Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Деякі аспекти щодо розслідування шахрайств з банківськими рахунками в мережі Інтернет

Годнюк Л.М.
курсант 4-го курсу
Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Павлова Н.В.
кандидат юридичних наук,
старший викладач кафедри криміналістики, судової
медицинита психіатрії Дніпропетровського державного
університету внутрішніх справ

Разом з розбудовою інформаційного суспільства в Україні швидкими темпами почали поширюватись і нові види кіберзлочинів. Згідно аналізу проведених досліджень більш ніж 75% від усіх збитків, заподіяних економічною злочинністю, припадає на сферу діяльності банківських установ. Однією із найбільших складностей є встановлення факту скоєння комп'ютерного злочину в банківській системі. Пояснюється це тим, що зовні сам факт вчинення комп'ютерного злочину та його прояви в оточуючому середовищі не завжди є помітними.

Наразі способів шахрайства з використанням віртуального електронного простору (кіберпростору) існує велика кількість. Їх можна розділити на такі основні групи:

1. Перехоплення інформації: безпосереднє перехоплення, і електромагнітне перехоплення.
2. Несанкціонований доступ до інформації: "комп'ютерний абордаж", "містифікація", "маскування", "непостійний вибір", "за хвіст", "аварійний", "за дурнем", "пролом", "люк", "склад без стін", "системні роззяви".
3. Маніпуляції з інформацією: "троянський кінь в ланцюгах", "троянська матрьошка", підміна даних, підміна коду, комп'ютерні віруси, "салямі", "логічна бомба", "асинхронна атака", моделювання, "повітряний змій", "пастка на живця".
4. Отримання і використання інформації із злочинною метою: крадіжка програмного забезпечення, крадіжка устаткування за допомогою комп'ютерних операцій, крадіжка грошей за допомогою отримання секретних кодів, крадіжка грошей шляхом комп’ютерного пересилання, крадіжка грошей шляхом маніпуляції з комп'ютером, внесення змін в програму [1].

Крадіжці грошей з карт звичайно передує тривала підготовка. За електронною поштою або ICQ засилається вірус, наприклад, відомий вірус типу Trojan (Trojan.PWS.LDPinch.1061), що запам'ятовує всі уведені паролі та логіни і відправляє їх шахраям. Після того як дані викрадені, злочинці в Україні звичайно використовують їх для оплати мобільних переговорів за допомогою електронно-платіжних систем або здобувають товари в послуги на інтернет-сайтах, де необхідно ввести тільки номер картки, ім'я користувача і спеціальний перевірочний код (verification code) [2].

Ще одним прикладом є вчинення злочину за допомогою системи «Приват-24». Даний спосіб полягає у наступному: зловмисник реалізуючи свій злочинний задум, під час телефонної розмови із потерпілим під приводом надання матеріальної допомоги на лікування, отримує інформацію про номер картки, телефону до якого прив’язана картка, ідентифікаційний код та пароль, надісланий банком у вигляді текстового смс-повідомлення. Внаслідок цього отримана конфіденційна інформація дає можливість здійснювати керування рахунками потерпілої особи від її імені в системі розрахунків «Приват-24». Гроші шахрай перераховує із рахунків осіб, відшуканих ним в соціальних оголошеннях, наступним чином: за допомогою конфіденційної інформації, яку отримав від потерпілої заходить до системи обирає операцію по зміні паролю, після чого система «Приват-24» відправляє смс-повідомлення у вигляді 8 цифр на номер телефону потерпілого. Зателефонувавши до власника карти, зловмисник отримує 8 цифр, які надійшли на телефон потерпілого і змінює пароль картки на новий і цим самим отримує змогу перераховувати кошти на підшукані заздалегідь картки [3].

На сьогоднішній день невирішеним залишається питання щодо практичних рекомендацій з розслідування кіберзлочинів, що в свою чергу сприяє безкарності винних осіб. На початковому етапі розслідування вказаних злочинів слідчий допускає низку криміналістичних помилок, серед яких: несвоєчасність огляду; неповнота та формальне відношення до нього; невикористання всіх можливостей з фіксації функціонування та впливу шкідливих програм.

Важливо під час розслідування злочинів, які пов’язані з комп’ютерами та комп’ютерними системами, уникати дій, які можуть пошкодити чи змінити наявну інформацію, у той чи інший спосіб змінити цілісність вилучених даних.

Алгоритм початкового етапу розслідування досліджуваних злочинів повинен включати:

1. Допит потерпілого та можливих свідків (очевидців) злочину. Так, слідчому необхідно у потерпілого встановити, що слугувало підставою для рішення про те, що був несанкціонований доступ, з'ясовується розмір матеріальної шкоди.

Слушною є думка Ю. В. Гавриліна про те, що у випадку неправомірного доступу до комп'ютерної мережі необхідно допитати інженерів-програмістів, що займаються розробкою програмного забезпечення, операторів, спеціалістів з технічного забезпечення, що займаються ремонтом засобів комп'ютерної техніки, системних програмістів, інженерів із засобів зв'язку та телекомунікаційному обладнанню, спеціалістів по забезпеченню безпеки комп'ютерних систем та інше [4, с. 23].

2. Проведення огляду місця події – місць виявлення слідів злочину з обов'язковим оглядом комп'ютерного засобу. Навіть при всій обережності в роботі з інформацією, інколи залишаються сліди. Це може бути якась випадково стерта інформація, або плутанина в програмі, яка могла статись при застосуванні не тої команди, яку потрібно було б застосувати. В ході огляду місця події слідчому необхідно з'ясувати характеристики комп'ютера; програмного забезпечення, що на ньому встановлене; розташування окремих елементів комп'ютерної системи, їх призначення, визначити наявність та можливість їх з'єднання з іншими комп'ютерними системами. При цьому з'ясовується розташування під'єднувальних кабелів та можливість підключення чи відключення певних пристроїв від комп'ютерної системи без доступу у приміщення, а також безпосередньо в самому приміщенні. З тим, щоб у подальшому виключити можливість оскарження в суді правильність проведеного огляду та його результатів слідчий повинен підбирати понятих, які мають певні знання в галузі комп'ютерної техніки (основних операціях, назвах комп'ютерних програм тощо) [5, с. 78].

3. Проведення комп'ютерних експертиз (програм для ЕОМ, баз даних, окремих файлів, спеціальних технічних засобів тощо). Під час розслідування можливі випадки, коли конкретно невідомо, яка інформація може становити інтерес для слідства. За цих умов особа, що здійснює досудове розслідування, вимушена за допомогою експерта ознайомитися з усіма вилученими матеріалами.

4. Отримання необхідних документів, що свідчать про протиправність події або відображають незаконність проведення операції у сфері комп'ютерної інформації (договору на отримання послуг Інтернет тощо); отримання у провайдера протоколу роботи в мережі даного абонента за певний період часу з зазначенням дати, часу, початку сесії, тривалості роботи, грошових коштів, списаних з рахунку клієнта; журналів реєстрації користувачів; актів відомчих комісій; журналів обліку збоїв у роботі комп'ютерної мережі окремих комп'ютерів чи технічних пристроїв з ладу; файлів адміністратора мережі, в яких фіксується вся робота мережі; актів за результатами антивірусних перевірок, інші [6].

5. Отримання ідентифікаційних даних про власника комп'ютерного засобу, що здійснив незаконний дистанційний доступ до комп'ютерної інформації.

6. Проведення оперативно-розшукових заходів щодо встановлення осіб, які причетні до злочину.

Отже, робота з комп'ютерами і комп'ютерним обладнанням потребує спеціальних знань та удосконалення збору і процесуального закріплення доказів при розслідуванні кіберзлочинів.

Література:

1. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: Підручник / Біленчук П.Д., Зубань М.А., - К., 1994.

2. Як боротися проти крадіжок грошей з кредитних карт? [Електронний ресурс]. – Режим доступу: http://news.finance.ua/ua/news/-/106543/yak-borotysya-proty-kradizhok-groshej-z-kredytnyh-kart

3. Вирок Таращанського районного суду Київської області від 06.09.2013: спр. № 379/1357/13-к [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/33328487

4. Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации: [учеб. пособие] / Ю. В. Гаврилин. – М.: ЮИ МВД РФ, Книжный мир, 2001. – 88 с.

5. Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений: [монография] / Л. Н. Соловьев. – М. : Собрание, 2004. – 224 с.

6. Яблоков Н.П. Криминалистическая характеристика финансовых преступлений // Вестник московского университета. Серия 11. Право. – 1999, № 1.