Токарчук Т.Г.
студентка,
Національний юридичний університет імені Ярослава Мудрого

СПОСІБ ВЧИНЕННЯ ЗЛОЧИНІВ ЯК ЕЛЕМЕНТ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КІБЕРЗЛОЧИНІВ

Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються злочини, які є однією з найдинамічніших груп суспільно небезпечних посягань – кіберзлочини. Це зумовлене прискореним розвитком науки й технологій у сфері комп`ютеризації, а також постійним і стрімким розширенням сфери застосування комп`ютерної техніки.

Слід зауважити, що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України вперше передбачив самостійний розділ про такі злочини – розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп`ютерних мереж»; двічі положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві і про потребу детальнішого теоретичного аналізу.

Дану категорію злочинів називають по-різному: кіберзлочини, комп'ютерні злочини, злочини в сфері комп'ютерних технологій, злочини в сфері комп'ютерної інформації. Але у зв'язку з ратифікацією Україною Конвенції про кіберзлочинність 7 вересня 2005 року вважається за доцільне вживати термін кіберзлочини.

Найважливішим елементом криміналістичної характеристики злочину є спосіб його вчинення. В. М. Кудрявцев розглядає спосіб вчинення злочину як певний порядок, метод, послідовність рухів і прийомів, застосовуваних особою для вчинення злочину [1, с. 95].

На сьогоднішній день відсутній єдиний підхід до описання способів вчинення „комп'ютерних» злочинів. Різні варіанти класифікацій способів вчинення кіберзлочинів були запропоновані Ю.М. Батуріним, П.Д. Біленчуком, В.Б. Веховим, В.В. Головачем, В.О. Голубєвим, М.А. Губанем, О.М. Жодзинським, Н.І. Клименком, О.І.Котляревським, В.Ю. Рогозіним, В.М. Салтевським, М.О. Селівановим, К.С. Скоромніковим, Б.Х. Толеубековою, О.М. Юрченком та ін.

Для досить різнорідної сукупності, утвореної кіберзлочинами, важко було б отримати єдину узагальнену картину, що характеризує все різноманіття способів їх вчинення. Крім того, розвиток інформаційних технологій, впровадження нових технічних і програмних засобів, посилення «інтелектуалізації» кримінального середовища в Інтернеті призводять до постійних змін способів вчинення протиправних діянь.

З метою виявлення основних способів вчинення всі кіберзлочини можуть бути розділені на дві групи за ступенем підготовленості.

Для злочинів першої групи умисел виникає раптово, під впливом провокуючої ситуації (наприклад, незахищеності об'єкта посягання). Як правило, фігурантами таких справ є малодосвідчені порушники, що

допускають велику кількість прорахунків, у зв'язку з чим їх встановлення не являє особливої складності для правоохоронних органів.

Друга група злочинів характеризується наявністю обдуманого плану, що включає вивчення об'єкта посягання, підготовку до вчинення протиправних дій і т. д. Ця група представляє великий інтерес в силу того, що виявлення злочинця тут, як правило, ускладнюється і вимагає застосування комплексу слідчих і оперативно-розшукових заходів.

Н. Г. Шурухнов поділяє способи неправомірного доступу до комп'ютерної інформації на такі три групи: способи безпосереднього доступу; способи віддаленого доступу; комплексні способи [2, с. 103-110]. До першої групи належать способи, які в літературі іноді називають «за дурнем» (коли для проникнення у заборонену зону правопорушник, тримаючи в руках предмети – елементи маскування, разом з якоюсь особою проникає до приміщення) та «прибирання сміття» (використання відходів інформаційного процесу – фізичних чи електронних, що залишені користувачем після роботи з комп'ютером) [3, с. 28].

До другої групи способів належать: підключення до телекомунікаційного обладнання, комп'ютерної системи чи мережі; проникнення в комп'ютерні мережі шляхом автоматичного перебирання абонентських номерів із подальшим з'єднанням з тим або іншим комп'ютером; проникнення у комп'ютерну систему з використанням чужих паролів («непоспішний вибір»); безпосереднє та електромагнітне перехоплення інформації. Останній спосіб ґрунтується на тому, що робота електронних пристроїв (дисплеї, принтери) супроводжується побічними електромагнітними випромінюваннями (так, сигнали з електронно-променевої трубки дисплея можна приймати, записувати й аналізувати на відстані понад 1000 м).

Третю групу утворюють такі способи: уведення в комп'ютерну програму команд, що дають змогу здійснювати незаплановані функції («троянський кінь»); модифікація комп'ютерної програми («містифікація»); доступ до баз даних і файлів шляхом знаходження слабких місць у системах захисту («маскарад»); використання помилок і недоліків у комп'ютерній програмі [3, с. 30-32].

Розглядаючи основні способи вчинення кіберзлочинів, слід зазначити, що хакери досить часто (практично на будь-якому з етапів вчинення злочину) застосовують різного роду психологічні прийоми і хитрощі, називаючи їх методами соціальної інженерії [4, с. 127]. У першу чергу при цьому передбачається отримання обманним шляхом інформації, необхідної для подолання захисного бар'єру мережевої системи.

Таким чином, можна зробити висновок, що під час вчинення кіберзлочинів, зловмисники застосовують значну кількість спеціальних програмних продуктів, як розповсюджуваних у готовому вигляді, так і створених власноруч, для вирішення своїх злочинних завдань. Тим не менш, знання про основні способи, застосовувані на різних етапах вчинення таких злочинів може значно полегшити процес встановлення всіх обставин події, виявлення та фіксації слідів, та планування процесу розслідування кіберзлочину.

Список використаної джерел:

1. Топольскова І.О. Боротьба із втягненням неповнолітніх у злочинну або іншу антигромадську діяльність: Монографія / МВС України, Луг. акад. внутр. справ ім. 10-річчя незалежності України; [Наук. ред. д-р юрид. наук, проф. В.П. Ємельянов]. – Луганськ: РВВ ЛАВС, 2003. – 192 с.

2. Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г. Шурухнова. – М. : Щит-М, 1999. – 254 с.

3. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юрид. лит., 1991. – 160 с.

4. Криміналістика (криміналістична техніка): Курс лекцій / П.Д. Біленчук, А.П. Гель, М.В. Салтевський, Г.С. Семаков. – К.: МАУП, 2001. – 216 с.