© Mazur V., Ivankevich O. Problems review of information security of the international payment systems // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 97-101.

ОБЗОР ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕЖДУНАРОДНЫХ ПЛАТЕЖНЫХ СИСТЕМ

Вера Мазур, Алексей Иванкевич

Национальный авиационный университет, Украина

МАЗУР Вера Ивановна, доцент НАУ

Год и место рождения: 1955 год, г. Киев, Украина.
Образование: Киевский политехнический институт (с 1995 года – Национальный технический университет Украины), 1981 год.
Должность: доцент кафедры международной информации с 2005 года.
Научные интересы: информационный бизнес, информационная и авиационная безопасность.
Публикации: более 60 научных публикаций, среди которых научные статьи, учебники, учебные пособия, учебно-методические издания.
E-mail: m_vi_55@mail.ru

ИВАНКЕВИЧ Алексей Викторович, к.т.н.

Год и место рождения: 1976 год, г. Киев, Украина.
Образование: Национальный авиационный университет, 1999 год.
Должность: доцент кафедры компьютерных систем и сетей с 2004 года, заместитель директора научно-технической библиотеки НАУ с 2009 года.
Научные интересы: высокопроизводительные вычисления, базы данных больших объёмов, глобальные информационные системы, наукометрия.
Публикации: более 70 научных публикаций, среди которых монографии, научные статьи, учебники, учебные пособия и патенты на изобретения.
E-mail: ntb@nau.edu.ua

Аннотация. *В статье рассматриваются проблемы обеспечения информационной безопасности в международных платежных системах. Проведен анализ систем и механизмов, призванных как гарантировать, так и повысить информационную безопасность Интернет-банкинга. Уделено внимание принципам организации информационной безопасности в международной платежной системе SWIFT. Рассмотрены особенности новой технологии 3D-Secure, которая существенно повышает уровень информационной безопасности международных карточных платежных систем. Проанализирован процесс имплементации технологии 3D-Secure в банковской сфере Украины. Рассмотрен достаточно обширный список технологических средств и мер, предпринимаемых для обеспечения безопасных расчетов с помощью международных платежных систем. Указано, что часто причиной мошеннического доступа к счетам пользователей является невнимательность и неосторожность самих пользователей.*

Ключевые слова: *международные платежные системы, информационная безопасность, SWIFT, безопасность Интернет-платежей, транзакции, карты Visa, MasterCard, Three-Domain Secure, технология 3D-Secure*

Введение

Меры обеспечения безопасности - установка межсетевых экранов и антивирусов, систем обнаружения вторжений и прочих, безусловно, необходимых средств, а также управление доступом, инцидентами, целостностью, непрерывностью, соответствием – это детали, из которых строится большая социотехническая система под названием «информационная безопасность».

Вопросам обеспечения информационной безопасности в компьютеризированных системах кредитно-финансовой сферы уделяется особое внимание.

Интенсивное развитие информационно-телекоммуникационных систем приводит к тому, что информационная среда, являясь определяющим фактором во всех сферах деятельности государства, становится центром устремлений со стороны криминальных структур. Со времени своего появления банковская сфера и платежные системы неизменно вызывали преступный интерес. И этот интерес связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в них сосредотачивается важная и зачастую закрытая

информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств.

Информационная преступность вышла на уровень, переводящий это явление в разряд наиболее серьезных и потенциально опасных национальных проблем. Ежегодные потери от нее в странах Западной Европы достигают 30 млрд. долларов, а в США – более 100 млрд. долларов. По официальным данным, предоставленным банками Национального банка Украины, общее количество мошеннических операций в 2013 году по сравнению с предыдущим увеличилось на 47%, а сумма убытков выросла на 20%. При этом эксперты отмечают, что 99,7% убытков, причиненных банкам по операциям с платежными картами, были осуществлены с картами международных платежных систем [1].

В последнее десятилетие рост убытков, связанный с информационной преступностью, стал устойчивой тенденцией. Общие риски функционирования платежных систем возникают из-за технических отказов и хищения денежных средств банков или клиентов. Другими словами, природа данного риска лежит в области технических особенностей работы систем, и его величина довольно значительна на сегодняшний день. Крупные платежные системы вынуждены закладывать в свои бюджеты расходные статьи с учетом возможных убытков от хищений, рассчитанные статистически на основе предыдущих периодов.

1. Принципы обеспечения информационной безопасности в международных платежных системах

Для обеспечения информационной безопасности международных платежных систем совокупность аппаратно–программных, организационно–технических средств и мер, реализующих систему безопасности, должны образовывать распределенный комплекс, функционирующий под контролем центров управления безопасностью.

Безопасность информации в информационно–телекоммуникационных сетях международных платежных систем обеспечивается выполнением следующих общих принципов: защита информации (с целью обеспечения ее конфиденциальности, целостности и достоверности) при ее хранении, обработке и передачи по сетям; подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь); обнаружение и предупреждение нарушения целостности объектов данных; устойчивость сети связи при компрометации части ключевой системы; защита технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки информации по побочным каналам и от возможно внедренных в технические средства электронных устройств съема информации; защита от несанкционированного доступа к информационным ресурсам и техническим средствам сетей, в том числе к средствам их управления; реализация организационно–технических мероприятий, направленных на обеспечение сохранности конфиденциальной информации [2].

В свете нынешних тенденций роста открытости технологий кредитно-финансовой сферы (использование Internet и других открытых сетей в качестве транспортных коммуникаций передачи данных) особую значимость приобретает вопрос обеспечения конфиденциальности, целостности и достоверности осуществляемых платежных транзакций.

Достичь этого можно только, используя криптографически стойкие и эффективно реализуемые криптосхемы, и организуя надежные и удобные системы распределения ключевой информации [3].

Банки стараются использовать различные системы и механизмы, призванные как гарантировать, так и повысить информационную безопасность использования Интернет-банкинга.

Некоторые банки предлагают клиентам Интернет-банкинга приобрести или взять в аренду специальное устройство — генератор одноразовых паролей. Генератор подключается к компьютеру через USB-порт и не требует специального программного обеспечения. Предлагается также использовать внешний электронный ключ, который генерируется при первом подключении к системе Интернет - банкинга, записывается на внешний носитель, а затем используется при проведении операций. Такие системы являются упрощенной версией электронной цифровой подписи.

Помимо перечисленных мер, банки зачастую применяют дополнительные меры для обеспечения безопасного пользования Интернет-банкингом:

- ограничение использования личного сертификата — система некоторых банков позволяет использовать электронный ключ или электронный сертификат только на том компьютере, на котором он был сгенерирован. Таким образом, осуществлять платежи через Интернет - банкинг можно только со своего личного компьютера, а просматривать выписки по счету можно и с помощью других устройств;
- виртуальная клавиатура — технология предназначена для того, чтобы мошенники не могли считывать регистрационные данные при вводе их с обычной клавиатуры с помощью вредоносного программного обеспечения;
- ограничение длительности сессии — в случае неактивности клиента сессия в системе Интернет-банкинга через определенное время будет закрыта. Для возобновления работы потребуется заново пройти аутентификацию;
- история подключений — с помощью этой функции пользователь Интернет-банкинга может отследить все несанкционированные операции [4].

На сегодняшний день практически всеми банками, предоставляющими услугу Интернет-банкинга, применяется стандарт SSL (Secure Socked Layer) — шифрование данных, передаваемых от компьютера пользователя в систему банка и обратно. Широко используемый и ставший практически

обязательным в Интернет-торговле протокол SSL позволяет всем участникам торговли спокойно передавать самую различную информацию. При попытке перехвата данных они будут закрыты шифром, взломать который невозможно за короткий промежуток времени.

Протокол SSL надежно защищает информацию, передаваемую через Интернет, но все же он не может уберечь частную информацию, хранимую на сервере продавца, — например, номера кредитных карт. Когда продавец получает данные кредитной карты вместе с заявкой на покупку, информация расшифровывается и сохраняется на сервере, пока заявка не будет выполнена. Если сервер не защищен и данные не зашифрованы, то возможен несанкционированный доступ к частной информации и дальнейшее использование ее в мошеннических целях.

В дополнение к использованию протокола шифрования передаваемых данных участники интернет-коммерции используют такие способы идентификации держателей карт, как проверка CVV2/CVK2-кодов (CVV2-код для карт платежной системы Visa и CVC2 — для MasterCard).

К интересным способам идентификации относится технология проверки адреса AVS (Address Verification Service). Она в большей степени характерна для североамериканского рынка электронной коммерции, но, тем не менее, с ней приходится сталкиваться и держателям карт российских и украинских банков, при использовании карт для оплаты товаров с доставкой на территории США.

2. Информационная безопасность в SWIFT

Наиболее известной и устойчивой из всех ныне существующих международных платежных систем является система SWIFT, которая получила широкое распространение в сфере международных межбанковских расчетов. С мая 1977 года, когда система начала функционировать, и до сегодняшнего дня число финансовых учреждений, пользующихся услугами этой системы, превзошло 10000 из 212 стран мира [5]. Число транзакций, пересылаемых этими учреждениями, составляет более 2,5 млрд ежегодно. В настоящее время пользователями услуг системы SWIFT в Украине являются 137 финансовых организаций. Первые восемь украинских банков были подключены к сети SWIFT еще в сентябре 1993 года [6].

Кроме того, система SWIFT может применяться для обмена информацией и осуществления взаиморасчетов при операциях с ценными бумагами и дорожными чеками. В перспективе предполагается использование данной системы и в других сферах экономики, где необходима оперативная, качественная среда для передачи финансово-значимой информации, требующая высокого уровня обеспечения конфиденциальности.

Многолетний успех системы SWIFT заключается в предоставлении широкого спектра услуг пользователям при передаче, хранении и обеспечении безопасности сообщений. Важным фактором также является своевременная поддержка пользователей в технических, административно-правовых, а также в вопросах обучения и консультирования при подключении новых пользователей. Но самое важное — высокий уровень ответственности перед пользователями за сохранность, своевременность и конфиденциальность передаваемой информации.

С технической точки зрения сеть представляет SWIFT собой международную телекоммуникационную сеть, позволяющую финансовым организациям из разных стран подключиться к ней, используя компьютеры и терминалы различных типов, для передачи банковской и финансовой информации. В системе принят особый формат банковских сообщений – стандарт, который развивается с помощью рабочей группы специалистов банков и самой организацией SWIFT. В системе SWIFT используются как международные стандарты, разработанные ISO, так и стандарты Международной торговой палаты (ICC).

В результате исторического развития сети SWIFT образована новая сеть – SWIFT II, которая базируется на 4-х уровневой сетевой архитектуре и на системе управления процессорами, находящимися в операционных центрах SWIFT.

Логическая архитектура системы SWIFT II подчиняется основным принципам установленным ISO (Международная организация стандартизации) для взаимодействия открытых систем. Активные компоненты архитектуры SWIFT II - узлы могут быть связаны между собой: прямыми выделенными линиями; местными (международными) коммутируемыми линиями; локальными сетями; спутниковыми каналами связи.

Архитектура системы состоит из четырех основных компонентов: SCP (процессор управления системой); SP (коммутационный процессор); RP (региональный процессор); CP (процессор передачи).

В настоящее время в системе SWIFT II была разработана и рекомендована Советом директоров для повсеместного использования улучшенная архитектура системы обеспечения безопасности, которая соответствует в широком смысле современному уровню развития телекоммуникационных технологий и криптографических методов. Основой нового подхода стало использование интеллектуальных карт (ICC), изменение алгоритма проверки достоверности и увеличение длины двухсторонних ключей, которыми обмениваются пользователи.

Фактически ядро системы SWIFT II сосредоточено в двух Центрах управления системой (SCC), которые расположены в Нидерландах и США. SCC включает в себя две ключевые компоненты системы, а именно SCP и SP. Для улучшения работоспособности и защиты от сбоев в системе SWIFT II применяется дублирование каждого SCP и резервирование работы каждого SP. В любое время только один SCP является активным и осуществляет непосредственное управление системой. Остальные

три SCP постоянно находятся в «горячем» резерве и непрерывно обновляют свое состояние по данным конфигурации активного SCP.

Все транзакции и сообщения, которые передаются по международным линиям связи систематически кодируются SWIFT с использованием шифров, действующих и меняющихся в течение произвольных промежутков времени.

3. Технология 3D-Secure

Нельзя обойти вниманием появление и широкое внедрение новой технологии 3D-Secure, которая существенно повышает уровень информационной безопасности международных карточных платежных систем [7].

По разным оценкам объем украинского рынка Интернет-торговли за прошедший год вырос более чем на 40%, превысив отметку в 10 млрд. долларов США. Потенциал роста огромен и фактически рынок E-commerce в Украине только начинает формироваться. По мнению экспертов, на сегодняшний день одним из сдерживающих факторов является недостаточный уровень развития инструментов электронного банкинга. Если платежные сервисы, такие как WebMoney, Qiwi, Яндекс-Деньги, еще пользуются спросом, то оплачивать Интернет-покупки банковскими картами Visa или MasterCard население отказывается по причине недоверия к уровню защищенности платежных транзакций.

Реагируя на сложившуюся ситуацию, платежная система Visa разработала новый протокол 3D-Secure, обеспечивающий безопасность Интернет-платежей по банковским картам.

Технология 3D-Secure позволяет проводить дополнительную аутентификацию держателя карты при проведении им платежей в сети Интернет на сайтах, поддерживающих данную технологию.

Название 3D-Secure происходит от английского термина Three-Domain Secure, указывающего на то, что данная технология реализована на основе трех доменов, в которых происходит порождение и проверка транзакций:

– домен эмитента, который поддерживает держателя карты и банк, выпускающий карты;

– домен эквайера, который поддерживает банк-эквайер и его клиентов;

– домен взаимодействия - содержит элементы, которые осуществляют проведение транзакций между двумя другими доменами, в основном этот домен поддерживает сети и сервисы карточных ассоциаций.

В процессе онлайн-проверки участвуют три независимые компании – банк продавца, на счет которого перечисляются деньги, банк покупателя и собственно платежная система. При оформлении платежа банковской картой в Интернет-магазине, поддерживающем данную технологию (определяется по наличию логотипа Verified By Visa), реквизиты покупателя перенаправляются на сервер банка-эмитента, выдавшего карту (банк также должен поддерживать данную технологию). Проверку подлинности владельца карты осуществляет банк, для этого используется пароль, известный только владельцу карты и банку. По результатам проверки банк-эмитент формирует ответное сообщение с использованием цифровой подписи с целью защиты информации от несанкционированных изменений.

Для ввода частной информации клиента, например, номера карты, используются защищенные страницы платежного сервера. Введенная информация сохраняется на платежном сервере, и получатель платежа не имеет доступа к этой информации, что наилучшим образом защищает от ее потери и хищения.

В результате у покупателя открывается диалоговое окно, в котором требуется ввести PIN-код (как в банкомате) или одноразовый пароль, присланный в виде SMS на номер контактного телефона (указывается при оформлении карты). После ввода пароля операция считается подтвержденной и происходит перечисление денежных средств с карты клиента на банковский счет магазина. Таким образом, если по какой-либо причине злоумышленники получили информацию о банковской карте, воспользоваться ею не удастся, поскольку подтвердить подлинность владельца карты без SMS-пароля не получится. Указанный пароль высылается непосредственно в момент совершения операции в Интернете после ввода реквизитов карты и может быть использован для подтверждения только один раз.

Такая система имеет ряд преимуществ. Во-первых, она достаточно проста в использовании — нет необходимости в специальном оборудовании, а процедура подтверждения операции занимает всего несколько минут. Во-вторых, она позволяет обезопасить учетную запись от использования злоумышленниками — даже если мошенникам станет известен логин и пароль для входа в систему, они не получат доступ к деньгам, а пользователь узнает о попытке провести несанкционированную операцию из SMS-сообщения [8-12].

Технология 3D-Secure не только обеспечивает безопасное проведение платежа, но и разграничивает риски участников транзакции за счет четкого разделения функций каждого.

Услуги, основанные на технологии 3D-Secure, также были приняты платежной системой MasterCard под названим MasterCard SecureCode (MCC) и японской платежной системой JCB International как J/Secure.

Выводы

С внедрением новой технологии 3D-Secure платежные системы Visa и MasterCard фактически уравняли степень защищенности Интернет-платежей с использованием банковских карт и платежей через сервисы, аналогичные WebMoney.

Вполне естественно, что технология новая, должного распространения еще не получила, и в Украине ряд продавцов продолжают принимать платежи «по старинке». Однако, опираясь на динамику подключения банков и соответственно Интернет-магазинов к 3D-Secure, можно

предположить, что в скором времени Интернет-платежи с банковских карт без подтверждения SMS-паролем станут недоступными. На наш взгляд, только в этом случае будет достигнут желаемый эффект – рост доверия граждан к онлайн-расчетам посредством карт Visa или MasterCard.

На сегодняшний день технологию 3D-Secure поддерживает большинство крупнейших банков Украины. Только в сентябре 2013 года новую технологию для держателей карт имплементировали три ведущих банка кредитно-финансовой сферы Украины - Райффайзен Банк Аваль, Пивденный, UniCredit Bank™ [13].

При достаточно обширном списке технологических средств и мер, предпринимаемых для обеспечения безопасных расчетов с помощью международных платежных систем, многое зависит от самих клиентов. Часто причиной мошеннического доступа к счетам пользователей является невнимательность и неосторожность самих пользователей. Поэтому, чтобы избежать возможных проблем, владельцам учетных записей необходимо беречь данные доступа к ним.

Литература

[1] Больше всего убытков банки несут при подделке карточек — НБУ. [Электронный ресурс] / Режим доступа: http://www.epravda.com.ua/rus/news/2013/02/10/360805/

[2] Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР. [Электр.ресурс] / Режим доступа: http://zakon2.rada.gov.ua/laws/show/537-v

[3] Про платіжні системи та переказ коштів в Україні. Закон України від 05.04.2001 № 2346-III (Редакція станом на 11.08.2013). [Электр. ресурс] / Режим доступа: http://zakon.rada.gov.ua/go/2346-14

[4] Резниченко Е. Безопасность Интернет-банкинга: практические аспекты. [Электр. ресурс] / Режим доступа: http://www.prostobank.ua/internet_banking/stati/

[5] Официальный сайт SWIFT. [Электр.ресурс] / Режим доступа: http://www.swift.com/about_swift/company_information/company_information

[6] Официальный сайт украинского отделения SWIFT. [Электр. ресурс] / Режим доступа: http://ukrswift.org/

[7] Официальный сайт банка Дистанционное Банковское Обслуживание. [Электр. ресурс] / Режим доступа: http:// www.bankdbo.ru/3-d-secure/

[8] Гончаров В.В. Безопасность и защита Интернет-платежей // Расчеты и операционная работа в коммерческом банке. — 2012. — № 4.

[9] Шаньгин В.Ф., Соколов А.В. Защита информации в распределенных корпоративных сетях и системах //Изд-во: ДМК. — 2002.

[10] Долгалева М.А. Интеграция системы международных расчетов Украины в глобальную платежную систему // Проблеми і перспективи розвитку банківської системи України: Збірник наукових праць. — 2005. — Т. 13. — С. 215-221.

[11] Усоскин В.М., Белоусова В.Ю. Мировые тенденции развития платежных систем //Деньги и кредит. — 2010. — №. 11. — С. 39-48.

[12] Обаева А.С. Национальная платежная система: инфраструктура, инновации, перспективы развития //Деньги и кредит. — 2010. — Т. 5. — С. 34-41.

[13] Официальный сайт Министерства Финансов Украины: раздел Новости. [Электр.ресурс] / Режим доступа: http://minfin.com.ua/2013/09/10/807265

УДК 004.056:331.211.54 (045)

Мазур В.І., Іванкевич О.В. Огляд проблем інформаційної безпеки міжнародних платіжних систем

Анотація. *В статті розглядаються проблеми забезпечення інформаційної безпеки в комп'ютеризованих системах кредитно-фінансової сфери. Проведено аналіз систем і механізмів, призначення яких полягає в підвищенні і гарантуванні інформаційної безпеки Інтернет-банкінгу. Приділено увагу принципам організації інформаційної безпеки в міжнародній платіжній системі SWIFT. Розглянуті особливості нової технології 3D-Secure, яка суттєво підвищує рівень інформаційної безпеки міжнародних карткових платіжних систем. Проаналізовано процес імплементації технології 3D-Secure в банківській сфері України. Розглянуто досить великий список технологічних засобів і заходів, що вживаються для забезпечення безпечних розрахунків за допомогою міжнародних платіжних систем. Зазначено, що часто причиною шахрайського доступу до рахунків користувачів є неуважність і необережність самих користувачів.*

Ключові слова: *міжнародні платіжні системи, інформаційна безпека, SWIFT, безпека Інтернет-розрахунків, транзакції, Visa, MasterCard, Three-Domain Secure, технологія 3D-Secure*

Mazur V., Ivankevich O. Problems review of information security of the international payment systems

Abstract. *Issues of information security in international payment systems are considered at the article. It is paid attention to principles of providing the information security at SWIFT international payment system. Specialties of 3D-Secure technology are reviewed. Specifications of new 3D-Secure technology, which significantly increases the level of information security of international card payment systems, are regarded. Process of 3D-Secure technology implementation to the bank system of Ukraine is analyzed. Adduce sufficient extensive list of technological means and measures taken to ensure the safety of payments with the help of international payment systems. Pointed out that often the cause of fraudulent access to the accounts of users is carelessness and negligence of the users themselves.*

Key words: *international payment systems, information security, SWIFT, security of Internet payments, transactions, Visa card, MasterCard, Three-Domain Secure, 3D-Secure technology*

Отримано *09 січня 2014 року*, затверджено редколегією *31 січня 2014 року*