УДК 004.056.5

Шевченко Ю.В.
Кіровоградський машинобудівний коледж
Кіровоградського національного технічного університету

Способи крадіжок у банківських інформаційно-обчислювальних системах

На даний час з впевненістю можна констатувати той фактор, що шахрайство відрізняється здатністю швидко змінювати форми прояву і проникати практично в усі сфери соціального життя. Найбільшою мірою вразливим перед шахрайством виявився банківський сектор, не зважаючи на те, що банки витрачають величезні кошти на підтримку власної безпеки свого майна і майна клієнтів.

Швидка модернізація банківського сектора, обумовлена появою електронних систем взаєморозрахунків, викликала до життя десятки нових форм шахрайства, які вимагають адекватної правової оцінки. В останні десятиліття в банківському секторі набули поширення форми шахрайства, пов’язані з використанням телеграфних авізо, пластикових платіжних засобів, електронного підпису, електронних цінних паперів, віртуальних Internet-магазинів. [1]

Зважаючи на істотні фінансові збитки, які завдаються "комп'ютерними злочинами" в сфері економіки, доцільно зупинитися на способах крадіжок в банківських інформаційно-обчислювальних системах.

Під способом крадіжок в інформаційних системах кредитно-фінансових структур розуміють сукупність прийомів і засобів, що забезпечують несанкціонований доступ до банківських інформаційних ресурсів і технологій, дозволяють здійснити модифікацію інформації з метою порушення відносин власності, що виражається у протиправному вилученні коштів. [2]

За своєю криміналістичною сутністю такого роду навмисні дії є злочином з чітко вираженими етапами розвитку. Вони відрізняються один від одного за характером дій і ступенем завершеності кримінального діяння. Такий поділ на стадії необхідний для правильної правової оцінки. Можна виділити наступні три етапи.

Приготування до злочину - отримання на час розкрадання знарядь діяння (наприклад, комп'ютера), написання спеціальної програми, що дозволяє подолати захист банківських мереж, збір інформації про клієнтів банку, системи захисту, підбір паролів, подолання систем захисту від несанкціонованого доступу до даних і комп'ютерної інформації (умисне створення умов для вчинення злочину).

Замах на злочин - проводиться шляхом маніпуляції даними, збереженими в пам'яті банківської інформаційної системи і її керуючими програмами для несанкціонованого руху грошових коштів на користь зловмисника або третьої особи.

Закінчення злочину - коли всі несанкціоновані транзакції завершені і зловмисник має можливість скористатися плодами свого діяння. [3]

До прийомів, які застосовуються в комп′ютерних злочинах у банківській сфері можна віднести наступні:

вилучення засобів обчислювальної техніки - проводиться з метою отримання системних блоків, окремих вінчестерів або інших носіїв інформації, що містять в пам'яті установчі дані про клієнтів, вкладників, кредиторів банку і т. д. Такі дії проводяться шляхом розкрадання, розбою, вимагання і самі по собі є звичайними "некомп'ютерними" злочинами;

перехоплення інформації також слугує для отримання певних відомостей за допомогою методів і апаратури аудіо-, візуального та

електромагнітного спостереження. Об'єктами, як правило, є канали зв'язку, телекомунікаційне обладнання, службові приміщення для проведення конфіденційних переговорів, паперові і магнітні носії (в тому числі і технологічні відходи). [3]

Несанкціонований доступ до засобів обчислювальної техніки - це активні дії по створенню можливості розпоряджатися інформацією без згоди власника. Несанкціонований доступ звичайно реалізується з використанням таких основних прийомів:

- "за дурнем"- фізичне проникнення у виробничі приміщення. Інший варіант - електронне проникнення в засоби обчислювальної техніки;

- "комп'ютерний абордаж"- зловмисник вручну, або з використанням автоматичної програми підбирає код "пароль"доступу до банківської системи;

- "неквапливий вибір" - зловмисник вивчає та досліджує систему захисту від несанкціонованого доступу, її слабкі місця, виявляє ділянки, що мають невдалу логіку програмної будови, розриви програм - "люки" і вводить додаткові команди, які дозволяють доступ;

- "маскарад" - зловмисник проникає в банківську комп'ютерну систему, видаючи себе за законного користувача з застосуванням його кодів "паролів" та інших ідентифікуючих шифрів; [4]

- "містифікація" - зловмисник створює умови, коли законний користувач здійснює зв'язок з нелегальним терміналом, будучи впевненим у тому, що він працює з потрібним йому законним абонентом. Формуючи правдоподібні відповіді на запити користувача і підтримуючи його помилки деякий час, зловмисник видобуває паролі доступу;

- "аварійний режим" - зловмисник створює умови для виникнення збоїв у роботі засобів обчислювальної техніки. При цьому включається особлива програма, що дозволяє в аварійному режимі отримувати доступ до найбільш цінних даних. У цьому режимі можливе «відключення» всіх наявних в банківській комп'ютерній системі засобів захисту інформації;

- "асинхронна атака"- є одним із прийомів підготовчого етапу до скоєння злочину. Злочинець, використовуючи асинхронну природу операційної системи, змушує працювати банківську комп'ютерну систему в помилкових умовах, через що управління обробкою частково або повністю порушується. Дана ситуація використовується для внесення змін в операційну систему, причому ці зміни не будуть помітні;

- "моделювання" - це найбільш складний і трудомісткий прийом підготовки до вчинення злочину. Зловмисник будує модель поведінки банківської комп'ютерної системи в різних умовах і на основі вивчення організації руху грошових коштів оптимізує спосіб маніпуляції даними. Наприклад, в декількох банках відкриваються рахунки на незначні суми, моделюється ситуація, при якій гроші переводяться з одного банку в інший і назад з поступовим збільшенням сум. В ході аналізу виявляються умови, при яких: а) в банку виявиться, що доручення про переведення не забезпечене необхідною сумою; б) коли в банк необхідно надіслати повідомлення з іншого банку про те, що загальна сума покриває вимогу про перший перевод; в) встановлюється, скільки циклів це потрібно повторювати, щоб на рахунку виявилася достатня сума і кількість платіжних доручень не видавалася підозрілою;

- "підміна даних" використовується безпосередньо для обернення грошових сум на свою користь і представляє собою спосіб модифікації відомостей, при якому зловмисником змінюються або вводяться нові дані;

- "троянський кінь", "хробак", "бомба" також слугують безпосередньо для обернення чужих грошей на свою користь. Це така маніпуляція, при якій зловмисник таємно вводить в прикладне програмне забезпечення спеціальні модулі, які

забезпечують відрахування на заздалегідь відкритий підставний рахунок певних сум з кожної банківської операції або збільшення суми на цьому рахунку при автоматичному перерахунку залишків, пов'язаних з переходом до комерційного курсу відповідної валюти. Банківські трояни сьогодні є причиною 80% випадків крадіжки грошей з банківських рахунків. Це програми, створені для того щоб викрадати особисті дані користувачів, особливо вони «загострені» на крадіжку пар логінів та паролів особистих кабінетів інтернет-банкінгу. Троянці також можуть перехоплювати SMS з секретними кодами, які надсилає банк і перенаправляти їх зловмисникам. Крім того, вони здатні також безпосередньо красти гроші з рахунку - все відразу або поступово невеликими транзакціями, щоб не так явно позначати свою діяльність і не бути виявленими; [5]

- «салямі» - оригінальна електронна версія методів вилучення «зайвих» грошових коштів на свою користь. При використанні цього методу зловмисник так само, як і в попередньому випадку, «дописує» прикладне програмне забезпечення спеціальним модулем, який маніпулює інформацією, перекидаючи на підставний рахунок результати округлення при проведенні законних транзакцій. Розрахунок побудований на тому, що відраховуються суми настільки малі, що їх втрати практично непомітні, а незаконне накопичення коштів проводиться за рахунок суми здійснення великої кількості операцій. [4]

Особливе місце займають методи, які застосовуються зловмисником для приховування слідів злочину. Ці дії спрямовані на те, щоб злочинець зміг скористатися плодами своєї неблагородної праці. Ці методи важливі при оцінці завершеності злочину. Одним з таких методів є дроблення грошових сум - зловмисник ділить отримані в результаті несанкціонованих маніпуляцій з банківською інформацією грошові кошти на нерівні часткові частини із зарахуванням на рахунки сторонніх банків, в яких можна було б згодом зняти переведені суми готівкою.

Актуальність проблем кібербезпеки у банківській справі сьогодні не викликає жодних сумнівів.

Для повноцінного захисту систем зберігання та обробки даних потрібна не просто установка відповідного програмного забезпечення, а цілий комплекс програмно-технічних, адміністративно-організаційних та нормативно-правових заходів.

Сьогодні в Україні прийнято ряд заходів для боротьби з кіберзлочинністю в банківській сфері – розроблена стратегія кібербезпеки України (Указ Президента України №96/2016 від 15 березня 2016 року), створено Центр реагування на інциденти кібернетичної безпеки у банківській системі та платіжному просторі України CERT-NBU, спрямований на вирішення проблем боротьби з кіберзагрозами і сприяння розвитку банківської системи України вцілому. Але законодавча і нормативно-правова база у сфері кібербезпеки залишається досить недосконалою, країна прагне до світового лідерства за кількістю кіберзагроз у банківській сфері та несе неймовірні збитки.

Список використаних джерел

1. *О.В. Кришевич Способи шахрайств в банківській сфері: кримінально-правовий аспект / О.В. Кришевич // Юридичний вісник. – 2012. - №2. - С. 112-116.*
2. *А.М. Клочко Злочини у сфері банківської діяльності /А.М. Клочко // Правовий вісник Української академії банківської справи. - 2014.- №1.- С. 68-71.*
3. *Чернявський, С.С. Фінансове шахрайство і методологічні засади розслідування: монографія / С.С. Чернявський.- К.: Хай-Тек Прес, 2010. - 624 с.*
4. *Характеристика современных угроз безопасности автоматизированных банковских систем [Електронний ресурс]. - Режим доступу:* http://www.rusnauka.com/11_NPE_2013/ Economics/1_134050.doc.htm. - Назва *з екрана.*
5. *Банківські троянці [Електронний ресурс]. - Режим доступу:* http://zillya.ua/bankivski-troyantsi. - Назва *з екрана.*