УДК 004.738.5

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ЭЛЕКТРОННОЙ КОММЕРЦИИ НА ОСНОВЕ ПРОТОКОЛОВ SET И SSL

**Губенко Н.Е.[1)], Кайдановский К.А.[2)], Левитасова В.Б.[3)]**
*Донецкий национальный технический университет*
*[1)] к.т.н., доцент; [2,3)] студенты*

## I. Постановка проблемы

Широкое внедрение IT-технологий и Internet не могло не отразиться на развитии электронного бизнеса. Одним из видов электронного бизнеса является электронная коммерция. В соответствии с документами ООН, бизнес признается электронным, если хотя бы две его составляющие из четырех (производство товара или услуги, маркетинг, доставка и расчеты) осуществляются с помощью Internet. Поэтому в такой интерпретации обычно полагают, что покупка относится к электронной коммерции, если, как минимум, маркетинг (организация спроса) и расчеты производятся средствами Internet. Более узкая трактовка понятия "электронная коммерция" характеризует системы безналичных расчетов на основе пластиковых карт [1].

## II. Цель работы

Целью исследования является сравнение двух наиболее распространённых протоколов защиты электронной коммерции.

## III. Особенности работы протоколов SET и SSL

Ключевым вопросом для внедрения электронной коммерции является безопасность. Платежные системы являются наиболее критичной частью электронной коммерции, и будущее их присутствия в сети во многом зависит от возможностей обеспечения информационной безопасности и других сервисных функций в Internet. SET и SSL - это два широко известных протокола передачи данных, каждый из которых используется в платежных системах Internet [1].

Протокол SET (Secure Electronic Transaction) предназначен для защиты электронных платежей в Internet с помощью платежных карточек. Спецификации SET были разработаны по инициативе MasterCard и Visa International в 1997 году. Протокол SET является протоколом верхнего уровня, и имеет довольно простую структуру (рис. 1) [2].

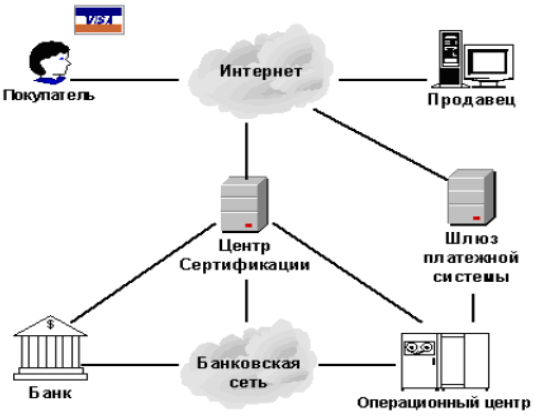


Рисунок 1 - Структура протокола SET

Все операции, осуществляемые через протокол SET, производятся в зашифрованном виде, что способствует повышенной конфиденциальности транзакций. Протокол SET позволяет безопасно передавать платежные данные покупателя продавцу и реализует другие операции по защите предоставленной информации:

- обеспечивает секретность данных оплаты и конфиденциальность информации заказа, переданной вместе с данными об оплате;
- сохраняет целостность данных платежей при помощи цифровой подписи;
- содержит специальную криптографию с открытым ключом для проведения аутентификации;
- имеет аутентификацию держателя по кредитной карточке, которая обеспечивается применением цифровой подписи и сертификатов держателя карточек;

- имеет аутентификацию продавца и его возможности принимать платежи по пластиковым карточкам с применением цифровой подписи и сертификатов продавца;

- выдаёт подтверждение того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым карточкам через связь с процессинговой системой;

- гарантирует безопасность передачи данных посредством преимущественного использования криптографии [1].

Криптографический протокол SSL (Secure Socket Layer) был разработан в 1996 году компанией Netscape и вскоре стал наиболее популярным методом обеспечения защищенного обмена данными через Internet. Этот протокол интегрирован в большинство браузеров и Web-серверов и использует ассиметричную криптосистему с открытым ключом, разработанную компанией RSA (рис. 2) [3].

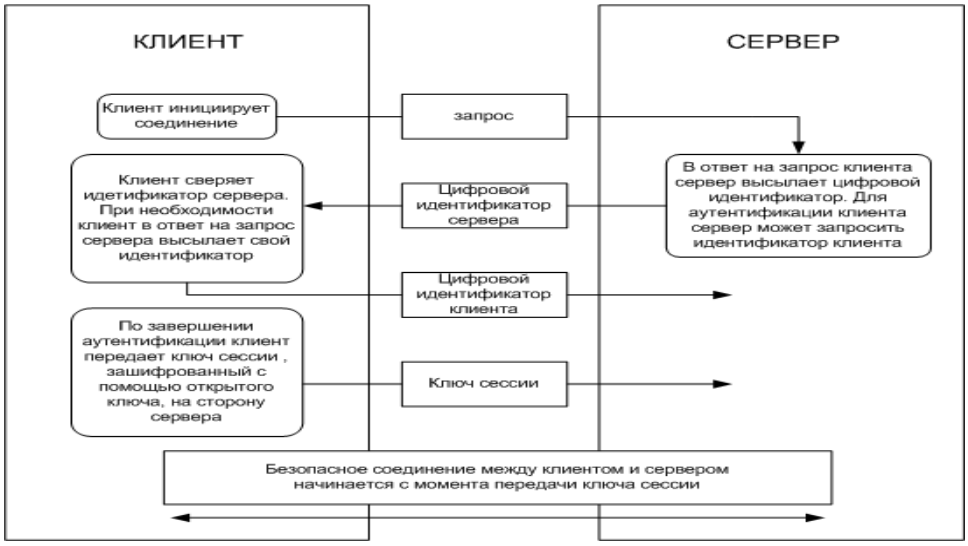


Рисунок 2 - Структура протокола SSL

Протокол SSL для распространения публичных ключей использует специальную форму – сертификат, который содержит:

- имя человека/организации, выпускающей сертификат;
- субъект сертификата (для кого был выпущен данный сертификат);
- публичный ключ субъекта;
- некоторые временные параметры (срок действия сертификата и т.п.).

SSL на сегодня является наиболее распространенным протоколом, используемым при построении систем электронной коммерции. С его помощью осуществляется 99% всех транзакций. Широкое распространение SSL объясняется в первую очередь тем, что он является составной частью всех браузеров и Web-серверов. Другое достоинство SSL - простота протокола и высокая скорость реализации транзакции [1].

**Вывод**

На основании изложенного материала можно с уверенностью утверждать, что протокол SET обеспечивает защиту значительно лучше протокола SSL, так как протокол SSL не аутентифицирует продавца и покупателя, а также не обеспечивает конфиденциальности информации о карте пользователя для продавца. То есть, нет возможности определить достоверность информации о субъектах сделки, а продавец при желании без проблем может воспользоваться данными о реквизитах карты покупателя в корыстных целях. Использование протокола SET позволяет избежать всех этих угроз. Однако SET-протоколы используются очень редко, в основном крупными фирмами, которые могут себе позволить тратить большие деньги на информационную безопасность (использование SET обходится гораздо дороже, чем использование SSL). Но учитывая высокий уровень мошенничества в сети Internet, можно сделать прогноз, что протокол SET в будущем станет ведущим протоколом обеспечения безопасности электронной коммерции.

**Список использованных источников**

1. Безопасность электронной коммерции. Электронный ресурс. Режим доступа: http://protect.htmlweb.ru/sslset3d.htm.
2. Электронная коммерция: теория и практические выкладки. Электронный ресурс. Режим доступа: http://www.toppayingcontents.com/praktik1_2.html.
3. Протокол SSL – что это такое? Электронный ресурс. Режим доступа: http://www.inssl.com/about-ssl-protocol.html.