ПРОБЛЕМНІ ПИТАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ВТРУЧАННЯМ У РОБОТУ БАНКОМАТІВ

Криволапов В.М., ад'юнкт наукової лабораторії з проблем досудового розслідування ННІ №1 НАВС.

Цього року Всесвітній огляд економічних злочинів робить акцент на зростаючу загрозу кіберзлочинності. У наш час багато людей та організацій використовують різні технології, включаючи Інтернет. Таким чином вони зустрічаються з потенційними ризиками атак шахраїв із будь-якого куточку світу. На фоні таких проблем, як викрадення даних та виток інформації, комп'ютерні віруси та атаки хакерів, особлива увага у нашому огляді приділяється значущості цього виду економічної злочинності та його впливу на організації в усьому світі.

На сьогодні кримінальні правопорушення у сфері інформаційних технологій - це одна з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства, так чи інакше, пов'язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією. Останнім часом в Україні значно зросла кількість Інтернет користувачів, адже підключення до глобальної мережі стало доступним та зручним. Сьогодні персональний

комп’ютер, КПК, мобільний телефон з підключенням до Інтернету сприймається як належне та необхідне. Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого. Інтернет – це чудовий засіб для зв’язку та спілкування. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп’ютерна інформація, трапляються, кримінальні правопорушення, кіберзлочини.

Криміналістична особливість кіберзлочинів, що вчиняються шляхом втручання в роботу банкоматів, полягає в тому, що розслідування та розкриття цих злочинів неможливе без застосування та використання комп’ютерних технологій. Це пов’язано з необхідністю відшукування, фіксування, вилучення та збирання доказів в електронній формі. Також комп’ютерні технології широко використовуються для проведення негласних слідчих(розшукових) дій.

Кіберзлочини можна класифікувати на два види: традиційні злочини, що вчиняються за допомогою комп’ютерних технологій та Інтернету(шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації і т.д.), та нові злочини, що стали можливі завдяки новітнім комп’ютерним технологіям (злочини передбачені Розділом XVI Кримінального кодексу України). Найчастіше з використанням комп’ютера та Інтернету вчиняються такі традиційні злочини: порушення авторського права і суміжних прав(ст. 176); шахрайство (ст. 190); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200); ухилення від сплати податків, зборів (обов'язкових платежів)(ст. 212); ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301); незаконне

збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231)[1]. Отже в криміналістичному аспекті кіберзлочини – це передбачені кримінальним законом суспільно небезпечні діяння, для скоєння та розслідування яких застосовуються комп'ютерні технології та/або використовується глобальна мережа Інтернет.

Так, працівники Департаменту кіберполіції Національної поліції України, Голосіївського управління столичної поліції, патрульної поліції та служби безпеки одного із українських банків, викрили стійке злочинне угрупування. Зловмисники, шляхом втручання в роботу банкоматів із використанням шкідливого програмного коду (вірусу) заволодівали грошима з касет банкоматів.

Одного із членів угрупування оперативники затримали на території Голосіївського району столиці саме під час вчинення чергової крадіжки з банкомату. На місці події у нього вилучено гроші, клавіатуру, обладнання та флеш-накопичувач з можливим шкідливим програмним продуктом. Відтак, вилучену техніку та флеш-накопичувач направлено до експертного центру для проведення їх повного дослідження.

Під час проведення огляду місця події працівники поліції також виявили 360 тисяч гривень біля банкомату, які зловмисники ініціювали на видачу з банкомату за допомогою програмного забезпечення. Крім того, у одного із зловмисників в сумці було виявлено 36 тисяч гривень, які він встиг сховати[2].

Специфіка даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється, практично не відходячи від "робочого місця", злочини є доступними; оскільки комп'ютерна техніка постійно дешевшає; злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для

використання її в якості речового доказу. Усе це, безумовно, є перевагами для кіберзлочинців.

Список використаних джерел:

1. Кримінальний кодекс [Електронний ресурс]. –Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14

2. У Києві знешкодили банду, що обкрадала банкомати (фото)[Електронний ресурс]. – Режим доступу: http://expres.ua/news/2017/06/20/248354-kyyevi-zneshkodyly-bandu-obkradala-bankomaty-foto