Сучасні проблеми дослідження криміналістичних особливостей кіберзлочинів

Усатий О.О.,
здобувач освітнього ступення «магістр»
Одеського державного університету внутрішніх справ
Ісмайлов К.Ю.,
завідувач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ,
кандидат юридичних наук

Процеси глобалізації виводять економічні відносини на принципово новий інформаційний рівень взаємодії. З розширенням впливу транснаціональних корпорацій розвивається і транснаціональна злочинність, об'єктом і предметом якої стають засоби комп'ютерних технологій. Від своєчасності і правильності виявлення їх особливостей безпосередньо залежить ефективність проведення слідчих (розшукових) дій, спрямованих на розкриття даного виду злочинів.

Кількість кіберзлочинів щороку зростає як на території України, так і в усьому світі. Актуальність боротьби з даним видом злочинів, а також їх розслідування і розкриття, мають пріоритетне значення для всієї держави, але з огляду на його специфічність виникають проблеми дослідження особливостей кіберзлочинів.

При дослідженні криміналістичних особливостей злочинів в сфері інформаційних технологій можна виділити ряд проблемних питань:

- висока латентність;
- складність збору доказів і процесу доказування, так як з'явився новий вид сліду, а саме «віртуальний слід»;
- широкий спектр криміналістично значущих ознак злочинів;
- відсутність єдиної програми боротьби з кіберзлочинами;
- складність розслідування комп'ютерних злочинів;
- відсутність узагальненої судової та слідчої практики у провадженнях даної категорії.

Для вирішення зазначених проблем необхідно виділити криміналістично значущі елементи характеристики кіберзлочинів:

- спосіб вчинення злочину;
- особливості слідової інформації;
- особливості обстановки скоєння злочину (місце скоєння злочину, час вчинення злочину та ін.);
- особистісна характеристика злочинця;
- особливості безпосереднього предмета злочинного посягання.

Спосіб вчинення злочину в криміналістиці є системою взаємообумовлених, рухливо детермінованих дій, спрямованих на підготовку, вчинення і приховування злочинів, пов'язаних, з використанням відповідних знарядь і засобів, а також часу, місця і інших обставин об'єктивної обстановки скоєння злочину.

У криміналістичній літературі можна зустріти безліч класифікацій способів скоєння комп'ютерних злочинів. Крилов В.В. наводить опис можливих способів порушення конфіденційності і цілісності комп'ютерної інформації без їх класифікації:

- розкрадання носіїв інформації у вигляді блоків і елементів ЕОМ;
- копіювання інформації;
- копіювання документів з вихідними даними;
- запам'ятовування інформації;
- фотографування інформації в процесі її обробки;
- виготовлення дублікатів вхідних і вихідних документів;
- використання недоліків програмного забезпечення та операційних систем;
- підміна елементів програм і баз даних.

Кіберзлочини залишають специфічну слідову картину: на місці події можна виявити як «традиційні» сліди, так і комп'ютерні сліди (віртуальні, комп'ютерно-технічні сліди), що залишаються в пам'яті електронних пристроїв.

Під віртуальними слідами розуміють сліди скоєння будь-яких дій (включення, створення, відкривання, активації, внесення змін, видалення) в інформаційному просторі комп'ютерних та інших цифрових пристроїв, їх систем і мереж [1, с. 47].

Будь-які дії з комп'ютерними або іншими програмованими пристроями (мобільними телефонами, смартфонами, планшетами і т.д.) отримують своє відображення в пам'яті, наприклад:

- в журналах адміністрування, журналах безпеки відображаються такі дії як включення, виключення, різні операції з вмістом пам'яті комп'ютера;
- в реєстрі комп'ютера відображаються дії з програмами (установка, видалення, зміна і т.д.);
- в log-файлах відображаються відомості про роботу в мережі Інтернет, локальних та інших мережах;
- у властивостях файлах відображаються останні операції з ними (наприклад, дата створення, останніх змін).

Віртуальні сліди можуть послужити доказами незаконного проникнення в пам'ять комп'ютера або іншого пристрою (злому), створення, використання і поширення шкідливих комп'ютерних програм, здійснення або підготовки скоєння злочину особою або групою осіб.

Обстановка місця скоєння злочину знаходиться в тісному зв'язку зі способом скоєння злочину і особистістю злочинця, так як спосіб вчинення злочину вибирається злочинцем з урахуванням можливої обстановки, в якій воно буде відбуватися, і конкретизується з урахуванням реально сформованої обстановки. Обстановка вчинення злочину може змінюватися під впливом застосованого злочинцем способу вчинення злочину.

Стосовно даного виду злочинів це перш за все означає, що спосіб вчинення комп'ютерного злочину буде визначатися найбільш характерними складовими обстановки:

- місцем і часом дії злочинця;
- особливостями організації інформаційної безпеки;
- можливостями порушення цілісності комп'ютерної інформації без безпосередньої участі людини;
- рівнем кваліфікації фахівців, що забезпечують захист інформації, а також адміністрування комп'ютерних мереж.

На сьогоднішній день одним з найбільш проблемних питань є визначення місця події. При вчиненні одного злочину, наприклад, неправомірного доступу до комп'ютерної інформації, може бути кілька місць події:

- робоче місце, робоча станція – місце обробки інформації, що стала предметом злочинного посягання;
- місце постійного зберігання або резервування інформації – сервер або стример;

- місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації, що знаходиться в іншому місці, при цьому місце використання може збігатися з робочим місцем, але перебувати поза організацією (наприклад, при сторонньому зломі шляхом зовнішнього віддаленого мережевого доступу);
- місце підготовки злочину (розробки вірусів, програм зламу, підбору паролів) або місце безпосереднього використання інформації (копіювання, поширення, спотворення), отриманої в результаті неправомірного доступу до даних, що містяться на ПК [2, с. 112].

Місцем події може бути одне приміщення, де встановлено комп'ютер і зберігається інформація, ряд приміщень, в тому числі в різних будівлях, розташованих на різних територіях, або ділянки місцевості, з якого проводиться дистанційний електромагнітний або аудіо перехват.

Також цікавим є питання, про те, чим же є кіберпростір і яке місце воно займає в криміналістичній характеристиці?

Найчастіше мережа Інтернет використовується як засіб скоєння злочину. Мережа може бути застосована для отримання інформації, що полегшує вчинення злочину, наприклад, відомостей про те, як створити вибуховий пристрій або виготовити складний синтетичний наркотик в домашніх умовах. З іншого боку можна застосувати кіберпростір для поширення незаконних матеріалів, інформації, в такому випадку він використовується для знаходження покупців, для пересилки інформації, і грошових коштів і таким чином використовується безпосередньо для здійснення суспільно небезпечного діяння. Саме використання глобальної мережі дозволяє в даному випадку створити розширену мережу збуту і сприяє як настанню злочинного результату, так і дозволяє залишити цю діяльність поза увагою правоохоронних органів.

При вчиненні злочину за допомогою кіберпростору можна говорити, що застосована нова сукупність прийомів, методів, послідовність дій, яка надає злочину унікальні властивості, не характерні для злочинів без використання мережі. Звісно ж, що в такому трактуванні вчинення злочину за допомогою Інтернет, сама мережа і є способом злочину [3, с. 92], і в той же час інформаційний простір є засобом як сукупність предметів і процесів

матеріального світу. Таке подвійне значення інформаційного простору під час скоєння злочину можливе завдяки його природі, яке є одночасно набором принципів, алгоритмів, правил взаємодій і в той же час воно реалізовано в матеріальному світі у вигляді сукупності з'єднаних комп'ютерів.

Виходить, що у випадках, коли кіберпростір безпосередньо використовується для вчинення злочину, він є способом і засобом одночасно, а в інших – лише засобом. Можна зробити висновок, що при скоєнні злочинів за допомогою кіберпростору змінюється його характеристика.

Також кіберпростір виступає не тільки засобом, а й місцем скоєння злочину, що досить сильно ускладнює процес розслідування комп'ютерних злочинів. В такому випадку традиційні способи огляду місця події вже не підходять, необхідна розробка та опрацювання абсолютно нової методики розслідування і розкриття кіберзлочинів, відповідно до властивостей із характерними особливостями Інтернет-простору.

1. Крылов В. В. Информационные компьютерные преступления : [учеб. и практ. пособие] / Крылов В. В. – М. : ИНФРА-М, 1997. – 276 с.
2. Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие : монографія / [И.Р. Шинкаренко и др.]. – Донецк : РВВ ЛДУВС, 2007. – 267 с.
3. Хахановський В.Г. Особливості криміналістичної характеристики кіберзлочинів / В.Г. Хахановський // Юридичний часопис Національної академії внутрішніх справ. – 2011. – № 1(1). – С. 89-93.

Застосування деяких аспектів аналітичної геометрії у задачах економіки

Фірман Л.Ю.,

старший викладач кафедри природничо-математичних дисциплін та інформаційних технологій Львівського інституту економіки і туризму

Рівняння лінії є найважливішим поняттям аналітичної геометрії. Найпростішою лінією на площині є пряма. Щоб скласти