Федеральное агентство по образованию

ГОУВПО “Удмуртский государственный университет”

Факультет информационных технологий и вычислительной техники

Реферат

по курсу «Корпоративные информационные системы»

# на тему: «Электронная торговля: безопасность хранимой и передаваемой информации ».

выполнил:

студент 5 курса

группы ИС-51

Шевнин Е.С.

проверил:

Романенко В.

Ижевск 2010

# Безопасность электронной коммерции

Широкое внедрение Интернета не могло не отразиться на развитии электронного бизнеса.

Одним из видов электронного бизнеса считается 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 Интернета. Поэтому в такой интерпретации обычно полагают, что покупка относится к электронной коммерции, если, как минимум, маркетинг (организация спроса) и расчеты производятся средствами Интернета. Более узкая трактовка понятия "электронная коммерция" характеризует системы безналичных расчетов на основе пластиковых карт.

Ключевым вопросом для внедрения электронной коммерции является безопасность.

Высокий уровень мошенничества в Интернете является сдерживающим фактором развития электронной коммерции. Покупатели, торговля и банки боятся пользоваться этой технологией из-за опасности понести финансовые потери. Люди главным образом используют Интернет в качестве информационного канала для получения интересующей их информации. Лишь немногим более 2% всех поисков по каталогам и БД в Интернете заканчиваются покупками.

Приведем классификацию возможных типов мошенничества в электронной коммерции:

* транзакции (операции безналичных расчетов), выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т.п.);
* получение данных о клиенте через взлом БД торговых предприятий или путем перехвата сообщений покупателя, содержащих его персональные данные;
* магазины-бабочки, возникающие, как правило, на непродолжительное время, для того, чтобы исчезнуть после получения от покупателей средств за несуществующие услуги или товары;
* увеличение стоимости товара по отношению к предлагавшейся покупателю цене или повтор списаний со счета клиента;
* магазины или торговые агенты, презназначенные для сбора информации о реквизитах карт и других персональных данных покупателя.

## 

## Протокол SSL

Протокол ***SSL*** (Secure Socket Layer) был разработан американской компанией Netscape Communications. SSL обеспечивает защиту данных между сервисными протоколами (такими как HTTP, NNTP, FTP и т.д.) и транспортными протоколами (TCP/IP) с помощью современной криптографии в соединениях "точка-точка". Ранее можно было без особых технических ухищрений просматривать данные, которыми обмениваются между собой клиенты и серверы. Был даже придуман специальный термин для этого - "sniffer".

Протокол SSL предназначен для решения традиционных задач обеспечения защиты информационного взаимодействия:

* пользователь и сервер должны быть взаимно уверены, что они обмениваются информацией не с подставными абонентами, а именно с теми, которые нужны, не ограничиваясь паролевой защитой;
* после установления соединения между сервером и клиентом весь информационный поток между ними должен быть защищен от несанкционированного доступа;
* и наконец, при обмене информацией стороны должны быть уверены в отсутствии случайных или умышленных искажений при ее передаче.

Протокол SSL позволяет серверу и клиенту перед началом информационного взаимодействия аутентифицировать друг друга, согласовать алгоритм шифрования и сформировать общие криптографические ключи. С этой целью в протоколе используются двухключевые (ассиметричные) криптосистемы, в частности, RSA.

Конфиденциальность информации, передаваемой по установленному защищенному соединению, обеспечивается путем шифрования потока данных на сформированном общем ключе с использованием симметричных криптографических алгоритмов (например, RC4\_128, RC4\_40, RC2\_128, RC2\_40, DES40 и др.). Контроль целостности передаваемых блоков данных производится за счет использования так называемых кодов аутентификации сообщений (Message Autentification Code, или MAC), вычисляемых с помощью хэш-функций (например [MD5](http://web-protect.net/ecp.htm#MD5)).

Протокол SSL включает два этапа взаимодействия сторон защищаемого соединения:

* установление SSL-сессии;
* защита потока данных.

На этапе установления SSL-сессии осуществляется аутентификация сервера и (опционально) клиента, стороны договариваются об используемых криптографических алгоритмах и формируют общий "секрет", на основе которого создаются общие сеансовые ключи для последующей защиты соединения. Этот этап называют также "процедурой рукопожатия".

На втором этапе (защита потока данных) информационные сообщения прикладного уровня нарезаются на блоки, для каждого блока вычисляется код аутентификации сообщений, затем данные шифруются и отправляются приемной стороне. Приемная сторона производит обратные действия: расшифрование, проверку кода аутентификации сообщения, сборку сообщений, передачу на прикладной уровень.

Наиболее распространенным пакетом программ для поддержки SSL является SSLeay. Он содержит исходный код на C, который может быть встроен в такие приложения, как Telnet и FTP.

В SSL используется криптография с открытым (публичным) ключом, также известная как асимметричная криптография. Она использует два ключа: один - для шифрования, другой - для расшифровывания сообщения. Два ключа математически связаны таким образом, что данные, зашифрованные с использованием одного ключа, могут быть расшифрованы только с использованием другого, парного первому. Каждый пользователь имеет два ключа - открытый и секретный (приватный). Пользователь делает доступным открытый ключ любому корреспонденту сети. Пользователь и любой корреспондент, имеющий открытый ключ, могут быть уверены, что данные, зашифрованные с помощью открытого ключа, могут быть расшифрованы только с использованием секретного ключа.

Если два пользователя хотят быть уверенными, что информацию, которой они обмениваются, не получит третий, то каждый из них, должен передать одну компоненту ключевой пары (а именно открытый ключ), другому и хранит другую компоненту (секретный ключ). Сообщения шифруются с помощью открытого, расшифровываются только с использованием секретного ключа. Именно так сообщения могут быть переданы по открытой сети без опасения, что кто-либо сможет прочитать их.

Целостность и аутентификация сообщения обеспечиваются использованием электронной цифровой подписи.

Теперь встает вопрос о том, каким образом распространять свои публичные ключи. Для этого (и не только) была придумана специальная форма - сертификат. Сертификат состоит из следующих частей:

* 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.).

Сертификат "подписывается" приватным ключом человека (или организации), который выпускает сертификаты. Организации, которые производят подобные операции называются Certificate authority (CA). Если в стандартном Web-браузере, который поддерживает SSL, зайти в раздел security, то там можно увидеть список известных организаций, которые "подписывают" сертификаты. Технически создать свою собственную CA достаточно просто, но также необходимо уладить юридическую сторону дела, и с этим могут возникнуть серьезные проблемы.

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.

В то же время, SSL обладает рядом существенных недостатков:

* покупатель не аутентифицируется;
* продавец аутентифицируется только по URL;
* цифровая подпись используется только при аутентификации в начале установления SSL-сессии. Для доказательства проведения транзакции при возникновении конфликтных ситуаций требуется либо хранить весь диалог покупателя и продавца, что дорого с точки зрения ресурсов памяти и на практике не используется, либо хранить бумажные копии, подтверждающие получение товара покупателем;
* не обеспечивается конфиденциальность данных о реквизитах карты для продавца.

## Протокол SET

Другой протокол безопасных транзакций в Интернете - ***SET*** (Security Electronics Transaction). SET основан на использовании цифровых сертификатов по стандарту Х.509.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и VISA при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя самый защищенный на настоящее время механизм выполнения платежей. SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карточек в Интернет. SET обеспечивает кросс-аутентификацию счета держателя карточки, продавца и банка продавца для проверки готовности оплаты товара, целостность и секретность сообщения, шифрование ценных и уязвимых данных. Поэтому SET можно назвать стандартной технологией или системой протоколов выполнения безопасных платежей с использованием пластиковых карточек через Интернет.

SET позволяет потребителям и продавцам подтвердить подлинность всех участников сделки, происходящей в Интернет, с помощью криптографии, применяя, в том числе, и цифровые сертификаты.

Объем потенциальных продаж в области электронной коммерции ограничивается достижением необходимого уровня безопасности информации, который обеспечивают вместе покупатели, продавцы и финансовые институты, обеспокоенные вопросами обеспечения безопасности платежей через Интернет. Как упоминалось ранее, базовыми задачами защиты информации являются обеспечение ее доступности, конфиденциальности, целостности и юридической значимости. SET, в отличии от других протоколов, позволяет решать указанные задачи защиты информации.

В результате того, что многие компании занимаются разработкой собственного программного обеспечения для электронной коммерции, возникает еще одна проблема. В случае использования этого ПО все участники операции должны иметь одни и те же приложения, что практически неосуществимо. Следовательно, необходим способ обеспечения механизма взаимодействия между приложениями различных разработчиков.

В связи с перечисленными выше проблемами компании VISA и MasterCard вместе с другими компаниями, занимающимися техническими вопросами (например IBM, которая является ключевым разработчиком в развитии протокола SET), определили спецификацию и набор протоколов стандарта SET. Эта открытая спецификация очень быстро стала де-факто стандартом для электронной коммерции. В этой спецификации шифрование информации обеспечивает ее конфиденциальность. Цифровая подпись и сертификаты обеспечивают идентификацию и аутентификацию (проверку подлинности) участников транзакций. Цифровая подпись также используется для обеспечения целостности данных. Открытый набор протоколов используется для обеспечения взаимодействия между реализациями разных производителей.

SET обеспечивает следующие специальные требования защиты операций электронной коммерции:

* секретность данных оплаты и конфиденциальность информации заказа, переданной вместе с данными об оплате;
* сохранение целостности данных платежей; целостность обеспечивается при помощи цифровой подписи;
* специальную криптографию с открытым ключом для проведения аутентификации;
* аутентификацию держателя по кредитной карточке, которая обеспечивается применением цифровой подписи и сертификатов держателя карточек;
* аутентификацию продавца и его возможности принимать платежи по пластиковым карточкам с применением цифровой подписи и сертификатов продавца;
* подтверждение того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым карточкам через связь с процессинговой системой; это подтверждение обеспечивается с помощью цифровой подписи и сертификатов банка продавца;
* готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
* безопасность передачи данных посредством преимущественного использования криптографии.

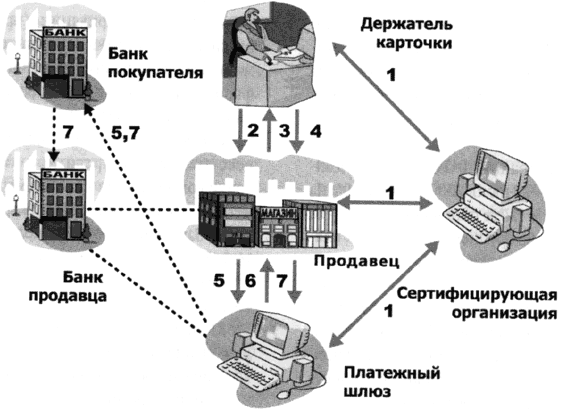
Основное преимущество SET перед многими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарт X.509, версия 3), которые ассоциируют держателя карточки, продавца и банк продавца с рядом банковских учреждений платежных систем VISA и MasterCard.

SET позволяет сохранить существующие отношения между банком, держателями карточек и продавцами, и интегрируется с существующими системами, опираясь на следующие качества:

* открытый, полностью документированный стандарт для финансовой индустрии;
* основан на международных стандартах платежных систем;
* опирается на существующие в финансовой отрасли технологии и правовые механизмы.

Кстати, совместный проект, реализованный компаниями IBM, Chase Manhattan Bank USA N.A., First Data Corporation, GlobeSet, MasterCard и Wal-Mart позволяет владельцам карточек Wal-Mart MasterCard, выпущенных банком Chase, приобретать товары на сайте Wal-Mart Online, который является одним из крупнейших узлов электронной коммерции США.

Рассмотрим более детально процесс взаимодействия участников платежной операции в соответствии со спецификацией SET, представленный на рисунке с сайта компании IBM:



На рисунке:

* Держатель карточки - покупатель делающий заказ.
* Банк покупателя - финансовая структура, которая выпустила кредитную карточку для покупателя.
* Продавец - электронный магазин, предлагающий товары и услуги.
* Банк продавца - финансовая структура, занимающаяся обслуживанием операций продавца.
* Платежный шлюз - система, контролируемая обычно банком продавца, которая обрабатывает запросы от продавца и взаимодействует с банком покупателя.
* Сертифицирующая организация - доверительная структура, выдающая и проверяющая сертификаты.

Взаимоотношения участников операции показаны на рисунке непрерывными линиями (взаимодействия описанные стандартом или протоколом SET) и пунктирными линиями (некоторые возможные операции).

Динамика взаимоотношений и информационных потоков в соответствии со спецификацией стандарта SET включает следующие действия :

1. Участники запрашивают и получают сертификаты от сертифицирующей организации.
2. Владелец пластиковой карточки просматривает электронный каталог, выбирает товары и посылает заказ продавцу.
3. Продавец предъявляет свой сертификат владельцу карточки в качестве удостоверения.
4. Владелец карточки предъявляет свой сертификат продавцу.
5. Продавец запрашивает у платежного шлюза выполнение операции проверки. Шлюз сверяет предоставленную информацию с информацией банка, выпустившего электронную карточку.
6. После проверки платежный шлюз возвращает результаты продавцу.
7. Некоторое время спустя, продавец требует у платежного шлюза выполнить одну или более финансовых операций. Шлюз посылает запрос на перевод определенной суммы из банка покупателя в банк продавца.

Представленная схема взаимодействия подкрепляется в части информационной безопасности спецификацией Chip Electronic Commerce, созданной для использования смарт-карточек стандарта EMV в Интернете (www.emvco.com). Ее разработали Europay, MasterCard и VISA. Сочетание стандарта на микропроцессор EMV и протокола SET дает беспрецедентный уровень безопасности на всех этапах транзакции.

Компания "Росбизнесконсалтинг" 20 июня 2000 г. поместила на своем сайте сообщение о том, что одна из крупнейших мировых платежных систем VISA обнародовала 19 июня 2000 г. свои инициативы в области безопасности электронной коммерции. По словам представителей системы, эти шаги призваны сделать покупки в Интернете безопаснее для покупателей и продавцов. VISA полагает, что внедрение новых инициатив позволит сократить количество споров по транзакциям в Интернете на 50%. Инициатива состоит из двух основных частей. Первая часть - это Программа аутентификации платежей (Payment Authentication Program), которая разработана для снижения риска неавторизованного использования счета держателя карточки и улучшения сервиса для покупателей и продавцов в Интернете. Вторая - это Глобальная программа защиты данных (Global Data Security Program), цель которой - создать стандарты безопасности для компаний электронной коммерции по защите данных о карточках и их держателях.

## Сравнительные характеристики протоколов SSL и SET

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 Интернете. SSL и SET - это два широко известных протокола передачи данных, каждый из которых используется в платежных системах Интернета. Мы попытаемся сравнить SSL и SET и оценить их некоторые важнейшие характеристики.

Итак, рассмотрим важнейшую функцию аутентификации (проверки подлинности) в виртуальном мире, где отсутствуют привычные физические контакты. SSL обеспечивает только двухточечное взаимодействие. Мы помним, что, в процесс транзакции кредитной карточки вовлечены, по крайней мере, четыре стороны: потребитель, продавец, банк-эмитент и банк-получатель. SET требует аутентификации от всех участвующих в транзакции сторон.

SET предотвращает доступ продавца к информации о пластиковой карточке и доступ банка-эмитента к частной информации заказчика, касающейся его заказов. В SSL разрешается контролируемый доступ к серверам, директориям, файлам и другой информации. Оба протокола используют современную криптографию и системы цифровых сертификатов, удостоверяющих цифровые подписи взаимодействующих сторон. SSL предназначен преимущественно для защиты коммуникаций в Интернете. SET обеспечивает защиту транзакций электронной коммерции в целом, что обеспечивает юридическую значимость защищаемой ценной информации. При этом через SET транзакция происходит медленней, чем в SSL, и ее стоимость намного выше. Последняя характеристика весьма актуальна для сегодняшнего российского рынка, на котором пока не считают риски и эксплуатационные расходы.

Следует добавить, что, используя SSL, потребители подвергаются риску раскрытия реквизитов своих пластиковых карточек продавцу.

Внедрение и эксплуатация SET осуществляется много лет в нескольких десятках проектов во всем мире. Например, первая транзакция SET была проведена 30-го декабря 1996 в PBS (Датский банк) в совместном проекте IBM и MasterCard. Аналогичная работа проведена в 1997 г. в крупнейшем японском банке Fuji Bank, где пришлось адаптировать протокол к специфическому японскому законодательству. За прошедшее время подобные внедренческие проекты позволили отработать функции протокола и соответствующую документацию.

Кстати, IBM имеет полный набор продуктов, который охватывает все ключевые аспекты комплексного использования SET в целом и обеспечивает развитую инфраструктуру:

* IBM Net.commerce Suite для продавцов, организующих интернет-магазины;
* IBM Consumer Wallet для держателей карточек;
* IBM Payment Gateway - шлюз платежей для банков;
* IBM Net. Payment Registry - продукт для аутентификации и сертификации.

SET функционирует на разных вычислительных платформах таких компаний, как IBM, Hewlett Packard, Sun Microsystems и Microsoft.

В свою очередь SSL используется в основном в Web-приложениях и для защиты коммуникаций в Интернете. Существует также свободно распространяемая версия SSL, называемая SSLeay. Она содержит исходный код на C, который может быть встроен в такие приложения, как Telnet и FTP. Благодаря этим качествам SSL получил широкое распространение в корпоративных интранет-сетях и в системах с небольшим количеством пользователей.

Несмотря на технологическое совершенство протокола SET, его использование в мире весьма ограничено. Тому имеется множество причин, решающей среди которых является высокая стоимость внедрения системы электронной коммерции на базе протокола SET (стоимость SET-решения колеблется от $600 до 1500 тыс.).

Протокол SSL обеспечивает лишь конфинденциальность данных транзакции при их передачи через сеть общего пользования, но при этом является существенно более дешевым для внедрения. В результате подавляющее число современных систем электронной коммерции используют протокол SSL.

Эксперты и разработчики протокола SET ошиблись, предсказывая быстрое и повсеместное внедрение этого стандарта. Более того, ведутся настойчивые разговоры о том, что протокол SET уже является вчерашним днем и его шансы на выживание ничтожны.

Такие разговоры начались еще летом 2000г., когда VISA International сделала заявление, в соответствии с которым протокол 3D SET (разновидность SET) становится стандартом для стран Евросоюза, Латинской Америки и некоторых других европейских стран, включая Россию. В то же время на самом крупном американском рынке в качестве стандарта был провозглашен протокол 3D SSL (другое название протокола - 3D Payer).

Глава российского представительства Visa Int. Лу Наумовский согласен с тем, что SET не нашел спроса:

"Это очень хорошая технология. Но, судя по реакции банков, не только российских, но и зарубежных, - она дороговата. Банку-эмитенту, использующему протокол SET для отслеживания операций по картам, приходится самому держать базу данных банков-эквайреров и торговых точек. Мы пытались найти более дешевую альтернативу этому протоколу".

В мае 2001 г. были опубликованы спецификации на стандарт 3D Secure, претендующий на роль глобального стандарта аутентификации в платежной системе Visa. По решению Европейского союза в июле 2002 г. все интернет-магазины получили идентификацию на уровне этого протокола. Следовательно, банк-эквайрер таких интернет-магазинов должен иметь возможность предоставить им этот протокол. В случае отсутствия 3D Secure всю ответственность при спорных трансакциях несет он сам. Если он использует 3D Secure, а банк-эмитент нет, то ответственность берет на себя последний.

Принцип работы 3D Secure в том, что есть три различных домена - банка-эмитента, интернет-магазина и Visa, через домен которой идет сообщение между покупателем, продавцом и банками. Очень важно, что все сообщения идут через интернет. При этом Visa обеспечивает конфиденциальность информации. После того как покупатель нажимает на интернет-странице на лозунг Verified by Visa и вводит свой пароль, эта информация идет к банку-эмитенту и происходит идентификация. Банк-эмитент через домен Visa отправляет запрос в интернет-магазин, после чего этот магазин идентифицируется своим банком-эквайрером. Таким образом, данные держателя карты известны только банку-эмитенту. В то же время владелец карты уверен в том, что данный магазин имеет Verified by Visa, то есть сертифицирован Visa через банк-эквайрер. В том случае, если банк-эмитент не получит от домена Visa подтверждения, что магазин имеет Verified by Visa, транзакция не произойдет.

Конечно, владелец карты может сделать покупки и в других, не имеющих статуса Verified by Visa, интернет-магазинах. Тогда ответственность по спорным сделкам несет банк-эмитент, и он должен будет предупреждать своих клиентов об этом.

TCP/IP(IPv6)

Протоколы TCP/IP нового поколения (IPv6) включают следующие новые черты: расширенное адресное пространство; улучшенные возможности маршрутизации; управление доставкой информации; средства обеспечения безопасности, использующие алгоритмы аутентификации и шифрования.

Спецификация IPsec, дополнительная по отношению к текущей версии протоколов TCP/IP и входящая в стандарт IPv6, разрабатывается Рабочей группой IP Security Тематической группы по технологии Интернет. В настоящее время IPsec включает 3 алгоритмо-независимых базовых спецификаций, опубликованных в качестве следующих RFC-документов.

Разработаный IETF протокол IPsec, предусматривает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и обеспечивает защиту на основе сквозного шифрования. IPsec шифрует каждый проходящий по каналу пакет независимо от приложения. Это позволяет организации создавать в Интернет виртуальные частные сети. IPsec поддерживает DES, MD5 и ряд других криптографических алгоритмов. IPsec предназначен для работы поверх связных протоколов.

Преимущества обеспечения информационной безопасности на сетевом уровне с помощью IPsec включают:

* поддержка немодифицированных конечных систем;
* поддержка иных протоколов, чем ТСР;
* поддержка виртуальных сетей в незащищенных сетях;
* защита заголовка транспортного уровня от перехвата, т.е. более надежная защита от анализа трафика;
* защита от атак типа "отказ в обслуживании".

IPsec имеет еще два важных преимущества - при его применении не требуется изменение промежуточных устройств в сети и рабочие места и серверы необязательно должны поддерживать IPsec.

IPsec - это система, использующая несколько различных методов для обеспечения комплексной информационной безопасности. Она использует:

* обмен ключами через открытую сеть на основе криптографического алгоритма Диффи-Хеллмана;
* применение цифровой подписи с использованием открытого ключа;
* алгоритм шифрования, подобный DES, для шифрования передаваемых данных;
* использование хэш-алгоритма для определения подлинности пакетов.

Протокол IPsec был разработан в рамках усилий по созданию средств защищенной передачи пакетов для IPv6, протокола IP следующего поколения сети Интернет - 2. Их спецификация продолжает совершенствоваться по мере выхода на рынок все новых и новых программных продуктов.

В нашей стране из различных стандартов по безопасности информационных технологий следует отметить ряд современных стандартов и документов, регламентирующих защиту взаимосвязи открытых систем (ВОС):

* ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации;
* ГОСТ Р ИСО/МЭК 9594-8-98 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации;
* ГОСТ Р ИСО/МЭК 9594-9-95 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 9. Дублирование;

К ним можно добавить нормативные документы по средствам, системам и критериям оценки защищенности средств вычислительной техники и автоматизированных систем, которыми являются:

* руководящий документ ГОСТЕХКОММИССИИ "РД. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" (Гостехкомиссия России, 1997);
* ГОСТ Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования";
* ГОСТ28147-89.Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;
* ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма;
* ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

Последняя группа документов преимущественно ориентирована на защиту государственной тайны также как и многие ранее созданные зарубежные документы.

Следуя по пути интеграции, в 1990 году Международная организация по стандартизации (ИСО) начала создавать международные стандарты по критериям оценки безопасности информационных технологий для общего использования, названные "Common Criteria(CC)" или "Общие Критерии Оценки Безопасности Информационных Технологий(ОК)". В разработке Общих Критериев участвовали: Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Голландия), Органы исполнения Программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция), которые опирались на солидный задел.

Новые критерии адаптированы к потребностям взаимного признания результатов оценки безопасности ИТ в мировом масштабе и предназначены для использования в качестве основы для такой оценки. За десятилетие разработки лучшими специалистами мира ОК неоднократно редактировались. В результате был подготовлен Международный Стандарт ISO/IEC 15408. Текст документа ISO/IEC 15408 был опубликован как "Общие критерии оценки безопасности информационных технологий" (ОК) и в 1999 году утвержден. Ведущие мировые производители оборудования ИТ основательно подготовились к этому моменту и сразу стали поставлять заказчикам любые средства, полностью отвечающие требованиям ОК.

Подводя итог вышеизложенному, следует отметить, что для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

* законодательного;
* административного;
* процедурного;
* программно-технического.

В современном мире нормативно-правовая база должна быть согласована с международной практикой. Назрела необходимость приведения российских стандартов и сертификационных нормативов в соответствие с международным уровнем ИТ вообще и по критериям оценки безопасности информационных технологий в частности. Приведем основные причины:

* необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских организаций;
* доминирование аппаратно-программных продуктов зарубежного производства.

Обеспечение безопасности ИТ невозможно без разработки соответствующих законодательных актов и нормативно-технических документов. Новые критерии оценки безопасности информационных технологий занимают среди них особое место. Только стандартизованные отечественные критерии позволяют проводить сравнительный анализ и сопоставимую оценку продуктов ИТ.

## Мошенничество в Интернете.

К сожалению, в Интернете высокие показатели уровня мошенничества являются сдерживающим фактором развития всей электронной коммерции. Потребители, торговля и коммерческие организации боятся использовать эту технологию из-за риска финансовых потерь. Интернет используется главным образом в качестве канала для получения информации. Лишь около 2% поисков по каталогам и базам данных Интернета заканчивается покупкой.

Существует множество типов мошенничества, от которых страдает безопасность электронной коммерции. Основные типы приведены ниже.

**Транзакции и безналичный расчет.** Выполненные мошенниками транзакции с использованием реквизитов карточки, передают им настоящие данные о карте и грозят полным опустошением счета без получения желаемых услуг или товаров.

**Базы данных и личная переписка.** Получение информации о клиенте через взлом баз данных торговых предприятий или путем несанкционированного доступа к личной переписке покупателя, содержащей его персональные данные.

**Магазины-однодневки.** Интернет-магазины, возникающие на непродолжительный период, созданные для получения средств от покупателей за несуществующие товары или услуги.

**Ложная стоимость и повторные списания.** Увеличение стоимости товаров по отношению к заявленной покупателю цене и повторные списания средств со счетов клиента.

**Магазины-шпионы.** Интернет-магазины и торговые агенты, предназначенные для сбора данных о реквизитах пластиковых карт и другой личной информации о клиенте.

Таким образом, безопасность электронной коммерции, как для клиентов, так и для организаций, является основной проблемой, сдерживающей развитие электронной коммерции в интернете.