій системі, то наявність службової інформації є ознакою роботи цього програмного комплексу, а область файлової системи разом із службовою інформацією – слідом. Ґрунтуючись на цьому роді ознак, програма розпізнає смислову інформацію в повідомленні, а криміналіст може судити про те, які класи програм брали участь у створенні корисної інформації і, можливо, які дії здійснювалися над нею.

Отже, цікава в криміналістичному розумінні властивість програми полягає у відтворенні налаштованої і формування відповідної службової інформації. Ознака роботи програми – це наявність відтвореного конкретного типу службової інформації. Слід – це вміст конкретної області у файловій системі (вільні кластери; кластери, зайняті під файли і каталоги; області кластера, не зайняті інформацією файлу, під який він розподілений).

Програмне середовище конкретного комп'ютера має властивість фіксувати свій стан зі службовою метою та зберігати для користувача інформацію у зовнішній пам'яті. Відповідні ознаки детермінуються складом програмної середовища, що забезпечує цю властивість. Тобто, кожний компонент програмного середовища комп'ютера забезпечує деяку його ознаку, за достатньою сукупностю яких його можна ідентифікувати. Таким чином, ідентифікації підлягає не вміст файлу, а програмне середовище комп'ютера в цілому, як певний об'єкт, що набуває індивідуалізуючих його ознак у процесі функціонування. Враховуючи, що для кожного компонента програмного середовища комп'ютера, як слідоутворюючого

фактора, існує відповідна характерна слідосприймаюча область файлової системи, ми можемо дати означення сліду в інформаційному середовищі комп'ютерної системи. *Слідом у комп'ютерних інформаційних системах є результат взаємодії об'єктів інформаційного середовища (програм і елементів файлової системи), який вказує на зміну стану складових інформаційної системи в результаті функціонування в ній програмних продуктів.*

Ідентифікація комп'ютерного інформаційного середовища можлива не тільки на локальному комп'ютері, а й на комп'ютері, логічно ввімкненому у мережу. Додатковим джерелом слідів у такій системі є програми мережевого забезпечення.

Таким чином, вплив в інформаційній системі може здійснюватися різними програмами, які можуть бути ініційовані іншими програмами і т.д., але на початку цього ланцюга знаходиться користувач, який, маючи цілком конкретну мету, справив початковий вплив на інформаційну систему. Варто зауважити, що, говорячи "інформаційна система", ми маємо на увазі будь-яку комп'ютерну систему, що є частиною всього існуючого на даний момент кіберпростору. Це необхідно підкреслити, оскільки поширення вірусу зі змінного носія може бути зумовлено не лише прямим умислом його розробника, а й ненавмисними діями власника цього носія, який може і не знати про його інфекованість. Отже, кіберпростір дозволяє використовувати комп'ютери жертв як знаряддя злочину.

Визначимо основні критерії класифікації слідів у комп'ютерних системах.

При реалізації інформаційних процесів цілком визначені об'єкти активного програмного забезпечення комп'ютерної системи залишають цілком визначені сліди, тобто конкретну інформацію в строго визначених областях файлової системи. Отже, сліди можна класифікувати за типом програмного забезпечення, яке їх залишає:

1. Сліди, залишені штатними програмними засобами:

– системні програми (компоненти і служби операційної системи (наприклад, для операційної системи Windows, служби управління об'єктами, журналювання, мережевого трафіку і маршрутизації, антивірусного захисту, файловою системою, тощо); інсталятори; драйвери реальних пристроїв і їх емулятори; сервери; утиліти обслуговування; мережеві сканери; програми шифрування тощо);

– прикладні програми (редактори; мережеві клієнти; прикладні компоненти СУБД; конструктори; програми-перекладачі тощо);

– інструментальне програмне забезпечення (транслятори і компілятори; конвертори, налагоджувачі і трасери; дизассемблери; шістнадцятирічні редактори тощо);

2. Сліди, залишені шкідливими програмами, чиїм об'єктом впливу є файлова система, оперативна пам'ять, конкретні файли, мережевий інтерфейс.

Іншою криміналістично виправданою підставою класифікації є розташування слідів на носії у термінах структур файлової системи за їх ієрархією:

1. Сліди в кластерах (розподілених під актуальні файли, розподілених під вилучені файли, зарезервованих, втрачених, в зазорах кластерів);

2. Сліди в керуючих і описуючих структурах файлової системи (таблиці розділів, завантажувальних секторах, резервних областях, областях свопінгу, таблицях розміщення файлів, каталогах);

3. Сліди в файлах:

– виконуваних модулях (компілятора; побудовника завдань (що використовує бібліотеки для конкретної операційної системи); програмного забезпечення,

використовуваного для редагування вже створених виконуваних модулів (зміна кількості і змісту програмних секцій, зміна точок входу, додавання і модифікація коду));

– даних (ініціюючих початковий стан програми (налаштування); які є реєстраційними даними роботи програм (журнали); службових для організації призначеного для користувача інтерфейсу (файли-посилання); службових для організації програмного інтерфейсу (файли-канали, файли свопінгу і спулінгу); що містять документи користувачів; що містять системні таблиці тощо);

4) Сліди у позакластерних структурах (на ділянках накопичувача, не розподілених під розділи і не описаних у поточній таблиці розділів).

На завершення зауважимо, що сліди інформаційних подій і процесів залишаються і на телекомунікаційних елементах комп'ютерних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аверьянова Т.В. Криминалистика : учеб. для вузов / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская ; под ред. Р.С. Белкина. – М. : НОРМА, 2001.

2. *Вехов В.Б.* Компьютерные преступления : способы совершения и раскрытия / В.Б. Вехов ; под ред. акад. Б.П. Смагоринского. – М. : Право и закон, 1996.

Отримано 23.05.2013