Кафедра Маркетинга и коммерции ВГУЭС
Кметь Елена Борисовна
к.э.н., доцент

Тема 15. Криптография и ее роль в дистанционном банковском обслуживании

Дисциплина
«Маркетинг в финансово-кредитных учреждениях»

СОДЕРЖАНИЕ ТЕМЫ

КЛЮЧЕВЫЕ ПОНЯТИЯ

Безопасность электронной коммерции

Верификация

Закрытый ключ ЭЦП

Криптография

Открытый ключ ЭЦП

Слепая подпись

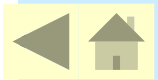
Цифровая подпись

Шифрование с закрытым ключом (симметричные алгоритмы)

Шифрование с открытым ключом (асимметричные алгоритмы)

Электронные деньги (или цифровая наличность)

Электронный сертификат



15.1. Безопасность электронной коммерции

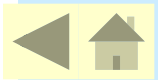
СОСТАВЛЯЮЩИЕ БЕЗОПАСНОСТИ

Понятие «безопасность» в русском языке трактуется как состояние, при котором отсутствует опасность, есть защита от нее.

Безопасность электронной коммерции – это состояние защищенности интересов субъектов отношений, совершающих коммерческие операции (сделки) с помощью технологий электронной коммерции, от угроз материальных и иных потерь.

Понятие «безопасность» предполагает три составляющих:

- физическую безопасность, под которой понимается обеспечение защиты от посягательств на жизнь и личные интересы сотрудников;
- экономическую безопасность, под которой понимается защита экономических интересов субъектов отношений, а также обеспечение защиты материальных ценностей от пожаров, стихийных бедствий, краж других посягательств;
- информационную безопасность, под которой понимается защита информации от модификации (искажения, уничтожения) и несанкционированного использования.



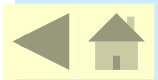
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Обеспечение информационной безопасности основывается на криптографических или шифровальных системах, которые обеспечивают *конфиденциальность, аутентификацию и целостность* информации.

Конфиденциальность предполагает защиту информации от несанкционированного доступа при ее хранении и при передаче. Доступ к информации имеет только тот, для кого она предназначена. *Шифрование данных обеспечивает конфиденциальность.*

Аутентификация предполагает необходимость однозначной идентификации отправителя послания. *Обеспечивается электронной цифровой подписью и сертификатом.*

Целостность предполагает, что информация должна быть защищена от несанкционированной модификации при ее хранении и при передаче. *Обеспечивается электронной цифровой подписью.*



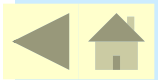
КРИПТОГРАФИЯ

Все системы шифрования работают по определенной методологии, которая включает один или несколько алгоритмов шифрования (математических формул), ключей, используемых этими алгоритмами, а также системы управления ключами.

Криптография - это специальная область математики, отвечающая за защиту информации.

Появление электронных платежных систем и цифровых денег стало возможно только с развитием этой области знаний. Поэтому далее рассмотрим основные методы шифрования и ключевые понятия криптографии.

Проблема надежности электронных платежей и их защищенности - сегодня один из наиболее важных факторов, влияющих на доверие клиентов. Функционирование платежных систем в Internet возможно только при обеспечении условий безопасности.



15.2. Шифрование сообщений

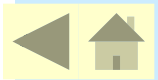
МЕТОДЫ ШИФРОВАНИЯ

Способов шифрования сообщений огромное количество, но все их условно можно разделить на две больших группы:

- методы шифрования закрытым ключом (симметричные алгоритмы)
- методы шифрования открытым ключом (ассиметричные алгоритмы).

Самая древняя криптографическая операция - метод Цезаря. Представляет собой циклический сдвиг алфавита на один шаг, можно использовать сдвиг на две позиции или три и т.д. Величина сдвига (число 1, 2, 3...) - это ключ, с помощью которого можно зашифровать и расшифровать текст или сообщение.

Подобные методы слишком просты и не являются надежной защитой. Сейчас шифровку и расшифровку сообщений производит программное обеспечение, а ключи вставлены в это программное обеспечение.



МЕТОДЫ ШИФРОВАНИЯ ЗАКРЫТЫМ КЛЮЧОМ

Существуют более криптостойкие методы. Для замены берутся не одиночные буквы, а наборы по две буквы и более, а в качестве ключей используются не просто числа, а комбинации букв и чисел и т.д. У всех упомянутых алгоритмов есть общая черта, они используют один и тот же ключ (пароль) для шифрования сообщения и его расшифровки.

Методы в криптографии, которые используют для шифровки и расшифровки сообщений один и тот же ключ, называются **шифрованием закрытым ключом** (или симметричными алгоритмами), а используемый ключ – **секретным** (симметричным).

Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных. Основной проблемой является безопасная передача закрытого ключа противоположной стороне, поэтому симметричный секретный ключ никогда не передается по незащищенным каналам связи.

ШИФРОВАНИЕ ОТКРЫТЫМ КЛЮЧОМ

Существуют методы, в которых для шифрования используется один ключ, а для расшифровки - другой. Программное обеспечение каждой стороны генерирует два ключа, связанных между собой по определенному правилу. По одному ключу восстановить другой невозможно.

Один из ключей открытый (общедоступный - public) для шифровки, другой ключ закрытый (персональный - private) для расшифровки.

Методы в криптографии, основанные на применении пары ключей (закрытый и открытый), называют **шифрованием открытым ключом** (или ассиметричными алгоритмами).

Имея такую пару ключей, открытый ключ можно передавать партнеру даже через газету. С помощью открытого ключа он шифрует сообщение, и даже он не сможет его расшифровать, так как расшифровать можно только с помощью второго, секретного ключа.

На поиски секретного ключа с помощью компьютерных программ могут уйти годы.

ШИФРОВАНИЕ ОТКРЫТЫМ КЛЮЧОМ

Каждый пользователь имеет два ключа, секретный ключ генерируется каждым пользователем самостоятельно, оба ключа математически связаны, открытые ключи помещаются в открытый справочник. Подобные методы являются более криптостойкими по сравнению с методами шифрования закрытым ключом.

Основной проблемой криптографических систем - распространение ключей. Асимметричные методы более приспособлены для Internet, но использование открытых ключей требует их дополнительной защиты и идентификации для определения связи с секретным ключом.

Шифрование передаваемых через Internet данных позволяет защитить их от посторонних лиц. Однако для полной безопасности должна быть уверенность в том, что второй участник транзакции является тем лицом, за которое он себя выдает.

В реальном мире наиболее важным идентификатором личности является его подпись. В электронной коммерции применяется электронный эквивалент традиционной подписи - цифровая подпись

15.3. Цифровая подпись (ЭЦП) и сертификат ключа подписи

ЦИФРОВАЯ ПОДПИСЬ

Системы цифровой подписи позволяют создавать в электронных документах аналог собственноручной подписи. При этом речь не идет о технологиях, позволяющих сохранить в электронном виде графическое изображение подписи. Механизмы цифровой подписи основаны на сложных математических задачах - это набор цифр, позволяющий идентифицировать лицо, сформировавшее эту подпись, но и обеспечить неизменность документа после подписи.

Цифровая подпись - это реквизит электронного документа, который уже не позволит отрицать подлинность этого документа и несет информацию о лице, которое имеет право его ставить.

Последние годы наблюдается процесс глубокого проникновения систем цифровой подписи в бизнес-процессы большинства организаций: системы «Клиент-банк», электронный документооборот, электронный бизнес и электронная коммерция, клиринг и т.д.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЭЦП

В настоящее время системы «клиент-банк» бурно развиваются и совершенствуются. Не только юридические, но и физические лица в настоящее время могут заводить счета в банках и управлять своими счетами через Internet, не выходя из дома. Благодаря технологии цифровой подписи стало возможно функционирование электронных платежных систем в Internet.

В США закон об ЭЦП вступил в силу уже **1 октября 2000 г.** Законы, аналогичные американскому, приняли на сегодняшний момент многие страны мира, включая Европейский Союз, Таиланд, Белоруссию.

Гражданский кодекс РФ закрепил возможность использования цифровой подписи наряду с иными аналогами собственноручной подписи в электронном документообороте. С момента принятия первой части Гражданского кодекса РФ системы электронного документооборота стали полностью юридически легальными. Был принят Федеральный закон **1-ФЗ «Об электронной цифровой подписи» 10 января 2002 г**, который вступил в действие с 10 июля 2002 г.

ТЕХНОЛОГИЯ ИСПОЛЬЗОВАНИЯ ЭЦП

В принятом законе вводится следующее понятие ЭЦП «*электронная цифровая подпись* - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе».

Из определения следует, что

- электронная цифровая подпись получена в результате криптографического преобразования информации с использованием закрытого ключа
- ЭЦП используется для создания сертификатов и подписи транзакций
- в механизме ЭЦП используются два криптографических ключа: открытый и закрытый, которые генерируются автором сообщения.

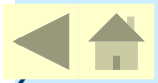
ТЕХНОЛОГИЯ ИСПОЛЬЗОВАНИЯ ЭЦП

В технологии цифровой подписи используется шифрование открытым ключом наоборот.

Отправляемый документ шифруется закрытым, а расшифровывается открытым ключом.

Открытый ключ ЭЦП - это общедоступная последовательность символов, предназначенная для проверки электронной подписи. Получатель документа, используя открытый ключ, проверяет ЭЦП. Открытый ключ позволяет только проверять существующую ЭЦП, но не позволяет расписаться (подписать). Создание ЭЦП возможно только с помощью закрытого ключа, который имеется только у владельца подписи.

Закрытый ключ ЭЦП - последовательность символов, предназначенная для выработки ЭЦП и известная только правомочному лицу - владельцу. Владелец использует этот ключ для создания своей подписи под каждым документом.



ТЕХНОЛОГИЯ ЦИФРОВОЙ ПОДПИСИ

1. Генерируется пара ключей (для каждой компании своя пара ключей). Открытый ключ известен всем, закрытый - только конкретному лицу. Берется любой файл (текст, музыка, видео, картинка), пропускается через известный математический алгоритм «хэширования», в результате получается новый файл небольшого размера, содержащий результат переваривания исходной информации алгоритмом. Результат переваривания и есть ЭЦП. Этот алгоритм является закрытым ключом, известным только конкретному лицу.

Если добавить один единственный пробел к исходному файлу, результат получается другой. Алгоритм устойчиво получает одну и ту же смесь из одной и той же информации. Алгоритм является односторонним.

2. Исходный файл передается вместе с цифровой подписью. Другая сторона с помощью открытого ключа расшифровывает (восстанавливает из подписи) исходный файл и сравнивает с присланным файлом. Их полное соответствие является доказательством, что присланное сообщение подписано конкретным лицом.

ЭЛЕКТРОННЫЙ СЕРТИФИКАТ

Для определения связи открытого ключа с закрытым ключом необходима ***верификация*** открытого ключа. Для этих целей используются электронные сертификаты.

Электронный сертификат (или сертификат ключа подписи) представляет собой цифровой документ, который связывает открытый ключ с конкретным пользователем (или приложением) и, одновременно, включает в себя открытый ключ электронной цифровой подписи.

Сертификат выдается удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи (содержит электронную цифровую подпись уполномоченного лица удостоверяющего центра).

Для заверения электронного сертификата используется электронная цифровая подпись доверенного лица удостоверяющего центра — Центра сертификации (ЦС).

ЭЛЕКТРОННЫЙ СЕРТИФИКАТ

Популярные источники сертификатов - компании Thawte (http://www.thawte.com) и VeriSign (http://www.verisign.com), однако существуют и другие системы сертификации, такие как World Registry (IBM), Cyber Trust (GTE) и Entrust (Nortel). В России дистрибьютором SSL-сертификатов компании Thawte сегодня является "РосБизнес-Консалтинг" (http://www.rbc.ru).

***Технология цифровых сертификатов*:**

1. Чтобы воспользоваться сертификатом, потенциальный покупатель должен прежде всего получить этот сертификат у надежного источника сертификатов. Для этого ему (необходимо каким-то образом доказать подлинность своей личности), а также передать источнику сертификатов копию своего открытого ключа.

2. Если он захочет что-либо купить в Internet, ему достаточно добавить к заказу свою электронную подпись и копию сертификата. Отдел обслуживания покупателей компании, в которой он совершил покупку, проверяет сертификат, чтобы убедиться, что к заказу приложен подлинный сертификат, а также выясняет, не аннулирован ли сертификат.

15.4. Слепая подпись

СЛЕПАЯ ПОДПИСЬ

Слепая подпись - это реквизит электронного документа (файла), который уже не позволит отрицать подлинность этого документа при частичном закрытии некоторой части информации в этом документе (файле) ослепляющим фактором.

Благодаря слепой подписи стало возможно функционирование электронных платежных систем в Internet с использованием цифровых наличных, электронных денег, web-денег.

Электронные деньги (или цифровая наличность) - это очень большие числа или файлы, которые и играют роль купюр и монет.

У цифровой наличности есть как достоинства, так и недостатки. Основными достоинствами является анонимность цифровой наличности (она не несет информации о своем владельце) и возможность осуществлять микроплатежи (менее одного доллара).

ПРОЦЕСС СОЗДАНИЯ ЭЛЕКТРОННЫХ ДЕНЕГ

1. Став участником платежной системы PayCash пользователь заводит счет в банке-участнике системы. На счет вносятся реальные деньги. Счет можно завести через Internet, не выходя из дома.
2. На компьютере пользователя устанавливается программное обеспечение (Кошелек), с помощью которого компьютер вычисляет необходимое количество цифровых монет и их номиналы для запрошенной суммы. Для монет создаются случайные серийные номера, на которые ставится *слепая подпись* (информация о серийных номерах закрывается ослепляющим фактором). Результат отсылается в банк.
3. Банк подписывает скрепленные слепой подписью числа своим секретным, закрытым ключом и производит дебетование счета клиента на соответствующую сумму.
4. Аутентифицированные монеты отсылаются обратно пользователю, который снимает свою слепую подпись (удаляет идентифицирующую его подпись).

Серийные номера совместно с подписью банка и являются электронными деньгами. Хранятся электронные деньги на компьютере пользователя или Smart-карте.

15.5. Стандарты безопасности

БЕЗОПАСНЫЕ ПРОТОКОЛЫ СЕАНСА СВЯЗИ

Гарантами безопасности электронных платежных систем являются стандарты безопасности.

В качестве стандартов безопасности выступают протоколы сеанса связи, обеспечивающие безопасную передачу данных.

Наиболее распространенными стандартами безопасности виртуальных платежей являются:

- **протокол SSL** (Secure Socket Layer Protocol), обеспечивающий шифрование передаваемых через Интернет данных
- **стандарт SET** (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard и обеспечивающий безопасность и конфиденциальность совершения сделок при помощи пластиковых карт.

ПРОТОКОЛ SSL

Протокол SSL — стандарт, основанный на методах шифрования с открытыми ключами, разработан компанией Netscape. Эта всемирно известная компания-разработчик программного обеспечения для работы с ресурсами Internet.

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.

Пользователи, совершающие покупки в Internet, озабочены надежностью средств, применяемых при выполнении платежей в Интернете с использованием банковских платежных карт. Протокол SSL позволяет решить часть проблем безопасности, однако его роль в основном ограничивается обеспечением шифрования передаваемых данных.

СТАНДАРТ SET

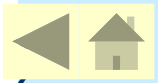
Поэтому совместно компаниями MasterCard и Visa при подержке Netscape, IBM, Versign и других был разработан **стандарт SET** (Secure Electronic Transaction specification - Безопасные электронные транзакции).

Протокол SSL в большинстве случаев используется для передачи информации о картах.

В основе спецификации SET лежит криптография с использованием публичных (открытых) ключей и цифровых сертификатов.

Технология выглядит следующим образом:

- номер карточки, передаваемый по сети, шифруется с использованием электронной подписи клиента.
- дешифровку могут осуществлять только уполномоченные банки и компании, осуществляющие обработку транзакций по карточкам.



СТАНДАРТ SET

Протокол SET предназначен для защиты клиентов от недобросовестных продавцов и для защиты продавцов от мошенничества при помощи подделанных или краденных карточек. Это обеспечивается тем, что процесс проверки безопасности включает сопоставление цифровых сертификатов, выданных покупателю, продавцу, банку и процессинговым компаниям.

SET предполагает **четыре основных элемента**:

1. *Бумажник владельца карты* (Cardholder Wallet), который работает в режиме on-line, позволяя проводить защищенные платежи.

2. *Серверная часть продавца* (Merchant Server), позволяющая осуществлять авторизацию и обработку платежных карт.

3. *Шлюз прохождения платежей* (Payment Gateway) – осуществляет авторизацию продавца и платежных инструкций, включая инструкции т покупателя, и взаимодействует с финансовыми сетями.

4. *Центр выпуска сертификатов* (Certificate Authority), который выпускает и сверяет сертификаты.

15.6. Роль закона «Об электронной цифровой подписи» во всех сферах деятельности

ДВЕ СХЕМЫ РЕГУЛИРОВАНИЯ СИСТЕМ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

10 января 2002 г. в третьем чтении был принят 1-ФЗ «Об электронной цифровой подписи». Разработчиком закона являлось ФАПСИ (Федеральное агентство правительственной связи и информации при Президенте РФ).

Системы без использования сертификатов и Удостоверяющих Центров (УЦ) не регулируются Законом «Об ЭЦП». Регулирование в них основано на следующих документах:

1) Гражданский кодекс Российской Федерации

2) Федеральный закон "Об информации, информатизации и защите информации"

3) официальные материалы Высшего арбитражного суда РФ

Таким образом, существуют две схемы регулирования: одна наиболее общая - на основе Гражданского кодекса и решений Высшего арбитражного суда (эта схема в ближайшее время найдет свое отражение в новом Законе «Об электронных подписях»), другая более узкая, регулирующая использование ЭЦП (в смысле определений, данных в законе).

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Какие составляющие безопасности известны и чем занимается криптография?

2. Раскройте содержание понятий конфиденциальность, аутентификация и целостность информации.

3. Чем отличаются методы шифрования закрытым и открытым ключом?

4. Опишите технологию использования электронной цифровой подписи. Для чего предназначены закрытый и открытый ключи ЭЦП?

5. Что означает термин верификация, чем она обеспечивается?

6. Опишите технологию работы цифрового сертификата.

7. В каких платежных системах и для чего используется слепая подпись?

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Закон Российской Федерации «Об электронной цифровой подписи» от 10 января 2002 г. № 1-ФЗ
2. Алексунин В.А., Родигина В.В. Электронная коммерция и маркетинг в Интернете: Учебное пособие. - М. : Издательско-торговая корпорация «Дашков и К», 2007, - 214 с.
3. Быстров Л.В., Воронин А.С., Гамольский А.Ю. и др. Пластиковые карты. 5-е изд., перераб. и доп. – М. : Издательская группа «БДЦ-пресс», 2005. - 624 с.
4. Кметь Е.Б. Электронная коммерция и экономика : уч. пос. Владивосток : ВГУЭС, 2009. 160 с.
5. Кобелев О.А. Электронная коммерция: Учебное пособие / Под ред. проф С.В. Пирогова. – 3-е изд., перераб. и доп. – М. Издательско-торговая корпорация «Дашков и К», 2008. – 684 с.

Спасибо за внимание

Использование материалов презентации

Использование данной презентации, может осуществляться только при условии соблюдения требований законов РФ об авторском праве и интеллектуальной собственности, а также с учетом требований настоящего Заявления.

Презентация является собственностью авторов. Разрешается распечатывать копию любой части презентации для личного некоммерческого использования, однако не допускается распечатывать какую-либо часть презентации с любой иной целью или по каким-либо причинам вносить изменения в любую часть презентации. Использование любой части презентации в другом произведении, как в печатной, электронной, так и иной форме, а также использование любой части презентации в другой презентации посредством ссылки или иным образом допускается только после получения письменного согласия авторов.