1. УДК 004.056

ПОЛИТИКА БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ В СЕТИ ИНТЕРНЕТ

Кравчук Я.О., Деркунская Ю.В., Губенко Н.Е.
Донецкий национальный технический университет
E-mail: y.o.kravchuk@mail.ru

Аннотация

Кравчук Я.О., Деркунская Ю.В., Губенко Н.Е. Политика безопасности электронных платежных систем в сети интернет. *Рассмотрены требования и пути повышения информационной безопасности электронных платежных систем. Представлены сравнения надежности платежных систем.*

Общая постановка проблемы

С каждым годом пользователей интернета становится все больше. Множатся и расширяются многочисленные сервисы, внедряются новые технологии. Во Всемирную сеть вышла торговля, через интернет, стали предоставляться разнообразные платные услуги. Это вызвало развитие электронных платежных систем.

Система электронных платежей – это система безналичных расчетов, заключение контрактов и перевода денег между продавцами и покупателями, банками и их клиентами с помощью средств электронной коммуникации с применением средств кодировании информации и ее автоматической обработки.

Электронные платежные системы являются одним из самых популярных видов работы с электронной валютой. С каждым годом они развиваются все активнее, занимая довольно большую долю рынка по работе с валютой. Вместе с ними развиваются и технологии обеспечения их безопасности. Поскольку на сегодняшний день ни одна электронная платежная система не может существовать без хороших технологий и систем безопасности, которые в свою очередь обеспечивают безопасную транзакцию денежных операций.

В качестве исходных положений исследований использованы результаты, изложенные в работах В.А. Герасименко, А.А. Грушо, Д.П. Зегжды, А.М. Ивашко, Мельникова Ю.Н. и многих других.

Целью работы является повышение информационной безопасности электронных платежных систем в сети интернет.

Самих электронных платежных систем, собственно, как и технологий по защите, существует очень много. Каждая из них имеет различные принципы и технологии работы, а также свои достоинства и недостатки (таб.1).

Функционирование платежных систем в Интернете возможно только при обеспечении условий безопасности. Понятие "безопасность информации" можно определить как состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации. Решение проблемы безопасности основывается на криптографических или шифровальных системах, обеспечивающих следующие свойства:

- конфиденциальность - информация должна быть защищена от несанкционированного доступа как при хранении, так и при передаче. Доступ к информации может получить только тот, для кого она предназначена. Обеспечивается шифрованием;

– аутентификацию - необходимо однозначно идентифицировать отправителя, при однозначной идентификации отправитель не может отказаться от послания. Обеспечивается электронной цифровой подписью и сертификатом;
– целостность - информация должна быть защищена от несанкционированной модификации как при хранении, так и при передаче. Обеспечивается электронной цифровой подписью[4].

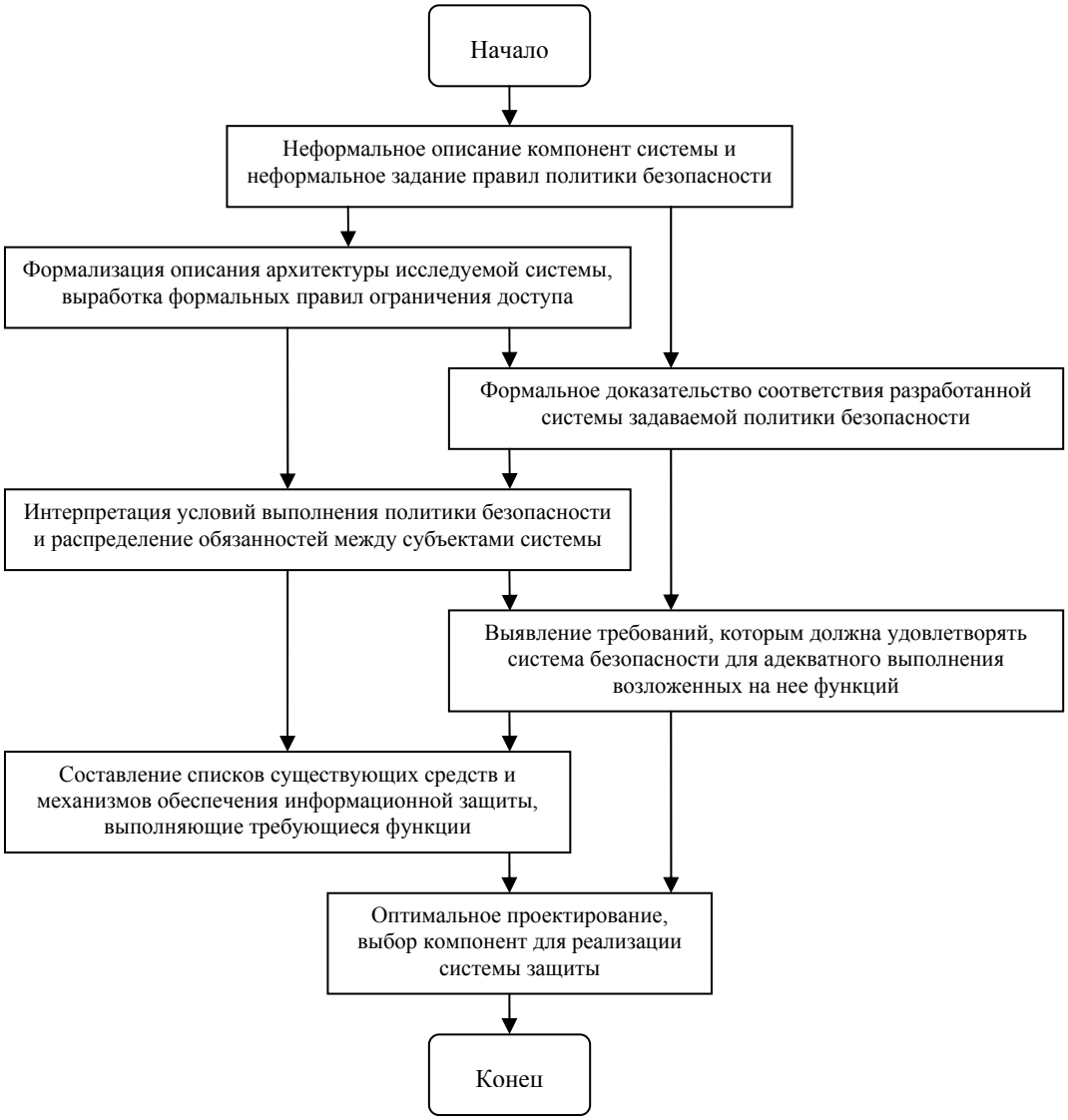

Рисунок 1 – Блок схема общего алгоритма построения системы защиты электронной платежной системы [2]

Гарантами безопасности платежных систем являются стандарты безопасности. Наиболее распространенными стандартами безопасности виртуальных платежей являются протокол SSL (Secure Socket Layer), обеспечивающий шифрование передаваемых через Интернет данных и стандарт SET (Secure Electronic Transactions).

Протокол SSL - стандарт, основанный на криптографии с открытыми ключами. Протокол обеспечивает защиту данных, передаваемых в сетях TCP/IP по протоколам приложений за счет шифрования и аутентификации серверов и клиентов. Это означает, что шифруется вся информация, передаваемая и получаемая Web-браузером, включая URL-адреса, все отправляемые сведения (такие как номера кредитных карт), данные для доступа к

закрытым Web-сайтам (имя пользователя и пароль), а также все сведения, поступающие с Web-серверов. Три основные функции безопасности, гарантированные в SSL, основаны на криптографии с открытым ключом.

Одной из основных причин медленного роста электронной коммерции является озабоченность покупателей надежностью средств, применяемых при выполнении платежей в Интернете. Описанный выше протокол SSL позволяет решить часть названных проблем безопасности, однако его роль в основном ограничивается обеспечением шифрования передаваемых данных. Поэтому для комплексного решения перечисленных выше проблем была разработана спецификация и создан набор протоколов, известные как стандарт SET (Secure Electronic Transaction - Безопасные электронные транзакции).

В основе системы безопасности, используемой стандартом SET, лежат стандартные криптографические алгоритмы DES и RSA. Инфраструктура SET построена в соответствии с инфраструктурой открытого ключа (Public Key Infrastructure - PKI) на базе сертификатов, соответствующих стандарту X.509 организации по стандартизации (ISO). Главная особенность SET - регламентация использования системы безопасности, которая устанавливается международными платежными системами[5].

Таблица 1 - Сравнительная таблица надежности платежных систем [4].

Характеристика	**WebMoney**	**«Яндекс.Деньги»**	**CyberPlat**	**E-port**
Аутентификация с использованием токенов	Есть	Нет	Нет	Нет
Многофакторная аутентификация	Пароль + файл-ключ	Пароль + программа-кошелек	Нет	Нет
Шифрование	Алгоритм типа RSA, ключ 1024 бита	Алгоритм RSA, ключ 1024 бита	Алгоритм RSA, ключ 512 бит	Технология SSL 3.0, ключ от 40 до 128 бит
Наличие SMS-сервиса	Есть	Нет	Нет	Есть
Возможность перевода средств между частными клиентами	Есть	Есть	Нет	Нет
Анонимность частных клиентов	Есть	Есть	Нет	Есть
Система blacklist	Есть	Нет	Нет	Нет
Дополнительные средства защиты от мошенников	Аттестация, арбитраж	Нет	Нет	Нет

Поскольку Интернет одновременно является и чрезвычайно эффективным коммуникативным средством и средой, вызывающей достаточно большое недоверие у

пользователей, безопасность электронных платежей является весьма серьезным критерием успеха конкретной системы и использующего ее электронного бизнеса. Важно, чтобы при любой реализации в системе не оставалось плохо защищенных участков, способных привести к крупномасштабному мошенничеству. Поэтому основными требованиями по безопасности являются:

- исключения возможности списания средств с аккаунта плательщика третьими лицами;
- обеспечение возможности легитимного подтверждения плательщиком перед третьими лицами (например, судом) факта совершения платежа, его получения получателем и назначения данного платежа (например, получения товара надлежащего качества);
- обеспечение возможности легитимного подтверждения получателем перед третьими лицами факта получения платежа и его назначения;
- обеспечение возможности легитимного подтверждения эмитентом факта проведения всех авторизованных транзакций по данному аккаунту действительным владельцем данного аккаунта;
- обеспечение гарантий, что перемещаемая с аккаунта сумма не будет украдена в момент передачи и попадет точно и исключительно по назначению;
- исключение возможностей подделки квитанций эмитента пользователям;
- обеспечение разрешения всех спорных вопросов между эмитентом и пользователями исключительно электронным образом с помощью сообщений с цифровой подписью;
- обеспечение возможности разрешения спорных вопросов между пользователями без участия эмитента; система в целом должна быть устойчива к мошенническим действиям, в том числе - в случае форс-мажорных обстоятельств[3].

Выводы

Решение проблемы информационной безопасности электронных платежных систем в сети интернет является наиболее важной составляющей обеспечения экономической безопасности электронного бизнеса. Протокол SET является на сегодняшний день одним из лучших открытых и устойчивых протоколов в электронных платежных системах.

Выбор механизмов, которые реализуют данные функции безопасности, осуществляется с использованием методов оптимального проектирования. Подобное решение задачи позволяет экономически эффективно построить систему защиты определенного уровня, предоставляет возможность учесть различные ограничения, вводимые разработчиком или заказчиком системы.

Список литературы

1. Головеров Д.В., Кемрадж А.С. и др. Правовые аспекты использования Интернет-технологий. М.: Книжный мир, 2008.
2. Деднев М. А., Дыльнов Д. В., Иванов М. А. Защита информации в банковском деле и электронном бизнесе. – М.: ИД КУДИЦ-ОБРАЗ, 2004.- 512с.
3. http://www.ram.ru/ - сайт российской ассоциации маркетинга (РАМ).
4. http://www.e-commerce.ru/ - Интернет-ресурсы информационно-консалтингового центра по электронному бизнесу.
5. http://www.e-management.ru/ - консультационный центр развития электронного бизнеса.