УДК 681.322;003.26

ЗАЩИТА ИНФОРМАЦИИ В ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ

Йона Л.Г., Йона Е.О., Запороженко А.А.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная,1.
Одесский национальный экономический университет,
65082, Украина, г. Одесса, ул. Преображенская,8.
lyona@list.ru, eyona@mail.ru, sashynya1692@mail.ru

ЗАХИСТ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМАХ

Йона Л.Г., Йона О.О., Запороженко О.О.

Одеська національна академія зв`язку ім. О.С.Попова,
65029, Україна, м. Одеса, вул. Ковальська,1.
Одеський національний економічний університет,
65082, Україна, м. Одеса, вул. Преображенська,8.
lyona@list.ru, eyona@mail.ru, sashynya1692@mail.ru

INFORMATION SECURITY IN ELECTRONIC PAYMENT SYSTEM

Yona L.G.,Yona O.O., Zaporojenko O.O.

O.S. Popov Odessa National Academy of Telecommunications,
1 Kovalska St., Odessa 65029, Ukraine.
Odessa National Economic University
8 Preobrajenskaya St., Odessa 65029, Ukraine.
lyona@list.ru, eyona@mail.ru, sashynya1692@mail.ru

Аннотация. В статье рассматриваются технологии защиты информации в электронных платежных системах, в частности, решения на базе технологий SET и 3-D Secure. Приведена классификация систем электронных платежей, рассмотрены преимущества и недостатки данных технологий защиты.

Ключевые слова: защита электронных платёжных систем, криптографический протокол, технология SET, технология 3D Secure.

Анотація. У статті розглядаються технології захисту інформації в електронних платіжних системах, зокрема, рішення на базі технологій SET и 3D Secure. Наведено класифікацію систем електронних платежів, розглянуто переваги та недоліки наданих технологій захисту.

Ключові слова: захист електронних платіжних систем, криптографічний протокол, технологія SET, технологія 3D Secure.

Abstract. The article considers the technology of information security in electronic payment systems, particularly those that are based on SET technologies and 3D Secure. The classification of electronic payment systems and the review of advantages and disadvantages of before mentioned protection technologies are given below. The article considers the technology of information security in electronic payment systems, particularly those that are based on SET technologies and 3D Secure.

Key words: protection of electronic payment systems, cryptographic protocol, SET technologies, 3D Secure technology.

Развитие технологий электронных платежей предъявляет повышенные требования к обеспечению безопасности электронных платежных систем.

Прежде чем приступить к рассмотрению методов защиты электронных платежей, необходимо разобраться с основными понятиями платежной системы.

Электронной платежной системой (ЭПС) называется такая система, в которой в качестве платежного инструмента используются электронные пластиковые карты.

Электронная пластиковая карта – это платежный инструмент, который предоставляет его владельцу возможность безналичной оплаты товаров и услуг, а также получение наличных средств в банкоматах и отделениях банков.

К электронным пластиковым картам предъявляются требования уникальности и необратимости.

Требование уникальности означает, что карта должна содержать данные, позволяющие идентифицировать саму карту и ее владельца. Это достигается при помощи элементов защиты, которые наносятся на карту при ее изготовлении.

Требование необратимости подразумевает невозможность восстановления первичной информации, записанной на карту. Для этого вся информация хранится на карте в зашифрованном виде.

Банк, который заключил соглашение с ЭПС и получил соответствующую лицензию,

может выступать в качестве банка эмитента или банка эквайера.

Банк эмитент – выпускает пластиковые карты и гарантирует выполнение финансовых обязательств, связанных с использованием этих карт в качестве платежного инструмента.

Банк эквайер – осуществляет финансовые операции, связанные с выполнением расчетов и платежей точками обслуживания (предприятиями торговли и сервиса, отделениями банков, принимающих в качестве платежного инструмента пластиковую карту).

Проведение взаиморасчётов между банками эквайерами и эмитентами обеспечивается наличием в платежной системе расчетного банка. Все это возможно благодаря наличию в системе процессингового центра (организации, которая хранит сведения о лимитах держателей карт и рассылает итоговые данные для взаиморасчетов между банками, а также формирует стоп–листы для банков эквайеров и точек обслуживания).

Интернет эквайринг – общий термин, которым обозначается прием платежей по пластиковым картам через Интернет с использованием специально разработанного web-интерфейса. Чтобы расплатиться с помощью данной системы необходимо иметь кредитную карту, счет которой предназначен специально для оплаты товаров и услуг не только в интернете, но и в реальных магазинах.

Электронные деньги (которые записаны на счетах в банковских компьютерах и перемещаются по электронным сетям) не являются общепринятым платежным средством, они находятся только в рамках определенной ЭПС и обычно носят то же название, что и платежная система.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ. Проблемам исследования методов защиты информации в электронных платежных системах посвящены труды Балакирского В.Б. [1], Гайковича В.Ю., Першина А.С. [2], и др. По данной тематике были написаны также работы: “Криптографічний захист електронного документообігу” Йона Л.Г., Йона О.О., Терешко В.С.[3]; “Методи інформаційної безпеки в банківських і платіжних системах” Копичинська І.А. за Йони Л.Г. [4]; “Методи захисту інформації в системах електронної комерції” Запороженко О.О. за кер. Йони Л.Г. [5]. Поскольку технологии защиты информации стремительно развиваются, возникает необходимость дальнейшего исследования этого вопроса.

ОСНОВНАЯ ЧАСТЬ. В настоящее время на рынке сложно определить платежную систему, которая доминировала бы во всех направлениях, поэтому наличные деньги, чеки и реальные кредитные карты широко используются параллельно своим электронным аналогам. Платежные системы могут совершать операции как с безналичными платежами, так и с обычными наличными средствами.

Существует множество электронных платёжных систем, среди них такие, как Visa, MasterCard, EasyPay, Portmone, iPay или PayU, RBS, Webmoney, Yandex-Деньги, RBK-Money, PerfectMoney, Liberty-Reserve, PayPal, LiqPay и др.

Электронные платёжные системы делятся на несколько типов.

На рис. 1 представлена классификация электронных платёжных систем

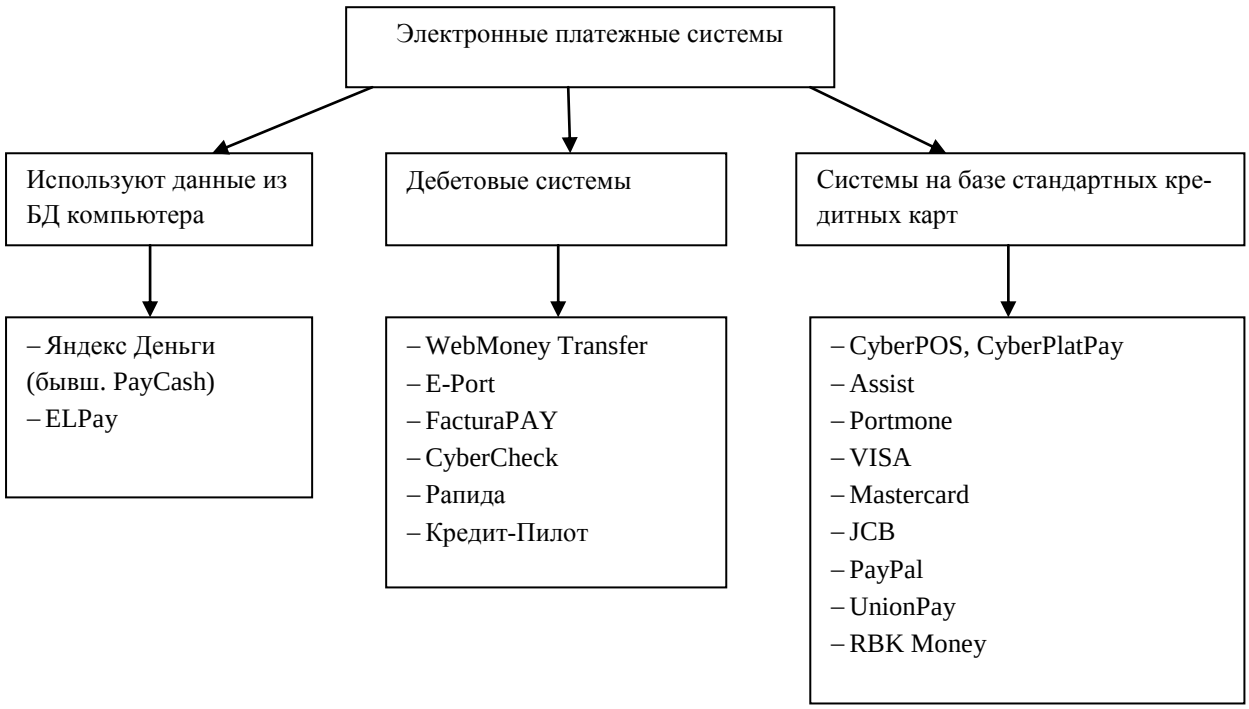

Рисунок 1 – Классификация электронных платёжных систем

Для того, чтобы владелец электронной карты мог без опасений осуществить платеж через сеть Интернет, необходимо иметь надежный механизм защиты прохождения электронных платежей. Для этого используются протоколы, использующие криптографическую защиту информации (шифрование данных, распределение ключей и использование цифровых подписей для аутентификации) [3].

Одним из таких протоколов является технология SET (Secure Electronic Transactions) “Безопасные электронные транзакции”, разработанная платёжными системами Visa и MasterCard . В данном протоколе для защиты транзакций при осуществлении электронных платежей используются процедуры шифрования и цифровой подписи. Протокол гарантирует, что при взаимодействии владельца пластиковой карты и продавца, информация о счете кредитной карты будет оставаться конфиденциальной (используется двойная цифровая подпись) [2].

Существует две схемы использования протокола SET.

В первой схеме используются открытые ключи, при этом каждый шаг реализации протокола SET сопровождается аутентификацией. Это не дает возможности злоумышленнику стать посредником и видоизменять данные транзакции. Для нормальной работы протокола SET все участники должны зарегистрироваться и передать партнерам свой открытый ключ.

Во второй схеме идентификация сторон производится путем обмена цифровыми сертификатами, удостоверяющими право участников сделки использовать пластиковые карты. При этом SET-сертификат магазина содержит идентификационные параметры торговой точки. SET-сертификат владельца карты несет в зашифрованном виде информацию об основных параметрах карты. Проведение оплаты с использованием SET- сертификата не требует от клиента ввода параметров его карты и не предусматривает получение продавцом данной конфиденциальной информации.

Система также позволяет осуществлять платежи с помощью пластиковых карт и без использования SET-сертификатов клиента, в случае, если клиенты такими сертификатами не располагают. В этом случае используется технология MIA SET (Merchant Initiated Authoriza-

tion). Для обеспечения безопасности платежей по технологии MIA SET, платежная система RBS предотвращает возможные мошеннические транзакции.

Преимуществом протокола SET является полная конфиденциальность сделки, однако главным недостатком остается большая стоимость внедрения этой технологии и дороговизна в использовании. Кроме того, уровень мошенничества в сети пока позволяет пользоваться более доступными протоколами.

Современный протокол 3D Secure лишён недостатков протокола SET, которые мешают его внедрению, он дешевле в реализации, удобнее в использовании и добавляет ещё один шаг аутентификации при осуществлении электронных платежей.

3D Secure является торговой маркой корпорации VISA. Компания VISA разработала его с целью повышении безопасности электронных платежей и предложила клиентам услугу Verified by Visa (VbV). Услуги, основанные на данном протоколе, также были приняты MasterCard под названием MasterCard Secure Code (MCC) и JCB International как J/Secure.

Протокол 3D Secure позволяет добавить к процессу финансовой авторизации проверку подлинности в режиме реального времени. Эта аутентификация основана на принципе трёх доменов (отсюда 3D в названии):

– домен эквайера (домен продавца и банка, в который перечисляются деньги);

– домен эмитента (домен владельца карты и банка, выдавшего карту);

– домен совместимости (домен, предоставляемый платёжной системой (MasterCard, Visa, CyberPlat и т. д.) для поддержки 3D Secure протокола).

При этом каждый из доменов выполняет свою функцию:

– эквайер – за корректный запрос и верный путь перенаправления владельца карты,

– эмитент отвечает за предоставление истинной информации о клиенте,

– платежная система – за сохранность данных.

При осуществлении платежа картой банка, поддерживающего протокол 3-D Secure, к ранее необходимой информации добавляется дополнительный запрос на подтверждение подлинности карты (обычно это одноразовый код подтверждения, который отправляется банком в sms-сообщении на мобильный телефон клиента).

Некоторые банки используют систему постоянных паролей (полученных при регистрации) и при совершении каждой электронной транзакции вводит именно его. Однако такой способ аутентификации является менее надёжным, чем одноразовый код подтверждения.

В технологии защиты 3D Secure имеются недостатки. Если в обычных транзакциях ответственность за операции по украденным картам несёт предприятие, на сайте которого была произведена покупка товара или услуги по украденной карте (при условии, что он не поддерживает технологию 3D Secure). В случае же транзакций, защищённых 3-D Secure, происходит так называемый “Перенос ответственности” (англ. Liability Shift), когда ответственность переносится на банк-эмитент, выпустивший карту, или на самого клиента.

Но все же главным недостатком технологии 3D Secure является то, что для защиты конфиденциальной информации используется криптографический протокол SSL/TLS, который имеет много уязвимостей.

Проводя сравнение технологий защиты электронных платежных систем SET и 3-D Secure, можно выделить их основные достоинства и недостатки. Преимуществом технологии SET является полная конфиденциальность сделки, а недостатками являются высокая стоимость внедрения и сложность использования данного протокола защиты. К преимуществам технологии 3D Secure можно отнести невысокую стоимость реализации и простоту использования. Однако, в технологии 3D Secure имеются свои недостатки. Это, в первую очередь, использование уязвимого криптографического протокола SSL/TLS и во вторую – “перенос

ответственности" на самого клиента (или на банк-эмитент), в случае использования злоумышленником украденной карты.

Подводя итог, можно сделать вывод о необходимости дальнейшего изучения и усовершенствовании технологий защиты электронных платежных систем.

ЛИТЕРАТУРА

1. Гайкович В.Ю., Безопасность электронных банковских систем: учебник / В.Ю. Гайкович, А.С. Першин. – М.: Единая Европа, 1994. – 354 с.

2. Балакирский В.Б. Безопасность электронных платежей / В.Б. Балакирский // Конфидент – 1996. – № 5. – С. 47–53.

3. Йона Л.Г. Криптографічний захист електронного документообігу / Л.Г. Йона, О.О. Йона, В.С. Терешко // Цифрові технології – Одеса. – 2013. – № 13. – С. 142–146.

4. Копичинська І.А. Методи інформаційної безпеки в банківських і платіжних системах / І.А. Копичинська; за керів. доц. Йони Л.Г. // Современные проблемы радиотехники и телекоммуникаций РТ-2014. – 2014. – С. 118.

5. Запороженко О.О. Методи захисту інформації в системах електронної комерції. / О.О. Запороженко за керів. доц. Йони Л.Г. // Современные проблемы радиотехники и телекоммуникаций РТ-2014. – 2014. – С. 119.

REFERENCES

1. Gaykovich, V., and A. Pershin. "Security of Electronic Banking Systems." *Threats to the Security of Automated Banking Systems* (1994): 186-89. Print.

2. V. Balakirskii Secure Electronic Payments / V. Balakirskii // Confident – 1996. – № 5. – 47–53 Print.

3. Yona, L., E Yona, and V. Tereshko. "Cryptography Security of Electronic Document Circulation." *Digital Technology* 13 (2013): 142-46. Print.

4. I. Kopichinska. "Means of Information Security in Banking and Payment Systems." *Modern Problems of Radio Engineering and Telecommunications* 10 (2014): 318. Print.

5. O. Zaporojenko. "Means of Information Security in Electronic Commerce." *Modern Problems of Radio Engineering and Telecommunications* 10 (2014): 319. Print.