Ученые записки Таврического национального университета имени В.И. Вернадского
Серия «Экономика и управление». Том 27 (66). 2014 г. № 1. С. 12-17.

УДК 004.056.5

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЛАТЕЖНЫХ СРЕДСТВ

Бойченко О.В.

Таврический национальный университет имени В.И. Вернадского, Симферополь, Республика Крым
E-mail: bolek61@mail.ru

В статье рассматриваются современные проблемы информационной безопасности платежных систем. Проводится анализ основных видов мошенничества с пластиковыми банковскими картами и представляется ряд рекомендаций по противодействию мошенничеству в платежных системах.
Ключевые слова: информационная безопасность, платежные системы, банковские карты, мошенничество.

ВВЕДЕНИЕ

Интенсивное внедрение банковских пластиковых карт в качестве инструмента безналичных расчетов за товары и услуги в России сопровождается, как и во всем мире, совершением ряда противозаконных действий, связанных с их использованием. Внедрение банковских карточек является важнейшей тенденцией развития технологии безналичных расчетов в банковской деятельности. Потому информационная безопасность такого способа расчетов становится одной из главных проблем защиты информационных ресурсов в экономических и финансовых информационных системах.

Карточки как финансовый инструмент постоянно совершенствуются, растет сфера их применения, расширяется комплекс оказываемых услуг с их использованием. С другой стороны, такая тенденция создает условия для совершения преступлений в сфере электронных платежных расчетов.

Так, ежегодная статья убытков, связанных со злоупотреблениями в этой сфере, составляет внушительную сумму. По результатам анализа, проведенного Computer Crime Research Center, ущерб от мошенничеств с использованием банковских пластиковых карт составил в 2013 году более 1 млрд. американских долларов, в том числе Master Card International потеряла из-за подделок самих карточек 213 млн. американских долларов, аналогичный показатель Visa International составил 380 млн. долларов.

Отдельные вопросы проблематики информационной безопасности платежных средств, в части организационно-правовых аспектов противодействия мошенничеству в кредитно-финансовой системе, рассматриваются в работах таких ученых как Гамза В. А., Балабанов И. Т., Васильеваа В. и других [1-3]. Однако возрастающая опасность данного рода преступлений, которые становятся все более изощренными благодаря стремительному научно-техническому прогрессу в области информационных технологий, требует проведения дальнейших научных исследований.

Цель исследования состоит в изучении проблематики информационной безопасности стремительно развивающихся платежных систем и разработка

рекомендаций противодействия мошенничеству в области электронных банковских расчетов.

ОСНОВНОЙ МАТЕРИАЛ

Бизнес на изготовлении и использовании поддельных пластиковых карточек приобрел в последние годы транснациональный характер. Лидерство здесь удерживает Юго-Восточная Азия, откуда осуществляется большинство операций.

За последние годы преступность в сфере оборота банковских пластиковых карт претерпела качественные изменения — от деяний, совершаемых одиночками и небольшими группами, до преступлений, совершаемых хорошо организованными группировками и преступными сообществами (численностью до 50 квалифицированные специалистов). На вооружении таких группировок находится самая современная техника, необходимые документы прикрытия.

На сегодняшний день из известных видов мошенничеств «лидирует» полная подделка карты. На заготовки полностью подделанных карточек наносятся логотип эмитента, поле для проставления подписи, точно воспроизводятся все степени защиты. В данном случае используются подлинные реквизиты существующих карт. На международном рынке в изготовлении и использовании поддельных пластиковых карт «лидирует» Юго-Восточная Азия, откуда осуществляется большинство операций. Активно действующие «филиалы» есть в Испании, Италии и Великобритании.

Вал преступлений в сфере оборота пластиковых карт грозит подорвать авторитет пластиковой карты как финансового инструмента. Недавний скандал с компрометацией банковских карт российских эмитентов побудил многих пользователей переходить на дорожные чеки.

В начале 21 века в сфере полных подделок банковских пластиковых карточек в Европе заметное место заняли преступные группировки выходцев из Африки. Африканцы используют подделки преимущественно для получения наличных денег непосредственно в банках. При этом они удостоверяют свою личность с помощью подделанных идентификационных документов. Используемые африканцами полные подделки изготавливаются в США (в Калифорнии неоднократно ликвидировались мастерские по производству фальшивок) [1].

Уровень незаконных операций с банковскими картами в Российской Федерации остается одним из самых низких в мире. Среди видов мошенничеств по-прежнему лидирует скимминг (доля скимминга составляет почти 50% в общем объеме мошеннических операций с картами Visa). Скимминг – один из наиболее популярных способов мошенничества с кредитными картами и воровства персональных данных. По данным ФБР только в Соединенных Штатах скимминг обходится честным держателям платежных карт в $8,5 млрд. Но если раньше суть мошенничества сосредотачивалась вокруг банкоматов, то теперь хакеры приняли на вооружение бесконтактные способы воровства – дистанционные, негласные и неотвратимые.

За последний год существенных изменений в уровне мошенничества с банковскими картами в России не произошло. Он по-прежнему остается на достаточно низком уровне (5 копеек на одну тысячу рублей).

В Украине уровень мошенничества в кредитной сфере банковской деятельности в 4-5 раз превышает среднемировой (наибольшее число приходится на Киев - 85%) [2].

В этой связи целесообразным будет представить международную классификацию мошенничества по видам правонарушений:

- мошенничество с утраченными и похищенными пластиковыми картами (74,2%);
- мошенничество с поддельными пластиковыми картами (22,5%);
- мошенничество с пластиковыми картами, не полученными законным держателем (2,7%);
- мошенничество с использованием счета (1,9%);
- другие формы мошенничества (3,6%).

Анализ наиболее распространенных схем мошенничества с банковскими картами в 2008-2013 гг. позволил представить следующую классификацию:

- заклеивание скотчем части банкомата, которая выдает деньги (часть кэш-диспенсера);
- получение информации о ПИН-коде карты;
- использование фальшивых банкоматов;
- копирование магнитной полосы (skimming);
- использование ложного ПИН-ПАД;
- фишинг (чаще всего используется в виде рассылки через Интернет писем от имени банка или платежной системы с просьбой подтвердить указанную конфиденциальную информацию на сайте организации);
- вишинг – новый вид мошенничества (голосовой фишинг, использующий технологию, позволяющую автоматически собирать информацию о номерах карт и счетов);
- неэлектронный фишинг (связан с осуществлением покупок в торговых организациях посредством обязательного ввода ПИН-кода);
- вирус, поражающий банкоматы;
- шимминг – новая «нанотехнология» кражи денег с банковских карт с помощью шиммера (устройства со светоотражательными частичками);
- использование телефона с возможностями NFC и особого приложения, имитирующего платежный терминал.

Новым видом киберпреступности в сфере электронных счетов является захват финансовых данных пользователей с использованием веб-страницы с фальшивым руководством по настройке безопасности. На компьютер заранее выбранной жертвы поступает сообщение, имеющее вид предупреждения системы безопасности провайдеров услуг, которые проводят платежные операции.

Внутри сообщения содержатся инструкции по повышению безопасности использования карт в Сети. На самом деле это руководство призвано вынудить жертву добровольно предоставить злоумышленникам банковские данные.

Вторая часть мошеннической схемы – это фишинговый сайт, который имитирует ресурс популярной платежной системы. На поддельном сайте пользователю предлагается пройти 3-шаговую процедуру активизации, которая предусматривает ввод пользователем имени, даты рождения, адреса местожительства, номера телефона и адреса электронной почты, а также данных о кредитной карте: номера, банка-эмитента, срока действия, кода подтверждения. После того, как жертва ввела все свои данные, они тут же попадают к злоумышленникам, которые могут использовать их как угодно по своему усмотрению [3].

Особую проблему информационной безопасности платежных средств представляет кардинг (организованное преступное сообщество, которое имеет свои сайты и форумы, на которых новички приобщаются к таинствам ремесла, а профессионалы обмениваются полезными советами). Кардерство, как преступление относится к категории так называемых латентных преступлений. И банки и интернет-магазины опасаются того, что подача заявления в правоохранительные органы может вызвать утечку информации и тогда разразится скандал, который приведет к потере клиентов и вероятному разорению. В 50% случаев владелец карточки также не будет обращаться к правоохранителям по двум причинам:

- опасение открыть свое финансовое положение;
- наличие возможности разобраться с самим магазином напрямую без вмешательства правоохранительных органов. В том случае, если пользователь карточки в состоянии доказать, что он не оформлял и не получал покупку, крайне велика вероятность того, что интернет-магазин вернет деньги, опять же боясь огласки [4].

Исследования проблем информационной безопасности платежных систем позволили выделить кардинг, как особый современный вид мошенничества, совершающегося в информационных и экономических сферах жизни нашей страны, отличающийся строго определенными вехами данного процесса, знание которых поможет построить эффективную систему противодействия хищению данных банковских карт [5].

1. Процедура получения мошенниками кредитных карт:

- регистрация параметров карты (номер, срок действия, иногда сверяет имя на карте с документом);
- обращение в центр обработки карт (процессинговый центр) за авторизацией транзакции (продавец сообщает, что он собирается совершить по данной карте транзакцию на сумму, скажем, $475);
- получение авторизации или отказа;
- регистрация числа авторизации (гарантия получения денег). При этом требуемая сумма считается уже потраченной, даже если хозяин карточки не совершает покупки.

Все вышесказанное справедливо как для покупки по карте «живьем», так и для покупки через Интернет или по телефону/факсу.

В итоге процедура характеризуется следующими признаками:

- продавец обращается не в банк, выдавший карту, а в местный центр обработки карт, который, как правило, в одном из местных банков;
- продавец не может узнать, сколько денег на счету. Он даже не может узнать, есть ли нужная ему сумма. Все, что он может, это попытаться получить авторизацию на нее;
- если продавец получил авторизацию на требуемую сумму, эта сумма на карточном счету замораживается. В случае легального использования карты это всего лишь мелкая неприятность, но становится проблемой при нелегальном использовании карты - уменьшается сумма, которую можно потратить, потому что аннулировать авторизацию практически невозможно.

2. Создание фейкового (поддельного) магазина (торгующего через Интернет, или порно сайт), взлом Интернет магазина, trashing (от англ. рытьё в мусоре) – в СНГ практически не применяется:

- создание легенды (название фирмы, род ее деятельности, имя руководителя компании и менеджера, который общается с «дропами»);
- размещение представительства фирмы в Интернете;
- поиск «дропов» («дропы» – граждане страны, в которой происходят закупки товаров по ворованным картам). Задача этих людей – получить вещи и переправить их в страну продаж. Предпочтительным для поиска «дропов» являются легальные онлайновые службы поиска. В качестве соискателя на позицию «менеджера или помощника по обработки корреспонденции «компании, занимающейся пересылкой товаров по всему миру», приглашаются люди, имеющие свободное время и готовые работать на дому;
- переписка кардера от имени менеджера с «дропом»;
- заключение договора (подложными документами занимаются отдельные «специалисты»);
- постепенное втягивание «дропа» в «бизнес компании». По данным самих кардеров, «срок жизни» такого наемника – 3-4 месяца, затем на него выходят представители органов власти. В странах продажи товаров кардеры предлагают покупателям ворованные вещи по цене на 30-70% ниже, чем в обычном магазине, но, разумеется, без гарантийного обслуживания.

3. Покупка и получение посылки кардером (с учетом платы местной таможне 50% от заявленной стоимости товара при получении посылки):

- кардеры звонят в нужную фирму и требуют чтобы при отправке груза курьерской компанией (FedEx / DHL / TNT / UPS) фирма обязала курьеров оплатить таможню. На посылке пишется CUSTOMS DUTY 50% PAID;
- курьерская компания в месте отправки выставляет магазину счет на сумму (сумма за перевозку + 50% от объявленной стоимости);
- магазин добавляет эту сумму в общий счет и снимает ее с карты. А курьерская компания в месте получения расплачивается с местной таможней самостоятельно. При этом получается, что таможенный сбор оплачен по той же карте;

•становление кардеров «своими» в курьерской фирме также происходит по строго определенному сценарию: а). Отправление посылки на произвольный адрес, фамилию и обращение в офис курьерской фирмы; б). Там спрашивают об отправлении на указанное имя. Конечно, в ответ им сообщают, что посылка в пути. Но они заходят на следующий день и снова спрашивают о ней. И так каждый день, даже по два раза; в). Спустя какое-то время их уже начинают узнавать в лицо, весь офис им сопереживает, и когда посылка доходит, ее отдают без проверки документов [6].

ВЫВОДЫ

Проведенные исследования проблематики информационной безопасности платежных систем позволили сформулировать ряд рекомендаций по противодействию мошенничеству в области электронных банковских расчетов:

1. Строгое выполнение владельцами пластиковых карт рекомендаций кредитной организации о мерах безопасности, перечень которых выдается при ее получении, а также проявление повышенной бдительности и осторожность в совершении операций с «пластиком»;
2. Использование сервиса Интернет-банкинг, позволяющего эффективно контролировать все списания с карты и, соответственно, оперативно отреагировать на нелегальные операции;
3. Использование карт с повышенным уровнем безопасности благодаря хранению части информации на специализированном микропроцессоре.

Список литературы

1. Гамза В. А. Безопасность коммерческого банка / В.А. Гамза, И.Б. Ткачук. – М., 2000. – 363 с.;
2. Ценова Т. Мошенничества в банковской сфере / Т. Ценова [Электронный ресурс]. – Режим доступа: http://newsland.com/news/detail/id/916726/
3. Балабанов И. Т. Банки и банковское дело: Банковская система; Лизинг и ипотека; Электронные платежи; Маркетинг в банках / И.Т. Балабанов. – СПб: Питер, 2002 – 267 с.;
4. Васильева В. Карты решают все / В. Васильева // Коммерсантъ-Деньги. – М., 2003. – №41. – С. 24-30;
5. Палютин А. Выбираем кредитную карту / А. Палютин // Рынок Ценных Бумаг. – М., 2002. – №21. – С. 33-45;
6. Бойченко О.В. Информационная безопасность платежных средств: проблема кардинга / О.В. Бойченко // Информационно-компьютерные технологии в экономике, образовании и социальной сфере: 3 межвуз. науч.-практ. конф.: тезисы докл. – Симферополь, 2008. – С. 59-61.

Статья поступила в редакцию 03. 02. 2014 г.