Рог Вікторія Євгенівна
викладач кафедри інформаційної безпеки факультету № 4 Харківського національного університету внутрішніх справ.

НАСЛІДКИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОМП'ЮТЕРНИХ СИСТЕМ

У теперішній час відкриття науковців і винаходи учених, інженерів наближають суспільство до якісно нового етапу розвитку, коли інформаційні послуги визначатимуть і забезпечуватимуть основу його існування. Глобальні інформаційні мережі і системи є технологічною основою міжнародного інформаційного обміну. Сьогодні інформаційні ресурси представляють величезну матеріальну та соціальну цінність, а несанкціонований доступ до цих ресурсів, якщо вони недостатньо захищені, може призвести до глобальних катастроф або, в умовах конкуренції, може радикально змінити ситуацію на користь того, хто здійснив такий доступ.

Слід зазначити, що не існує загальноприйнятого визначення кіберзлочинності. Існуюча в криміналістиці традиційна класифікація слідів скоєння злочинів практично не охоплює ті їх види, які виникли при появі кіберзлочинності. Основою для класифікації наслідків кіберзлочинів мають стати способи вчинення цих злочинів, різноманіття яких постійно збільшується.

До кіберзлочинів може бути віднесене будь-який злочин, здійснений в електронному середовищі. Злочин, здійснений в кіберпросторі, - це протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні дії, здійснені за допомогою комп'ютерів, комп'ютерних мереж і програм.

Основним завданням кіберполіції стануть реалізація державної політики усфері протидії кіберзлочинності, зокрема – у сфері використання платіжних систем, електронної комерції та господарської діяльності, а також інтелектуальної властивості та інформаційної безпеки.[1]

Основою будь-якого досудового провадження при розслідуванні злочинів у комп'ютерній сфері є криміналістичне дослідження процесу слідоутворення. Важливим питанням у цій області є питання про природу слідів у комп'ютерній системі, і ряд пов’язаних із ним запитань, зокрема: що є об'єктами взаємодії в комп'ютерних системах; які властивості притаманні цим об'єктам; які їх ознаки знаходять своє відображення у слідах, пов'язаних із подією злочину.

Безсумнівно, природа слідів у комп'ютерній системі - матеріальна, оскільки дані, які є безпосереднім об'єктом криміналістичного дослідження, мають матеріальну основу.

Втім, для встановлення ознак слідоутворюючого об'єкта чи процесу цього недостатньо. Адже інформація в комп'ютерні системи передається та обробляється шляхом електромагнітної взаємодії. Враховуючи досить бідний арсенал трасологічних ознак на електронних носіях інформації, можна стверджувати, що система матеріальних слідоутворюючих і слідосприймаючих об'єктів може виступати як об'єкт аналізу щодо обставин впливу на комп'ютерну інформацію в досить незначній кількості ситуацій. 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 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. Проте, такий шлях не може бути ефективним. Адже для того, аби передати людині семантику повідомлення, інформація, зафіксована на комп'ютерному носії, повинна пройти ряд перетворень, абсолютно звичайних для інформаційних систем. Інформація, зафіксованої на комп'ютерному носії, поступово перетворюється у більш загальні структури: від біта - до запису у відповідному форматі, який подається 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'язан із функціонуванням конкретного програмного забезпечення. 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 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. Оскільки програма залишає сліди тільки тоді, коли вона знаходиться в активному стані, тобто виконується в оперативній пам'яті комп'ютера, а виконання програми є деяким процесом, то програма є слідоутворюючим процесом. 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. З цієї точки зору програма, як файл, є слідоутворюючим об'єктом.

Усі комп'ютерні дані, які можуть бути слідами, містяться на комп’ютерних носіях 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 при вимкненні 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.

Пристрої 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.

Висновок. Криміналістичне дослідження програмного забезпечення як слідоутворюючого об’єкта та файлової системи комп’ютера як слідосприймаючого об’єкта є перспективним напрямом розвитку трасологічних експертиз при розслідуванні кіберзлочинів.

Список бібліографічних посилань:

1. Сезонова І.К. Інформаційна безпека в сучасних умовах/ Сезонова І.К.// Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали IV Міжнародної науково-практичної конференції – Харків, 2015. – С.412-415.
2. Тропина Т.Л. Киберпреступность. Понятие, состояние, уголовно-правовые меры борьбы : монография. – Владивосток, 2009. – 237 с.