Риски электронных расчетов

написано Александр Астахов | 10 июня, 2023

Одно из первых ограблений крупного банка, выполненное с помощью компьютеров и подчеркнувшее глобальный характер киберпреступности, произошло в 1994 году, когда российский хакер Владимир Левин взломал автоматизированную банковскую систему (АБС) Ситибанка и перекачал 10 млн. долл. на свои счета. Все похищенное, за исключением 400 тысяч долларов, было восстановлено. В 1995 году Левин был арестован и в 1997 году выдан в США. В 1998 году он был признан виновным в компьютерном мошенничестве и приговорен к трем годам лишения свободы и штрафу в 240 тысяч долларов.

Наглядную иллюстрацию информационных рисков, которым изо дня в день подвергается практически каждая организация являет случай с таинственным уводом денег со счетов Уральского банка.

> *Со счетов «Уральского бюро экспертизы и оценки», обслуживавшихся через систему интернет-банкинга в Уральском банке реконструкции и развития «исчезло» 1,5 млн. руб. Эта сумма составляла почти весь оборотный капитал фирмы. На сайте, где он обслуживался, сообщается, что «обнаружен вирус, похищающий секретные ключи клиентов».*

Это только один из многочисленных примеров тех рисков, которые возникают при электронных расчетах. В таких случаях очень сложно что-либо доказать. Как правило, Банк не несет никакой ответственности и не компенсирует убытки в том случае, если электронная подпись на платежном поручении принадлежит организации. Наша практика показывает, что многие компании адекватно не оценивают рисков, связанных с использованием систем Клиент-Банк, без всяких на то оснований полагаясь в этом вопросе на банки, и не принимают необходимых защитных мер, а ведь в данном случае возможный ущерб – это прямые финансовые потери организации в размере остатков на ее

расчетных счетах.

По сообщению Интерфакс в 2007 году:
В управление обратились официальные представители полиции США. Они сообщили российским коллегам, что с карточных банковских счетов граждан США регулярно похищаются крупные суммы денег. По информации американских коллег, эти деньги снимались наличными через банкоматы в Москве. При этом сами хозяева банковских карт Россию никогда не посещали.

В ходе проверки информации удалось установить, что все наличные средства снимались через десять московских банкоматов. Все эти банкоматы имели встроенную скрытую видеокамеру. Получив у служб безопасности банков, которым принадлежали банкоматы, видеосъемку, оперативники УБЭП выяснили, что деньги похищали четыре жителя Москвы – двое бывших банковских служащих, а также двое студентов.

За ними было установлено скрытое наблюдение. Вскоре выяснилось, что молодые люди через Интернет вошли в сговор с преступными группами в США, Канаде и Франции. За вознаграждение они получили от этих партнеров данные о тысячах карточных счетов в американских банках. Молодые люди арендовали квартиру, где наладили производство поддельных банковских карт. Затем по ночам при помощи таких карт они снимали деньги через банкоматы.

Оперативники управления по борьбе с экономическими преступлениями задержали мошенников с поличным в момент, когда они получали по поддельной карте через банкомат 2,5 тыс. долларов. Во время задержания у них изъяли еще 12 поддельных банковских карт с PIN-кодами.

Всего, по данным ГУВД, мошенники за время своей деятельности похитили у граждан США более 500 тыс. долларов. Все четверо арестованы, им предъявлено обвинение в мошенничестве.

Россия догнала Европу по уровню преступности в карточном

бизнесе. Ежегодный ущерб от хищения денежных средств клиента с помощью платежных карт в международных платежных системах достигает сотен миллионов долларов. Эксперты прогнозируют, что принимаемые странами Европы энергичные меры по укреплению безопасности карточного оборота могут в самые ближайшие годы – в результате миграции этого вида преступности – привести к еще большему росту хищений в России. Это делает актуальным внедрение в российских банках новых технологий защиты.

В 2005 году в Москве ликвидирована группа мошенников, занимавшихся хищением денег с банковских карт. Как сообщил начальник пресс-группы УБЭП ГУВД Москвы Филипп Золотницкий, группа мошенников состояла в основном из студентов.

По данным следствия, метод работы мошенников был отработан до мелочей. Студенты связывались через Интернет с преступными группами в странах Западной Европы и получали от них данные кредитных банковских карт западноевропейских граждан с PIN-кодами. Используя эту информацию, мошенники изготовляли поддельные карты, с помощью которых снимали наличные средства в банкоматах Москвы.

До момента задержания преступная группа успела снять в общей сложности более 60 тыс. долл. При обыске у мошенников были обнаружены данные банковских карт и поддельные кредитные карты, по которым был возможен доступ к счетам на общую сумму более полумиллиона долларов.

Крупное мошенничество подобного рода было совершено в 2003 году, когда в Москве была задержана очередная группа вечно голодных студентов, похитивших с банковских счетов более 700 тыс. долларов. Группировка мошенников состояла из студентов технических вузов столицы.

Недоучившиеся инженеры разработали собственную систему обмана банков. Они устанавливали на банкоматах миниатюрные видеокамеры, которые фиксировали PIN-код владельца, а на отверстие для карточки монтировали специальную рамку, которая

считывала параметры карточки и сумму, оставшуюся на счете.

Когда эта книга уже готовилась к печати, СМИ сообщили о появлении «трояна» в банкоматах ряда российских банков, перехватывающего информацию с банковских карт. Банкоматы и раньше подвергались вирусным атакам, однако в худшем случае они могли привести к некорректной работе данных устройств. Появившийся недавно вирус действует иначе и способен нанести серьезный ущерб клиентам российских банков, которые используют банкоматы.

> *В марте 2009 года в СМИ появились сообщения о появлении новой угрозы в закрытых сетях банкоматов некоторых российских банков. Уникальность обнаруженного вируса состоит в его способности перехватывать данные о банковских картах пользователей, которые ранее пользовались зараженным банкоматом. Тем самым с помощью полученной информации злоумышленники получают возможность уводить со счетов людей все деньги, которыми они располагают. Троян Trojan.Skimer собирает информацию о кредитных картах и PIN-кодах к ним. Единственное, что требуется злоумышленникам, использующим данный вирус, — подойти к банкомату, ввести код и получить на чеке распечатку с данными потенциальных жертв мошенничества.*
>
> *В связи с тем, что, как правило, сети банкоматов не связаны с сетью Интернет, единственный способ проникновения на них подобной вредоносной программы — участие в этом людей, тесно связанных с банком или являющихся их сотрудниками. Об этом также говорит тот факт, что на банкоматах устанавливается специальное ПО, поставляемое непосредственно их производителем. Соответственно, велика вероятность того, что создавали данный вирус люди, близко знакомые с логикой работы данного ПО и структурой его кода.*

Как уже было отмечено, количество преступлений в данной сфере продолжает расти несмотря на то, что банки и правоохранительные органы пытаются совместно разрабатывать

системы защиты.

На этом мы остановимся в живописании глобальных информационных рисков. Этой теме можно было бы посвятить несколько увесистых томов, однако и приведенных фактов вполне достаточно для того, чтобы осознать насколько серьезны и разнообразны информационные риски, которым подвергается современное общество, часто даже об этом не подозревая.