## 3.5. Інноваційні підходи до встановлення причинності в комп'ютерно-технічній експертизі

Інтенсивне використання комп'ютерних технологій правопорушниками, застосування знань комп'ютерних наук до вдосконалення способів злочинів різних видів ускладнює виявлення електронних слідів, викриття злочинців, розкриття і розслідування протиправних діянь. В силу цього в даний час в практиці кримінального судочинства гостро затребувані рекомендації криміналістики і судової експертизи з дослідження комп'ютерної техніки, електронного середовища слідоутворення, різних електронних слідосприймаючих і слідоутворюючих об'єктів, механізму формування електронних слідів. У розглянутій спеціальній сфері слідоутворення однією з загальних для криміналістичних та експертних знань основ є положення про причинність, що передбачають вивчення зв'язку між причиною (діями особи або комп'ютерної програми) і наслідком (утворених на електронному носії комп'ютера слідами).

У експертному та криміналістичному дослідженні комп'ютерної техніки під причиною в найбільш загальних рисах

[1] Див.: Про судову експертизу. Закон України. / Законодавство України. – [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/4038-12.

пропонується розуміти таку, що відбувається в штучному (технічному) середовищі подію впровадження з певного джерела функцією деякої програми змін в існуючий стан справ на електронному носії. Із зазначеного випливає, що причина є динамічною подією, в якій бере участь і взаємодіє причинний комплекс об'єктів. Невід'ємною характеристикою причини також є і внесення змін в стан справ з певного джерела на основі активності функції деякої програми. Змістовно таке джерело змін може бути об'єктним або суб'єктним.

Суб'єктне джерело причинності направляє пізнання на зміни, впроваджені дією особи і розглядає дану особу (підозрюваного, потерпілого, свідка-очевидця) в якості причинного агента, що починає при реалізації механізму злочину причинний ланцюг або причинний мережу подій. Прояви активованих зусиллям, поведінкою людини функцій (в тому числі недокументованих) програмного забезпечення призводять до взаємодії компонентів події-причини, об'єднання їх в криміналістичний причинний комплекс і до формування ряду ознак в утворених електронних слідах. Такий контекст у зв'язку з дієвою, агентською роллю особи можна умовно назвати суб'єктною причинністю.

Електронне слідоутворення відбувається в умовах програмного середовища, в якій взаємодія людини і носія сліду завжди здійснюється із застосуванням інструментарію, а саме – певного програмного забезпечення. Знання ознак проявів функціональних можливостей програмного забезпечення використовується при зворотному причинному аналізі виявлених електронних слідів, тому в якості кінцевого результату експертне дослідження причинності може вказувати на специфічні ознаки функції програми, застосованої особою при вчиненні дій, або на обліковий запис користувача, що застосував дану програму, або на інший компонент події-причини, але не на саму особу, як біологічний індивід[1]. При цьому формується інструментальна суб'єктна

[1] Примітка : Результати біометричної ідентифікації складають окрему групу електронних слідів.

причинність, яка передбачає причинний вплив на стан справ шляхом використання особою знаряддя – певним чином функціонуючої програми. Прикладами суб'єктної інструментальної причинності, зокрема, є внесення шістнадцятирічним редактором змін в оперативну пам'ять комп'ютера; використання уразливості в установленому додатку для віддаленого виконання в системі довільного коду; використання модифікованого програмного забезпечення при підробці документів. Знання слідчим криміналістичних особливостей електронного слідоутворення, характерних для способів здійснення конкретних видів і підвидів злочинів, становить основу причинного вивчення місця події на якому присутня комп'ютерна техніка використана злочинцем. Таке вивчення полягає в знаходженні в специфічному програмному середовищі інструментальних компонентів подій-причин, наприклад, прикладного програмного забезпечення, відповідного стадіям механізму правопорушення.

Встановлення причинності в комп'ютерно-технічній експертизі також охоплює і об'єктний контекст, в якому особа не є діючим агентом і не включена в причинну послідовність. Причинність в даному випадку пояснюється із застосуванням знань комп'ютерних наук, а подія-причина полягає у змінах, внесених автоматизованими діями функцій деякого системного або прикладного програмного забезпечення в наявний стан справ, при цьому виникнення і здійснення таких автоматизованих дій не залежить від суб'єктивної волі особи. Основною відмінністю між суб'єктними і об'єктними причинами є джерело впровадження активності деякої функції програми, взаємодії програми з носієм сліду і внесення змін до змісту даних. У першому випадку таким джерелом є людина, а в другому – причиною є подія самостійної, автоматичної активності іншої програми.

Завдання вивчення об'єктного контексту причинності виникає в зв'язку з необхідністю диференціації причинних комплексів об'єктної і суб'єктної причинності, що тягнуть за собою настання схожих наслідків. Так, наприклад, зміна даних на електронному

носії може статися внаслідок автоматизованих дій неправильно працюючої системної програми, а може бути викликана умисними діями злочинця.

З практичної точки зору розглянута структура причини дозволяє вказати на: 1) об'єктний або суб'єктний характер причини; 2) задіяні функції програмного забезпечення; 3) компоненти причинного комплексу, що взаємодіяли.

Сукупність електронних об'єктів, що знаходяться на досліджуваному носії інформації лише з певною часткою умовності можна назвати наслідком механізму електронного слідоутворення. Тому пропонується серед об'єктів, які спостерігаються на електронному носії по завершенні слідоутворення, розрізняти, по-перше, наслідки події електронного слідоутворення і, по-друге, програми і файли, що входили в причинний комплекс.

Наслідком події електронного слідоутворення є електронний слід, який може приймати форму змістовної відмінності, внесеної в раніше існуючий об'єкт, наприклад, розширені права доступу до файлу; змінені значення в частині полів бази даних (часткова змістовна відмінність); замінений файл на інший з таким же ім'ям, але з іншим змістом (повна змістовна відмінність) та ін. Новостворені об'єкти також є електронними слідами, наприклад, раніше відсутній (створений або скопійований користувачем в систему) файл; новий системний процес; нова системна служба та ін.

Наслідок також має характер події і якщо причина це завжди динамічна подія, то наслідок може бути як статичною, так і динамічною подією. Значущі компоненти стану справ і обстановки статичних подій-наслідків з часом або не змінюються, або змінюються незначно, потрапляючи в поле зору слідчого під час кримінального провадження практично в тому ж вигляді, в якому вони існували при слідоутворенні. Динамічні події-наслідки, навпаки, в силу внутрішньої специфіки, як правило, мають у своїй основі виконуваний код і застосовуються або для причинного впливу на компоненти програмного середовища, або для власної видозміни, часто можуть втрачати криміналістичні ознаки, а тому вимагають

швидкої і правильної процесуальної фіксації з метою припинення подальшого причинного впливу.

При цьому залежно від ступеня доступності для спостереження компонентів електронного причинного комплексу може бути розглянута повна і неповна слідова картина. Прикладом першого виду матеріальної обстановки є ситуація виявлення на електронному носії: програми, використаної для видалення даних (наприклад, WinHEX); залишених системних файлів; зайнятого залишками віддалених даних незаповненого простору (slack space) від мітки кінця файлу до завершення сектора або кластеру; присутніх в кореневому каталозі диска одного або декількох видалених файлів великого розміру (4 ГБ і більше). Другий вид матеріальної обстановки утворюється, наприклад, в ситуації виявлення на електронному носії pdf-файлу з розташованим в ньому програмним кодом експлойта при відсутності прикладної програми використаної для його впровадження. В даному випадку присутній слідосприймаючий об'єкт (pdf-файл), електронний слід (програмний код експлойта), проте відсутній слідоутворюючий об'єкт – інструментальний засіб (наприклад, Blackhole, Sweet Orange або Neutrino). Таким чином, виявлені на електронних носіях слідоутворюючі і слідосприймаючі об'єкти дозволяють вести мову як про вже встановлені компоненти причини утворення сліду, так і про компоненти причини утворення сліду, що тільки підлягають встановленню. При цьому необхідно підкреслити, що дані об'єкти хоча і пов'язані з подією слідоутворення, однак не є в прямому сенсі слова його наслідками.

Причинний зв'язок між подією-причиною і подією-наслідком в електронному слідоутворенні встановлюється на основі принципів зворотного або прямого причинного слідування при вирішенні пошукових експертних завдань з використанням типових або експериментальних зразків. При зворотному причинному слідуванні перехід відбувається від відомих електронних слідів до шуканих компонентів причинного комплексу, що взаємодіяли на основі активності функцій деякої програми. Прикладом

зворотного причинного слідування є питання: «За допомогою якого програмного забезпечення могли бути утворені представлені на дослідження електронні сліди?»

Принцип прямого причинного слідування полягає в переході від відомих компонентів причинного комплексу до шуканих електронних слідів. Спочатку можуть бути виявлені програми та файли, які були компонентами причинного комплексу та лише потім – на основі принципу прямого причинного слідування – деякий наслідок, який сформувався в результаті їх взаємодії. Ілюструє прямий перехід таке питання: «Які файли на електронному носії створені (модифіковані) за допомогою представленого на дослідження програмного забезпечення?»

Таким чином, причиною, в єдиному експертному і криміналістичному сенсі при дослідженні комп'ютерної техніки, є подія взаємодії та зміни компонентів причинного комплексу, яке відбувається в програмному середовищі на основі активованої з певного джерела функції деякої програми. Наслідком електронного слідоутворення є електронний слід в формі змістовної відмінності, що відбулась в результаті взаємодії компонентів причинного комплексу. Як для причини, так і для наслідку можуть бути запропоновані загальні і спеціальні типології. Практичною формою застосування знань про причину і наслідок є реалізація пошукових експертних завдань щодо встановлення зв'язку між подією-причиною і подією-наслідком з використанням принципів зворотного і прямого причинного слідування.

Національна академія правових наук України

Науково-дослідний інститут вивчення проблем злочинності
імені академіка В. В. Сташиса

# ІННОВАЦІЙНІ ЗАСАДИ ТЕХНІКО-КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ КРИМІНАЛЬНОЇ ЮСТИЦІЇ

*Монографія*

*За редакцією*
*академіка НАПрН України В. Ю. Шепітька,*
*члена-кореспондента НАПрН України В. А. Журавля*

Харків
2017

УДК 343.98 : 001.895
ББК 67.52
І 67

*Рекомендовано до друку вченою радою Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса Національної академії правових наук України (протокол № 11 від 26 жовтня 2016 р.)*

**Рецензенти:**
***Коновалова В. О.*** – професор кафедри криміналістики Національного юридичного університету іменні Ярослава Мудрого, доктор юридичних наук, професор, академік Національної академії правових наук України
***Степанюк Р. Л.*** – завідувач кафедри криміналістики та судової експертології факультету №1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор

**Колектив авторів:**
Шепітько В. Ю. – Передмова, §§ 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 3.1, 3.2; Журавель В. А. – Передмова, §§ 1.2, 4.1, 4.2, 4.3, 4.4; Авдєєва Г. К. – §§ 1.1, 1.2, 1.3, 1.4, 1.5, 2.3, 3.2, 3.3, 3.4; Білоус В. В. – §§ 2.1, 2.4; Великанов С. В. – §§ 2.5, 3.5; Гетьман Г. М. – § 2.2; Затенацький Д. В. – §§ 2.7, 2.8; Керик Л. І. – § 2.6; Павлюк Н. В. – §§ 4.2; 4.4; Резнікова О. І. – §§ 4.1; 4.4.

І 67 Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції : Монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. – Х.: Вид. агенція «Апостіль», 2017. – 260 с.

Монографію присвячено проблемам розроблення інноваційних засад техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції. У роботі розкрито сутність інновацій у техніко-криміналістичному забезпеченні діяльності органів кримінальної юстиції, досліджено проблеми застосування новітніх інформаційних технологій у діяльності органів досудового розслідування, інноваційні підходи до використання спеціальних знань у правозастосовній діяльності та питання техніко-криміналістичного забезпечення розслідування кримінальних правопорушень корупційної спрямованості.

Для науковців, працівників правоохоронних та судових органів, викладачів, аспірантів та студентів юридичних навчальних закладів.

ББК 67.52


ISBN