**4. Обеспечение безопасности в системах электронной коммерции**

Электронная коммерция предполагает взаимодействие между партнерами посредством информационных технологий, что существенно повышает гибкость, эффективность и масштабность бизнес-процессов.

**Информационная технология** – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

В системах электронной коммерции проведение транзакций обеспечивается посредством автоматизированных банковских систем реализующих механизм контроля доступа клиентов банка к их счетам, причем такой доступ выполняется владельцем удаленно, т.е. без физического присутствия в офисе банка, что требует соответствующих процедур обеспечения безопасности.

Таким образом, для реализации удаленного доступа необходимо выполнить последовательно следующие процедуры:

1. **Идентификация** - процесс присвоения уникального признака субъекту, по которому он в последствии будет опознан автоматизированной системой;

2. **Аутентификация** - проверка подлинности идентификатора субъекта;

3. **Авторизация** - предоставление субъекту прав доступа к объекту.

Указанные процедуры поддерживаются в автоматизированных системах **ядром безопасности** - элементы аппаратного и программного обеспечения, защищенные от модификации и проверенные на корректность, которые разделяют все попытки доступа субъектов к объектам.

Таким образом, **идентификатор** – это определенный вид информации, предоставляемый субъектом системе при его аутентификации. Такой информацией являются:

1. Пароль - отличительная характеристика субъекта представляющая собой секретную информацию, которая неизвестна непосвященным людям.

2. Устройство аутентификации - некоторый уникальный предмет, находящийся у субъекта и являющийся его отличительной характеристикой (например, смарт-карты, OTP-токены и т.д.).

3. Биометрия - измеримая физиологическая или поведенческая черта живого человека.

В настоящее время широко распространены в системах электронной коммерции парольная аутентификация (информация вводима с клавиатуры) и устройства аутентификации (банковские платежные карты).

Для аутентификации участников систем электронной коммерции может использоваться протокол Kerberos, который предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные средства. Каждый субъект обладает секретным ключом. Чтобы субъект C мог доказать свою подлинность субъекту S (без этого S не станет обслуживать C), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. C не может просто послать S свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что S не знает (и не должен знать) секретный ключ C. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в проверке подлинности.

Чтобы с помощью Kerberos получить доступ к S (обычно это сервер), C (как правило – клиент) посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый билет, зашифрованный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента. Клиент должен расшифровать вторую часть данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент – именно тот, за кого себя выдает. При этом секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) – они только использовались для шифрования (рисунок 5.5).

|  |
| --- |
| 10-1  Рисунок 5.5. – Схема проверки сервером S подлинности клиента C |

Взаимодействие участников системы электронной коммерции включает в себя не только операции, связанные с куплей-продажей товаров и услуг, но и операции, направленные на поддержку извлечения прибыли, - создание спроса на товары и услуги, поддержку клиентов после продажи и т.п. (рисунок 5.6.).

|  |
| --- |
| Рис 2  Рисунок 5.6. – Схема взаимодействия участников системы электронной коммерции |

Платежные средства способствуют обмену товаров и услуг и отвечают специфическим требованиям. Каждое средство имеет свою социальную и технологическую историю, определяющую их использование в специфических областях. На сегодняшний день банки предлагают большое количество платежных средств, связанных с автоматической обработкой транзакций и постепенной дематериализацией денег, отличающихся по способу применения в разных странах.

Можно выделить следующие виды платежных средств:

‑ наличные (в форме металлических монет или бумажных банкнот);

‑ кредитные переводы;

‑ прямое дебетование;

‑ межбанковские переводы;

‑ платежные карты (кредитные или дебетовые).

Развивающиеся виды платежных средств основаны на дематериализованных деньгах, хранящихся в смарт-картах, электронных или виртуальных кошельках.

Для обеспечения безопасности транзакций в сети Интернет используются различные протоколы, наиболее известными из которых являются SSL и SET.

Самый известный протокол Интернета ‑ SSL (Secure Socket Layer). Этот протокол был разработан компанией Netscape и является составной частью всех известных Интернет-браузеров и Web-серверов (сегодня используется версия 3.0 протокола SSL). Протокол реализуется между транспортным и сеансовым уровнями эталонной модели взаимодействия открытых систем (OSI). Это, с одной стороны, означает возможность использования протокола для организации защищенной сессии между программами, работающими по различным протоколам прикладного уровня OSI (FTP, SMTP, Telnet, HTTP и т.п.), а с другой ‑ закрытие любых данных, передаваемых в SSL-сессии, что приводит к снижению производительности протокола.

Последняя версия протокола SSL поддерживает режимы аутентификации:

‑ взаимную аутентификацию сторон;

‑ одностороннюю аутентификацию сервера (без аутентификации клиента).

Как следует из описания протокола SSL, асимметричные алгоритмы шифрования используются только на этапе установления защищенной сессии. Для защиты информационного обмена от несанкционированного доступа используются только симметричные алгоритмы. Это делается в первую очередь для того, чтобы повысить производительность протокола SSL.

Достоинства протокола:

1. Широкое распространение протокола SSL, которое объясняется в первую очередь тем, что он является составной частью всех известных Интернет-браузеров и Web-серверов. Это означает, что фактически любой владелец карты, пользуясь стандартными средствами доступа к Интернету, получает возможность провести транзакцию с использованием SSL;

2. Простота протокола для понимания всех участников ЭК;

3. Хорошие операционные показатели (скорость реализации транзакции). Последнее достоинство связано с тем, что протокол в процессе передачи данных использует только симметричные протоколы шифрования.

Недостатками протокола SSL в приложении к ЭК являются:

1. Отсутствие аутентификации клиента Интернет-магазином, поскольку сертификаты клиента в протоколе почти не используются. Использование «классических» сертификатов клиентами в схемах SSL является делом практически бесполезным. Такой «классический» сертификат, полученный клиентом в одном из известных центров сертификации, содержит только имя клиента и, что крайне редко, его сетевой адрес.

2. Протокол SSL не позволяет аутентифицировать клиента обслуживающим банком.

3. При использовании протокола SSL торговое предприятие (ТП) аутентифицируется только по своему адресу в Интернете (URL). Это значит, что клиент, совершающий транзакцию ЭК, не аутентифицирует ТП в полном смысле. Аутентификация ТП только по URL облегчает мошенническим ТП доступ к различным системам ЭК. В частности, торговые предприятия, занимающиеся сбором информации о картах клиентов, могут получить сертификат в каком-либо известном центре сертификации общего пользования на основании только своих учредительных документов.

4. Протокол SSL не поддерживает цифровой подписи, что затрудняет процесс разрешения конфликтных ситуаций, возникающих в работе платежной системы (цифровая подпись используется в начале установления SSL-сессии при аутентификации участников сессии). Для доказательства проведения транзакции требуется либо хранить в электронном виде весь диалог клиента и ТП (включая процесс установления сессии), что дорого с точки зрения затрат ресурсов памяти и на практике не используется, либо хранить бумажные копии, подтверждающие получение клиентом товара.

5. При использовании SSL не обеспечивается конфиденциальность данных о реквизитах карты для ТП.

Для операций с кредитными карточками используется протокол SET (Secure Electronic Transactions), разработанный совместно компаниями Visa, MasterCard, Netscape и Microsoft.

В отличие от SSL протокол SET узко специализирован. Целью SET является обеспечение необходимого уровня безопасности для платежного механизма, в котором участвует три или более субъектов. При этом предполагается, что транзакция реализуется через Интернет.

На базовом уровне SET осуществляет следующие функции:

**Аутентификация.** Все участники кредитных операций идентифицируются с помощью электронных подписей. Это касается клиента-покупателя, продавца, банка, выдавшего кредитную карточку, и банка-продавца.

**Конфиденциальность.**Все операции производятся в зашифрованном  
виде.

***Целостность сообщений.*** Информация не может быть подвергнута модификации по дороге, в противном случае это будет сразу известно.

**Совместимость.**Должна быть предусмотрена совместимость с любыми программными продуктами и с любыми сервис-провайдерами.

**Независимость от транспортного протокола.** Безопасность операций не должна зависеть от уровня безопасности транспортного протокола. Такие гарантии особенно важны, так как протокол SET ориентирован для работы в Интернет.