Федеральное агентство по образованию
Нижегородский государственный университет им. Н.И. Лобачевского

Национальный проект «Образование»
Инновационная образовательная программа ННГУ. Образовательно-научный центр «Информационно-телекоммуникационные системы: физические основы и математическое обеспечение»

Л.Ю. Ротков, А.В. Зобнев

Электронная цифровая подпись в электронном документообороте

Учебно-методические материалы по программе повышения квалификации «Электронный документооборот»

Нижний Новгород
2006

Учебно-методические материалы подготовлены в рамках инновационной образовательной программы ННГУ: Образовательно-научный центр «Информационно-телекоммуникационные системы: физические основы и математическое обеспечение»

Л.Ю. Ротков, А.В. Зобнев. Электронная цифровая подпись в электронном документообороте. Учебно-методические материалы по программе повышения квалификации «*Электронный документооборот*».
Нижний Новгород, 2006, 42 с.

В учебно-методическом пособии представлены основные сведения и понятия в области современных корпоративных систем, в том числе систем электронного документооборота. Рассмотрены вопросы внедрения и применения технологий электронной цифровой подписи в информационных системах. Представлены сведения о современных криптографических алгоритмах и стандартах, используемых в системах электронной цифровой подписи.

ГЛАВА 1. ОБЩИЕ СВЕДЕНИЯ.

В настоящее время бурно развиваются системы электронного документооборота, постоянно увеличивается объем документов, обрабатываемых в электронном виде.

В системах бумажного и электронного документооборота актуальными являются такие задачи как:

- защита документов от модификации и подделки;
- определение автора документа, а также подлинности документа;
- обеспечение юридической силы документов;
- защита документов от несанкционированного просмотра.

В основе традиционных систем бумажного документооборота лежит принцип заверки документов подписью и печатью ответственного лица. Достоверность такого документа определяется визуально при его предъявлении. Степень защиты бумажных документов от различного рода угроз (подделка, дублирование и пр.) достаточна мала.

В системах электронного документооборота для решения такого рода задач используются технологии Электронной Цифровой Подписи (ЭЦП).

ЭЦП представляет собой небольшой объем информации, который добавляется к электронному документу. При получении или предъявлении документа, подписанного ЭЦП, можно легко установить его авторство и подлинность. Кроме того, ЭЦП защищает документ от модификации и подделки, так как содержит в себе сжатый и зашифрованный образ электронного документа – «дайджест» документа.

Технологии электронной цифровой подписи базируются на криптографических алгоритмах с открытыми ключами (асимметричная криптография). На основе криптографических алгоритмов с открытыми ключами можно реализовать защиту информации при передаче по открытым каналам связи.

Комплекс организационно-технических мероприятий и программно-аппаратных средств, необходимых для использования технологии с открытым распределением ключей называется – ***Инфраструктурой открытых ключей***.

Инфраструктура открытых ключей позволяет решать широкий спектр задач по защите информации в различных информационно-телекоммуникационных системах: электронный документооборот, сдача отчетности, медицина и телемедицина, платежные и трейдинговые системы.

ГЛАВА 2. ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Документ. Документооборот.

Рассмотрим основные термины, относящиеся к документообороту.

Документ — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Электронный документ — документ, в котором информация представлена в электронно-цифровой форме.

Документооборот — движение документов с момента их создания или получения до завершения исполнения, отправки адресату или передачи в архив.

Делопроизводство — комплекс мероприятий по документационному обеспечению управления (ДОУ) организации, систематизации архивного хранения документов, обеспечению движения, поиска, хранения и использования документов.

Архив — организация или ее структурное подразделение, осуществляющее прием и хранение документов с целью использования ретроспективной информации.

Электронный архив — предназначен для систематизации архивного хранения электронных документов в рамках ДОУ.

Документ в процессе своего жизненного цикла (ЖЦ) проходит определенные стадии:

- создание;
- визирование, согласование;
- подписание, утверждение;
- регистрацию;
- рассмотрение;
- исполнение;
- списание в дело;
- хранение, уничтожение.

Движение документов осуществляется в виде потоков циркулирующих между пунктами обработки информации и пунктами технической обработки документов. По отношению к аппарату управления потоками различают потоки входящих (поступающих), исходящих (отправляемых) и внутренних документов.

На этапе создания документ не имеет юридической силы и является проектом документа. Документ приобретает юридическую силу после оформления и удостоверения в установленном порядке.

Электронный документ получает юридическую силу после его подписания электронной цифровой подписью (ЭЦП). Электронная цифровая подпись подтверждает, что содержательная информация документа не претерпела изменений с момента его подписания и документ подписан определенным лицом. При этом алгоритмы ЭЦП, а также механизмы и порядок применения ЭЦП должны соответствовать государственным нормативно-правовым требованиям.

Системы электронного документооборота

Развитие компьютерных технологий позволило во многих областях заменить бумажный документооборот безбумажным (электронным).

Основные недостатки бумажного документооборота:

- длительный поиск нужных данных и, как следствие, неоперативный доступ к необходимой информации;
- возможность потери или порчи документа;
- недостаточная конфиденциальность информации;
- высокая вероятность подделки документа и/или реквизитов документа;
- дублированный ввод информации;
- учет документов требует дополнительных финансовых и трудовых затрат.

Системы электронного документооборота (СЭД) позволяют решать проблемы бумажного документооборота.

Первые системы электронного документооборота появились в банковской сфере. В западной литературе такие системы получили название "системы электронного перевода денежных средств" (The Electronic Funds Transfer Systems (EFTS)). Одна из таких систем SWIFT1 функционирует с начала 1970-х годов.

В дальнейшем системы электронного документооборота стали широко применяться и для обмена другой коммерческой информацией (Английское название таких систем Electronic Data Interchange, или сокращенно EDI.). Уже много лет такие системы используются для продажи и бронирования авиационных билетов.

СЭД — это специальный программно-аппаратный комплекс, предназначенный для коллективной работы с документами в сетевой среде. Благодаря СЭД документы можно объединять в логические блоки, обеспечивая их архивное хранение и поиск (см. рис.1).

Рис. 1. Этапы прохождения электронного документа в СЭД.

Базовой единицей СЭД является **электронный документ** (ЭлД). В общем случае ЭлД представляет собой совокупность файлов разного типа (составных частей документа) и снабжен регистрационной карточкой.

Регистрационная карточка содержит набор реквизитов, таких как название организации, вид документа, отметки о согласованиях и утверждениях, даты, адреса сторон и т.д., и позволяет регистрировать, идентифицировать и находить документ, контролировать исполнительскую дисциплину, отслеживать историю документа и архивировать его.

Основная задача СЭД — управление полным жизненным циклом документа, начиная с его создания и заканчивая списанием в архив, т.е. управление движением документов (документооборотом).

Как правило, СЭД состоит из двух основных блоков: статического (электронный архив) и динамического (документооборот). Первый блок обеспечивает первичную обработку документов (регистрация входящей и исходящей информации, поиск, составление отчетов и пр.), а второй — организацию информационных потоков, по которым проходят документы, контроль исполнения, групповую работу над документом и т.п.

Помимо базовых функций в современных СЭД реализовано множество других подсистем, обеспечивающих такие функции как: потоковый ввод бумажных документов; поддержка

истории работы с документом (для учета обращений и подготовки отчетов), поиск по атрибутам документа и по его содержанию, разграничение прав доступа, маршрутизация документов по рабочим местам пользователей, интеграция с почтовыми системами, формирование отчетов, защита документов с помощью шифрования и ЭЦП.

Корпоративные информационные системы.

Делопроизводство – это деятельность по созданию документов и организации работы с ними. Под организацией работы с документами понимают создание условий, обеспечивающих движение, поиск и хранение документов. Движение документов между пунктами их обработки представляет собой документооборот.

По отношению к задачам делопроизводства и применяемым информационным технологиям корпоративные информационные системы подразделяются:

- **СУД** – Системы управления документами (DMS - Document Management System);
- **САДП** – Системы автоматизации деловых процессов (WMS - Workflow Management System);
- **СОГР** – Системы организации групповой работы (GroupWare);
- **Электронные архивы**;
- **АСКИД** – Автоматизированные системы контроля исполнения документов.

1. Автоматизированная система контроля исполнения документов

Задачами такого рода систем является учет всей документации учреждения, а также постановка на контроль и контроль исполнения документов. В общем случае, система ведет журналы регистрации и контроля или регистрационно-контрольные карточки (РКК) документов, сигнализирует о приближении сроков окончания исполнения, о просроченных документах, выдает информацию в виде отчетов. Система рассчитана на делопроизводственный персонал и группы контроля.

2. Электронный архив

Система автоматизации, предназначенная, прежде всего, для физического хранения электронных копий документов и их поиска, может включать в себя функции АСКИД. Хранение документов осуществляется либо в файловой системе ОС, либо в БД. Реализованы функции поиска, как по атрибутам, так и по содержанию документов. Основывается на персональных или на клиент-серверных СУБД.

3. Системы организации групповой работы (СОГР)

Западный термин – groupware. К СОГР относят, прежде всего, Microsoft Exchange, Lotus Notes и Novell GroupWize. Системы организации групповой работы представляют, расширенные варианты почтовых программ и изначально предназначены для организации обмена информацией в группе – обмена документами. СОГР характеризуются ограниченным размером базы данных собственного формата или же имеют возможность odbc-связи с СУБД, частичной поддержкой SQL, неразвитой системой полнотекстового поиска. Системы, построенные на платформе СОГР, автоматизируют, прежде всего, документооборот, а также контрольные и учетные функции, функции хранения и поиска.

4. Системы автоматизации деловых процессов (САДП)

Workflow-системы или WMS (Workflow Management System). В основу функционирования таких систем положено понятие потока работ. Базовой единицей в САДП есть работа, которая должна быть выполнена с определенными условиями в заданной последовательности и заданными исполнителями. Исполнение работы может производиться в различных временных рамках, контролироваться по времени и содержанию, с ней могут связываться документы, задания, резолюции и т.п. Понятие работы в workflow гораздо шире, чем документа, понятие движения работ шире движения документов, т.е. workflow, в сущности, включает в себя документооборот как частный случай. Информацию о работах (карты работ) workflow-система хранит в БД, документы и другие прикрепления к работам либо хранятся на сервере (в файловой системе, в БД), либо передаются физически от исполнителя к исполнителю согласно карте работы. В случае хранения документов на сервере пользователям передаются только права доступа к ним. Неотъемлемой частью таких систем – наличие графического редактора маршрутов работ. Возможна жесткая, свободная и смешанная маршрутизация, с параллельным и последовательным выполнением работ.

5. Системы управления документами (СУД)

Системы управления документами, западный термин EDMS – Electronic (Enterprise) Document Management System. Такое название основывается на утверждении, что и делопроизводство и документооборот являются всего лишь частным случаем более общего понятия “управление документами”. Данный класс систем считается универсальным, т.е. автоматизирующим весь комплекс задач, возлагаемых на делопроизводство, от разработки и

создания проекта документа, до списания в дело, включая документооборот и хранение документов.

СУД должна отвечать следующим требованиям:

- осуществлять ведение пользователей на основе организационно-штатной структуры организации;
- вести журналы регистрации и контроля исполнения (РКК);
- контролировать сроки исполнения документов, оповещать исполнителя и делопроизводителя о приближении сроков контроля, о невыполненных в срок документах;
- хранить документы в системе;
- поддерживать шаблоны документов, составные документы, версии и подверсии, перекрестные ссылки между документами;
- отслеживать документы вне системы, осуществлять выписку документов из системы;
- осуществлять поиск документов: атрибутивный, полнотекстовый, нечеткий поиск;
- поддерживать разработку документов на стадии проекта, включая коллективную разработку;
- поддерживать визирование, согласование, утверждение документов;
- осуществлять движение документов – документооборот, поддерживать все виды маршрутизации, автоматическую рассылку уведомлением, обмен сообщениями и поручениями внутри системы, формировать реестры отправки во внешние организации;
- вести классификаторы документов (по типу, виду и т.п.), справочники внешних и внутренних организаций, др. справочники;
- осуществлять жесткое разграничение полномочий в системе, поддерживать роли, осуществлять протоколирование и аудит действий пользователей;
- поддерживать возможность шифрования, цифровую подпись;
- вести дела документов, поддерживать функцию списания документов в дело, передачу дел на хранение в архив;
- формировать требуемые отчеты, в т.ч. статистические отчеты по делопроизводству организации.

СУД основываются на промышленных СУБД - Oracle, Informix, MS SQL Server, Sybase. Организация хранения документов может осуществляться как в БД, так и файловой системе. Недостатком хранения в БД есть жесткая привязка к конкретной СУБД и сложность восстановления после сбоев, в файловой системе – низкая безопасность хранимой информации. Обмен документами между пользователями осуществляется подсистемой обмена и маршрутизации документов, зачастую роль этой подсистемы выполняют workflow-системы. Многие СУД снабжены редакторами (дизайнерами) справочников, регистрационно-контрольных карт для задания различных атрибутов различных видов документов.

Безопасность корпоративных информационных систем

Комплексная безопасность информационной системы определяется возможностью противодействовать широкому спектру угроз, как внутренних, так и внешних. Для противодействия и сведения к минимуму ущерба от различного рода вредоносных воздействий необходимо реализовать соответствующие подсистемы защиты. В общем случае конкретная подсистема защиты представляет собой комплекс мероприятий, направленный на снижение риска и ущерба от определенного рода угроз, обеспеченный необходимой ресурсной базой: нормативно-правовые документы, программно-аппаратные средства, квалифицированный персонал.

Для оценки безопасности информационных систем и технологий возможно использование различных методик. В частности, в интерпретации ГОСТ Р ИСО/МЭК 15408-2002 (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.) выделяют следующие критерии безопасности информационных технологий:

- Идентификация пользователей (возможность однозначно идентифицировать субъекта);
- Аутентификация пользователей (проверка принадлежности субъекту предъявленного им идентификатора, подтверждение подлинности);
- Авторизация доступа к ресурсам (информация должна быть доступна только для того, для кого она предназначена);
- Целостность информации (информация должна быть защищена от несанкционированной модификации, как при хранении, так и при передаче);
- Невозможность отказа от совершенных действий (субъект не может отказаться от совершенного действия);

- Конфиденциальность информации (информация должна быть защищена от несанкционированного прочтения, как при хранении, так и при передаче).

Критерии безопасности подразумевают реализацию соответствующих подсистем информационной безопасности. Большинство из задач, описываемых данными критериями, можно решать с использованием Инфраструктуры Открытых Ключей (ИОК).

Инфраструктура Открытых Ключей – это комплекс организационно-технических мероприятий и программно-аппаратных средств, необходимых для использования технологии с открытым распределением ключей (асимметричной криптографии).

Инфраструктура открытых ключей позволяет решать широкий спектр задач по защите информации в корпоративных информационно-телекоммуникационных системах: электронный документооборот, сдача отчетности, медицина и телемедицина, платежные и трейдинговые системы и пр.

Одной из самых распространенных информационных технологий реализованных на базе ИОК является **Электронная Цифровая Подпись** (ЭЦП).

ГЛАВА 3. ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

Инфраструктура открытых ключей (ИОК) базируется на асимметричной криптографии (криптография с открытыми ключами). Асимметричная криптография как раздел науки криптографии появилась в конце 70-х годов 20-го века. В настоящее время в системах защиты информации широко используются, как симметричная, так и асимметричная криптографии.

Криптография является разделом математики и занимается поиском и исследованием методов преобразования информации с целью сокрытия ее содержания.

Криптографические алгоритмы

Процесс криптографического преобразования (шифрования) информации выглядит следующим образом. ***Открытый текст*** (информацию, которую требуется зашифровать) шифруют с помощью определенного ***криптографического алгоритма*** и ***ключа шифрования***. Зашифрованный по надежному криптографическому алгоритму текст практически невозможно расшифровать без дополнительных данных, которые называются ***ключом расшифрования***.

Характеристика шифра (криптографического алгоритма), определяющая его стойкость к расшифрованию без знания ключа расшифрования называется ***криптостойкостью***.

1. Симметричные алгоритмы

Криптография с симметричным, или секретным, ключом использует одинаковые ключи для шифрования и расшифровывания сообщений (см. рис.2). Ключ этот знают только отправитель и адресат, он не должен быть известен третьему лицу. Поэтому главная проблема симметричной криптографии состоит в предварительной **передаче секретного ключа одним абонентом другому по надежному каналу**. Кроме того, ее применение требует хранения множества ключей для разных абонентов и разных типов сообщений.

Рис. 2. Схема симметричного шифрования.

Существует огромное разнообразие конкретных реализаций алгоритмов шифрования симметричными ключами. Наибольшее распространение получил алгоритм DES (Data Encryption Standard), принятый национальным бюро стандартов США в 1977 году. В 1991 году аналогичный алгоритм был принят в качестве отечественного стандарта (ГОСТ 28147-89). Определенное распространение получили также алгоритмы RC4, RC5, IDEA и пр.

2. Асимметричные алгоритмы (алгоритмы с открытым ключом)

В алгоритмах этого типа для шифрования и расшифровки информации используются пара ключей: ***открытый и закрытый***, каждый из которых не может быть получен из другого (см. рис.3). Открытый ключ рассылается всем абонентам, закрытый держится в тайне. Для того чтобы отправить сообщение абоненту, нужно при шифровании использовать его открытый ключ, получатель же расшифровывает сообщение при помощи своего закрытого секретного ключа. Никто, кроме получателя, не может расшифровать сообщение, так как никто больше не имеет доступа к этому закрытому ключу. Даже тот, кто зашифровал сообщение с помощью открытого ключа, не сможет его расшифровать. Такой протокол обеспечивает приватность без необходимости обладания надежным каналом, которого требует обычная криптография с секретным ключом.

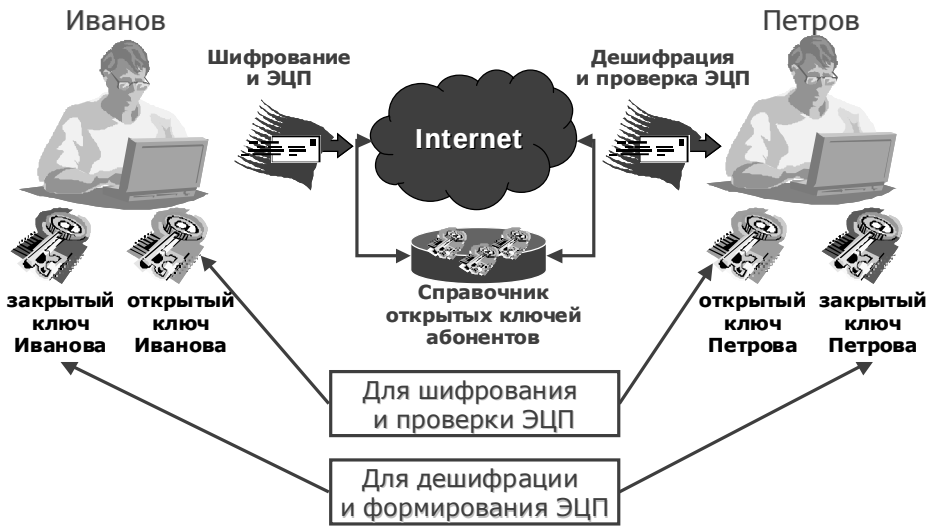

Рис. 3. Схема асимметричного шифрования.

При использовании алгоритма с открытым ключом отпадает потребность в секретном канале связи для передачи ключа, т.к. открытый ключ не является секретной информацией.

Различие ключей – открытого и закрытого – в криптографии с открытыми ключами позволило создать следующие технологии:

- **электронные цифровые подписи**
  (задачи обеспечения целостности, авторства, актуальности информации, аутентификации субъекта и информации, неотказуемости);
- **распределенная проверка подлинности**
  (задачи идентификации, аутентификации субъекта, авторизация доступа субъекта к информации);
- **согласование общего секретного ключа сессии**
  (задачи обеспечения конфиденциальности информации при передаче по открытым каналам связи);
- **шифрование больших объемов данных без предварительного обмена общим секретным ключом**
  (задачи обеспечения конфиденциальности информации).

В настоящее время хорошо известен целый ряд алгоритмов шифрования с открытым ключом. Некоторые алгоритмы, например RSA (Rivest-Shamir-Adleman) и ECC (Elliptic Curve

Cryptography), универсальны, они поддерживают все перечисленные выше операции. Другие алгоритмы более специализированы и поддерживают не все возможности.

К числу алгоритмов шифрования с открытым ключом относятся:

- российский алгоритмы электронной цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001;
- алгоритм электронной цифровой подписи DSA (Digital Signature Algorithm, входящий в принятый в США государственный стандарт цифровой подписи Digital Signature Standard, FIPS 186);
- алгоритм DH (Diffie-Hellman), применяемый для выработки общего секретного ключа сессии.

Сертификаты открытых ключей

В алгоритмах криптографии с открытыми ключами важным аспектом является определение принадлежности конкретного открытого ключа конкретному пользователю. В общем случае открытые ключи пользователей системы хранятся в общедоступном справочнике открытых ключей, и существует вероятность перехвата или подмены злоумышленниками открытого ключа какого-либо пользователя. Поэтому нужен механизм, который может обеспечить уверенность в том, что имеющийся открытый ключ принадлежит нужному пользователю, а не кому-либо другому. Один из таких механизмов основан на сертификатах открытых ключей, выдаваемых Удостоверяющими Центрами.

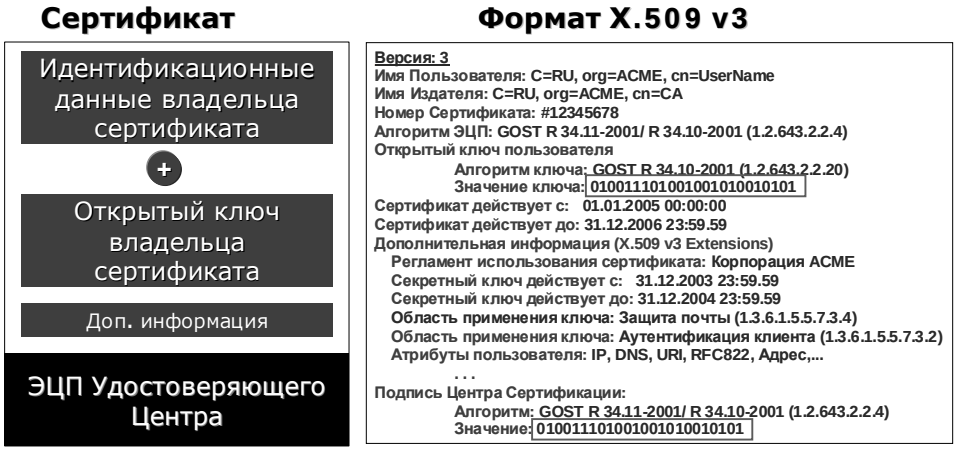

Рис. 4. Сертификат открытого ключа.

Сертификаты открытого ключа обеспечивают механизм надежной связи между открытым ключом и субъектом, которому принадлежит соответствующий закрытый ключ (см. рис.4).

Сертификат – это цифровой документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью удостоверяющего центра выдавшего сертификат. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель (удостоверяющий центр) удостоверяет подлинность связи между открытым ключом субъекта и информацией, его идентифицирующей (см. рис.5).

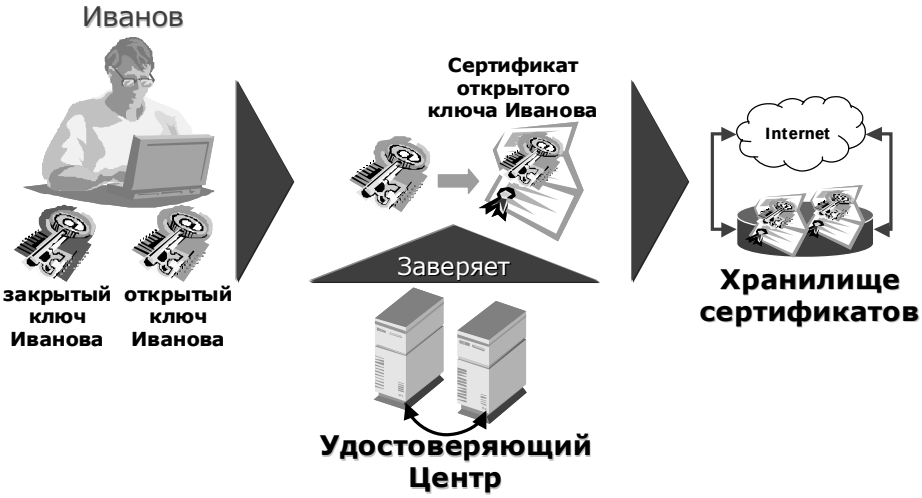

Рис. 5. Схема формирования сертификата открытого ключа.

В настоящее время наиболее часто используются сертификаты на основе стандарта Международного союза телекоммуникаций ITU-T X.509 v3 и рекомендаций IETF (Internet Engineering Task Force) RFC 2459.

Удостоверяющий Центр

Удостоверяющий Центр - это служба, которая выдает сертификаты. Удостоверяющий Центр является гарантом связи между открытым ключом субъекта и содержащейся в сертификате информацией по идентификации этого субъекта. Различные УЦ устанавливают и гарантируют эту связь различными способами, поэтому прежде чем доверять сертификатам того или иного УЦ, следует ознакомиться с его политикой и регламентом.

Удостоверяющие центры являются одной из основных составляющих ИОК. При построении ИОК в информационной системе с существенно распределенной структурой (например, организация с большим количеством подразделений или информационная

система, объединяющая несколько организаций) встает задача построения и объединения в единую сеть нескольких Удостоверяющих центров.

Наибольшее распространение получила иерархическую модель построения Удостоверяющих центров. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом коммерческих продуктов и УЦ различных поставщиков. Простейшая форма иерархии УЦ состоит из одного УЦ, а в общем случае – из множества УЦ с явно определенными отношениями родительский – дочерний (см. рис.6).

В иерархической модели дочерние Удостоверяющие Центры сертифицируются родительским. Удостоверяющий центр, находящийся на самом верхнем уровне иерархии, обычно называется корневым. Подчиненные УЦ являются промежуточными или выдающими УЦ. Выдающим УЦ называется тот удостоверяющий центр, который выдает сертификаты конечным пользователям. Промежуточным УЦ называется тот УЦ, который не является корневым и выдает сертификаты только другим УЦ, а не конечным пользователям.

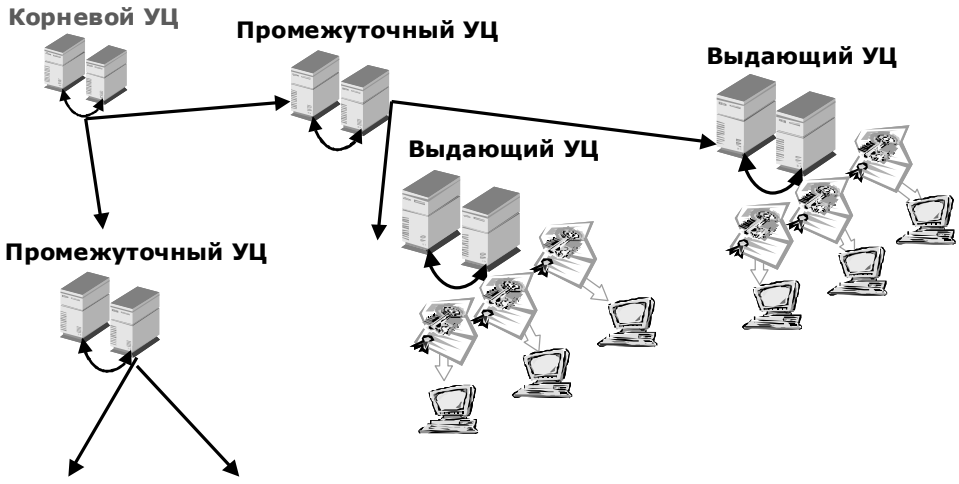

Рис. 6. Иерархическая модель объединения Удостоверяющих Центров.

Фундаментальное преимущество этой модели состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых УЦ. В то же время эта модель позволяет иметь различное число УЦ, выдающих сертификаты.

Список отозванных сертификатов

Удостоверяющие центры периодически выпускают списки отозванных сертификатов, в которых фиксируются сертификаты пользователей, вышедшие из обращения в системе.

Список отозванных сертификатов (CRL – Certificate Revocation List) – это цифровой документ, который содержит перечень сертификатов, являющихся отозванными из обращения в УЦ. Удостоверяющий центр поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов. Абоненты могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

Технологии на основе ИОК

1. Электронные цифровые подписи

Одно из самых распространенных применений алгоритмов шифрования с открытыми ключами – **электронная цифровая подпись (ЭЦП)**. Часто оказывается необходимым не зашифровывать содержимое электронного документа, а установить его авторство и подлинность.

Основой электронной цифровой подписи является математическое преобразование подписываемых данных с использованием личного закрытого ключа подписывающего и выполнением следующих условий.

- Создать электронную цифровую подпись можно только с использованием личного закрытого ключа.
- Проверить действительность электронной цифровой подписи может любой, имеющий доступ к соответствующему открытому ключу.
- Любое изменение подписанных данных (даже изменение всего одного бита в большом файле) делает электронную цифровую подпись недействительной.

При использовании цифровой подписи информация не шифруется и остается доступной любому пользователю, имеющему к ней доступ.

Процесс подписи документа

Процесс подписи документа выглядит следующим образом. На первом шаге строится специальная функция (хэш-функция), напоминающая контрольную сумму, она идентифицирует содержимое документа (создается "дайджест" документа).

На втором шаге автор документа шифрует содержимое хэш-функции своим персональным закрытым ключом. Зашифрованная хэш-функция помещается в то же сообщение, что и сам

документ. Цифровая подпись является производной “дайджеста” и личного закрытого ключа, чем гарантируется её абсолютная уникальность (см. рис.7).

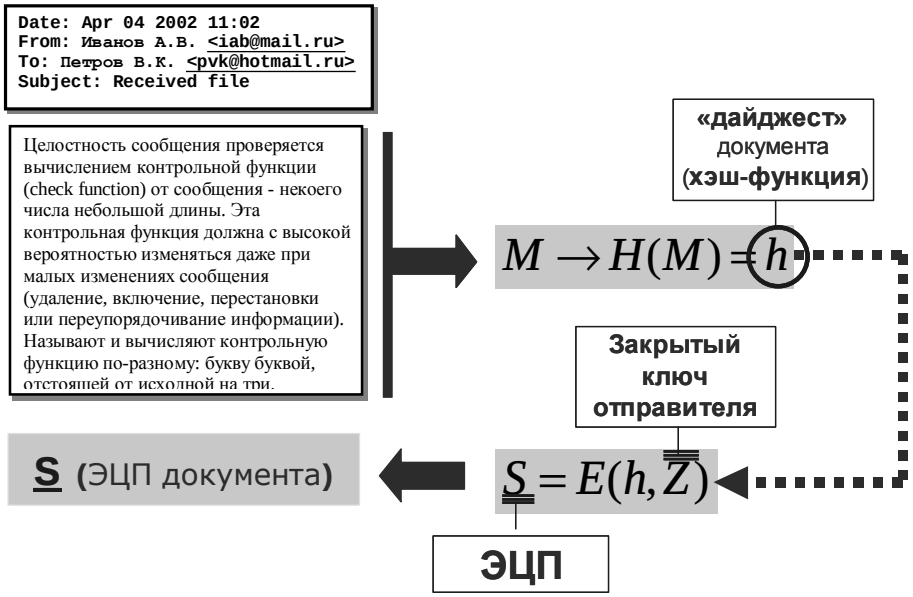

Рис. 7. Алгоритм формирования ЭЦП.

Используемая в алгоритме ЭЦП хеш-функция должна удовлетворять ряду требований, а именно:

- сообщение любой длины должно преобразовываться в бинарную последовательность фиксированной длины;
- полученная хешированная версия сообщения должна зависеть от каждого бита исходного сообщения и от порядка их следования;
- по хешированной версии сообщения нельзя никакими способами восстановить само сообщение.

Алгоритм верификации электронной подписи

Алгоритм верификации электронной подписи состоит в следующем. На первом этапе получатель сообщения строит собственный вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержащейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш-

функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства (см. рис.8).

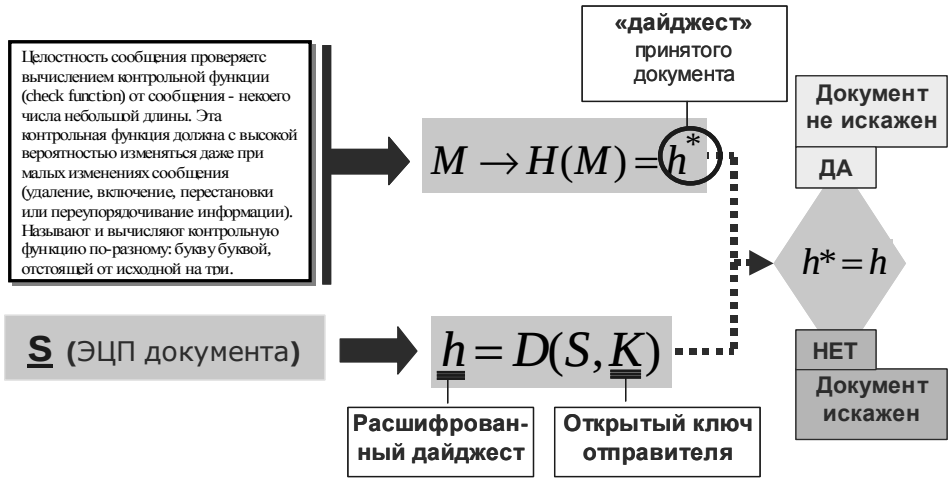

Рис. 8. Алгоритм верификации ЭЦП.

Электронную цифровую подпись, как и любые другие данные, можно передавать вместе с подписанными, то есть защищенными ею данными. Кроме того, цифровая подпись позволяет убедиться в том, что данные при передаче адресату не были изменены (случайно или преднамеренно).

Шифрование и электронная подпись могут с успехом применяться вместе. Сначала можно подписать документ личным закрытым ключом, а потом зашифровать открытым ключом адресата. Подпись удостоверяет личность, шифрование защищает письмо от чужих глаз.

2. Проверка подлинности

Криптография с открытыми ключами обеспечивает надежные службы распределенной идентификации, аутентификации и авторизации. Такого рода задачи возникают при любом факте доступа субъекта (пользователя системы) к информации. В частности при подключении клиента к серверу в условиях открытого канала (Интернет).

Идентификационные данные клиента и сервера присутствуют в соответствующих сертификатах открытых ключей, выданных единым удостоверяющим центром, либо удостоверяющими центрами из одной иерархии. Таким образом, при подключении клиента к серверу можно произвести взаимную идентификацию.

Аутентификация – проверка принадлежности клиенту или серверу предъявленного им идентификатора – можно реализовать на основе ИОК и соответствующих сертификатов открытых ключей.

Аутентификация возможна несколькими способами.

1. Сервер посылает клиенту запрос на подтверждение подлинности зашифрованный открытым ключом клиента, полученным из сертификата открытого ключа клиента. Клиент расшифровывает запрос личным закрытым ключом и возвращает серверу, подтвердив таким образом, что он является владельцем соответствующего закрытого ключа, и, следовательно, идентификационные данные в сертификате принадлежат именно ему.
2. Сервер посылает запрос на подтверждение подлинности открытым текстом. Клиент отвечает на запрос, подписав его собственной электронной цифровой подписью. Сервер проверяет ЭЦП клиента с помощью открытого ключа полученного из сертификата открытого ключа клиента и удостоверяется в том, что клиент действительно имеет соответствующий личный закрытый ключ.

Описанная схема называется протоколом доказательства владения (proof-of-possession), поскольку отправитель доказывает, что он владеет требуемым для дешифрации и создания электронной цифровой подписи личным секретным ключом.

3. Согласование общего секретного ключа сессии

Криптография с открытыми ключами также позволяет двум сторонам согласовать общий секретный ключ сессии при обмене информацией через незащищенные каналы связи.

Схема выработки общего ключа сессии выглядит следующим образом. Сначала клиент и сервер генерируют по одному случайному числу, которые используются как половины их общего секретного ключа сессии. Затем клиент отправляет серверу свою половину секретного ключа, зашифрованную открытым ключом, полученным из сертификата открытого ключа сервера. Сервер отправляет клиенту свою половину, зашифрованную открытым ключом, полученным из сертификата открытого ключа клиента. Каждая из сторон расшифровывает полученное сообщение с недостающей половиной секретного ключа, и создает из этих двух половин общий секретный ключ. Выполнив такой протокол, стороны могут пользоваться общим секретным ключом для шифрования последующих сообщений.

4. Шифрование без предварительного обмена симметричным секретным ключом

Технология шифрования с открытым ключом позволяет шифровать большие объемы данных в том случае, если у обменивающихся информацией сторон нет общего ключа. Существующие алгоритмы шифрования с открытым ключом требуют значительно больше вычислительных ресурсов, чем симметричные алгоритмы, поэтому они неудобны для шифрования больших объемов данных. Однако можно реализовать комбинированный подход с использованием, как симметричного шифрования, так и шифрования с открытым ключом.

Сначала выбирается алгоритм шифрования с секретным ключом (ГОСТ 28147-89, DES и т. п.) затем создается случайный сеансовый ключ (random session key), который будет использоваться для шифрования данных.

Далее отправитель шифрует этот ключ сеанса, используя открытый ключ получателя. Затем он отправляет получателю зашифрованный ключ и зашифрованные данные. Своим личным закрытым ключом получатель расшифровывает ключ сеанса и использует его для дешифрации данных.

Подтверждение доверия ЭЦП

При получении подписанного ЭЦП сообщения, возникает вопрос доверия этой подписи (действительно ли данная ЭЦП принадлежит отправителю сообщения). Целостность подписи можно проверить с помощью известного открытого ключа отправителя и криптографических алгоритмов. Однако при этом необходимо удостовериться, что используемый для проверки открытый ключ действительно принадлежит субъекту, именем которого подписано сообщение.

Если возможно найти сертификат открытого ключа отправителя, выданный удостоверяющим центром, которому есть доверие, тогда можно получить убедительное подтверждение того, что открытый ключ отправителя действительно принадлежит отправителю. Таким образом, можно удостовериться, что открытый ключ принадлежит именно данному отправителю, если найден сертификат, который:

- имеет действительную с криптографической точки зрения подпись его издателя;
- подтверждает связь между именем отправителя и открытым ключом отправителя;
- выдан удостоверяющим центром, которому есть доверие.

Если был найден такой сертификат открытого ключа отправителя, то подлинность этого сертификата можно проверить с помощью открытого ключа удостоверяющего центра.

Однако возникает вопрос проверки принадлежности открытого ключа данному удостоверяющему центру. Необходимо найти сертификат, заверяющий подлинность этого удостоверяющего центра.

Таким образом, в процессе проверки сертификата происходит продвижение по цепочке сертификатов (certification path). В конце цепочки сертификатов, ведущей от сертификата открытого ключа отправителя через ряд удостоверяющих центров, находится сертификат, выданный тем УЦ, которому есть полное доверие. Такой сертификат называется доверенным корневым сертификатом (trusted root certificate), поскольку он образует в иерархии связей «открытые ключи – личность» корень (самый верхний узел), который считается надежным. Если есть явное доверие данному доверенному корневому сертификату, то тогда появляется неявное доверие всем сертификатам, выданным доверенным корневым сертификатом и всеми сертифицированными им УЦ.

Набор доверенных корневых сертификатов, которым есть явное доверие – это единственная информация, которую необходимо получить надежным способом. На этом наборе сертификатов базируется система доверия и обоснование надежности инфраструктуры открытых ключей.

В общем случае при верификации сертификата необходимо проверить следующие поля сертификата:

- Тип сертификата – *сертификат разрешено использовать в данном режиме*.
- Срок действия – *сертификат действителен в данный момент*.
- Целостность – *цифровая подпись УЦ, выдавшего сертификат, верна*.
- Легитимность – *сертификат не был отозван*.
- Доверие – *сертификат корневого УЦ присутствует в хранилище «доверенные корневые УЦ»*.
- Запреты – *списки CTL не запрещают использование сертификата для данной задачи*.

Отзыв сертификатов открытых ключей

Инфраструктура открытых ключей требует секретного хранения закрытых ключей пользователей. Наиболее часто закрытые ключи хранятся на специальных съемных ключевых носителях (дискета, процессорные карты, таблетки Touch-Memory, электронный ключ или сменный носитель с интерфейсом USB и пр.). Ключевые носители необходимо хранить в

защищенных хранилищах. В случае не соблюдения правил эксплуатации и хранения ключевых носителей может возникнуть ситуация компрометации ключей.

Компрометация ключей возникает в случае утраты доверия к тому, что используемые ключи обеспечивают безопасность информации.

К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

1. Потеря ключевых носителей.
2. Потеря ключевых носителей с их последующим обнаружением.
3. Увольнение сотрудников, имевших доступ к ключевой информации.
4. Нарушение правил хранения и уничтожения (окончания срока действия) закрытого ключа.
5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того что, данный факт произошел в результате несанкционированных действий злоумышленника).

Различают два вида компрометации закрытого ключа: **явную** и **неявную**. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

При компрометации ключа у пользователя он должен немедленно прекратить связь по сети с другими пользователями**.**

Пользователь (администратор безопасности организации**)** должен немедленно известить УЦ о компрометации ключей пользователя**.**

При получении сообщения о компрометации ключа одного из пользователей сети, администратор УЦ добавляет в список отозванных сертификатов сертификат, соответствующего скомпрометированному закрытому ключу. Дата, с которой сертификат считается недействительным в системе, устанавливается равной дате изготовления списка отозванных сертификатов, в который был включен отзываемый сертификат.

Сертификат открытого ключа пользователя не удаляется из базы УЦ и хранится в течение установленного срока хранения для проведения (случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭЦП.

Доверенные корневые УЦ

При использовании криптографии с открытыми ключами важнейшее значение для пользователя имеет доверие к проверке сертификата. Обычно проверка основывается на доверии к УЦ, выдавшему данный сертификат. Инфраструктура открытых ключей предполагает иерархию УЦ, в которой управление доверием основано на решении о доверии корневому УЦ. Если проверка показывает, что данный сертификат конечного пользователя является конечным звеном цепочки, ведущей к доверенному корневому УЦ, и если сертификат используется с целью, соответствующей контексту приложения, то такой сертификат считается действительным. Если какое-либо из указанных условий не соблюдено, то сертификат считается недействительным.

Пользователи имеют возможность принимать решения о доверии, затрагивающие только их самих. Они могут делать это путем установки или удаления сертификатов доверенных корневых УЦ в хранилища на своих рабочих станциях. Однако в общем случае доверительные отношения следует устанавливать как часть политики предприятия.

Обеспечение юридической значимости ЭлД с ЭЦП

Принятый 10 января 2002 года Федеральный закон № 1 «Об электронной цифровой подписи» (далее ФЗ) дает основу для построения деловых отношений между государственными организациями и юридическими лицами в режиме реального времени.

Согласно данному закону документ в электронном виде, подписанный электронной цифровой подписью, приобретает статус оригинала.

В соответствии с положениями ФЗ, электронная цифровая подпись - 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.

В соответствии с формулировками ФЗ, средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи;
- подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;
- создание закрытых и открытых ключей электронных цифровых подписей.

Одной из важнейших характеристик средства ЭЦП является возможность формирования закрытого ключа пользователя. Причем эта возможность в соответствии с ФЗ должна обеспечиваться как собственно в Удостоверяющем Центре (УЦ), так и на рабочем месте пользователя.

Под закрытым ключом электронной цифровой подписи понимается уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Электронная цифровая подпись в первую очередь предназначена для обеспечения:

- целостности информации;
- авторства информации;
- актуальности информации;
- аутентификации субъекта и информации;
- неотказуемости.

При использовании ЭЦП в различных системах документооборота необходимо:

- Обеспечить формирование ключа владельца сертификата с использованием средств ЭЦП (СКЗИ).
- Обеспечить формирование сертификата открытого ключа с использованием удостоверяющего центра.
- Обеспечить возможность указания сведений применения ЭЦП при формировании сертификата.
- Обеспечить формирование ЭЦП электронного документа с проверкой при этом срока действия сертификата и цели применения ЭЦП.

- Обеспечить верификацию ЭЦП электронного документа с проверкой при этом срока действия сертификата и цели применения ЭЦП.
- Проверить принадлежность сертификата владельцу (доверие УЦ, аннулирование сертификата).

В соответствии с формулировками ФЗ "Об ЭЦП" **сертификат ключа подписи** – это документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Сертификат открытого ключа должен включать:

- Уникальный регистрационный номер сертификата ключа подписи
- Фамилию, имя, отчество владельца сертификата ключа подписи или его псевдоним
- Даты начала и окончания срока действия сертификата ключа подписи
- Открытый ключ электронной цифровой подписи
- Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью имеет юридическое значение
- Наименование средств электронной цифровой подписи
- Наименование и место нахождения удостоверяющего центра

Удостоверяющий центр - комплекс аппаратно-программных средств и организационных мероприятий, обеспечивающих применение использования технологии с открытыми ключами в соответствии с положениями ФЗ «Об ЭЦП».

Основные функции УЦ, определенные ФЗ "Об ЭЦП".

Статья 9. Деятельность удостоверяющего центра

1. Удостоверяющий центр:

- *изготавливает сертификаты ключей подписей;*
- *создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;*
- *приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;*

- *ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;*
- *проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;*
- *выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;*
- *осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;*
- *может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.*

Применение электронной цифровой подписи в автоматизированной системе может приводить к конфликтным ситуациям, заключающимся в оспаривании сторонами (участниками системы) авторства и/или содержимого документа, подписанного электронной цифровой подписью (ЭЦП).

Разбор подобных конфликтных ситуаций в соответствии с действующим законодательством и особенностями формирования самой электронной цифровой подписи требует применения специального программного обеспечения для выполнения проверок и документирования данных, используемых при выполнении процедуры проверки соответствия ЭЦП содержимому электронного документа.

Разбор конфликтной ситуации заключается в доказательстве авторства подписи конкретного электронного документа конкретным исполнителем.

Для разбора конфликтных ситуаций, связанных с использованием ЭЦП, подтверждения подлинности электронной цифровой подписи в электронном документе и в выданных УЦ сертификатов, в состав УЦ входит АРМ разбора конфликтных ситуаций.

Разбор конфликтной ситуации выполняется по инициативе любого участника автоматизированной системы и состоит из:

- предъявления претензии одной стороны другой;
- формирования комиссии;
- разбора конфликтной ситуации;

- взыскания с виновной стороны принесенного ущерба, если это определено соглашениями сторон.
- Проверка изданного сертификата открытого ключа подписи включает в себя выполнение следующих действий:
- определение сертификата, необходимого для проверки ЭЦП издателя;
- проверка ЭЦП издателя сертификата открытого ключа, путем построения цепочки сертификатов до сертификата доверенного корневого УЦ;
- проверка действительности сертификатов на текущий момент времени;
- проверка отсутствия сертификатов в списке отозванных сертификатов (CRL).

ГЛАВА 4. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭЦП

В операционных системах семейства MS Windows присутствуют специальные криптографические модули для работы с симметричной и асимметричной криптографией. Приложения, использующие криптографические модули операционной системы, функционируют в соответствии с программным интерфейсом CryptoAPI, описывающим стандартные процедуры взаимодействия высокоуровневого приложения с низкоуровневыми криптографическими модулями.

В базовый пакет ОС MS Windows входят приложения, такие как MS Outlook Express и MS Internet Explorer, позволяющие использовать Инфраструктуру Открытых Ключей в технологиях электронной почты и WEB.

В ОС MS Windows может присутствовать большое количество сертификатов открытых ключей (сертификаты корневых УЦ, сертификаты промежуточных УЦ, сертификаты других пользователей, личные сертификаты и т.д.). Сертификаты организованы в виде хранилищ в соответствии с категорией владельца сертификата.

В ОС MS Windows для поддержки криптографическими модулями российских криптоалгоритмов необходимо инсталлировать дополнительное криптографическое программное обеспечение (криптографическое ядро) сторонних разработчиков. В соответствии с российскими государственными нормативно-правовыми требованиями криптографическое ядро должно быть сертифицировано уполномоченными государственными органами.

Одним из наиболее распространенных криптографических ядер, реализующих российские криптоалгоритмы, является средство криптографической защиты информации (СКЗИ) «КриптоПро CSP», разработанное фирмой «Крипто-Про». Данное криптоядро позволяет приложениям взаимодействовать через стандартный интерфейс CryptoAPI с криптографическими модулями, реализующими российские криптоалгоритмы.

Основные сервисные функции СКЗИ «КриптоПро CSP»

Доступ к настройкам СКЗИ можно получить используя пункты меню **Пуск, Настройка, Панель управления** в окне панели управления выберите значок **КриптоПро CSP**. Модуль управления КрптоПро CSP представлен в виде нескольких вкладок, объединенных в соответствии с функциональным назначением.

- Вкладка **Общие** – информация о версии ПО и ввод лицензии.
- Вкладка **Оборудование** – управление ключевыми носителями (добавление, удаление, конфигурирование) и датчиками случайных чисел.
- Вкладка **Безопасность** – настройка правил хранения и обращения ключей на локальном компьютере.
- Вкладка **Дополнительно** – настройка времени ожидания ввода.
- Вкладка **Алгоритмы** – настройка криптоалгоритмов.
- Вкладка **Сервис** – сервисные функции работы с ключевыми контейнерами и сертификатами.

Подробную информацию по сервисным функциям можно найти в руководстве пользователя СКЗИ КриптоПро.

1. Ключевой контейнер

При формировании закрытые ключи записываются на ключевой носитель (в ключевой контейнер).

Ключевой контейнер может содержать:

- только ключ подписи;
- только ключ шифрования;
- ключ подписи и ключ шифрования одновременно.

Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т.п.

Каждый контейнер (независимо от типа носителя), является полностью самостоятельным и содержит всю необходимую информацию для работы, как с самим контейнером, так и с закрытыми (соответствующими им открытыми) ключами.

Реализация КриптоПро CSP позволяет хранить личные сертификаты пользователя не только в локальном справочнике сертификатов компьютера, а так же вместе с личными ключами пользователя на ключевом носителе. При этом сертификат может храниться в виде записей в ключевом контейнере или в виде отдельного файла.

Хранение сертификата на ключевом носителе позволяет пользователю переносить всю необходимую ключевую информацию с компьютера, где был сформирован ключ пользователя на другие рабочие места.

В процессе работы с ключами (генерация ключей, использование в процедурах формирования подписи, аутентификации и шифрования), имеется возможность установки на ключевой контейнер дополнительного средства защиты ключевого контейнера - пароля (ПИН-кода). Сменить пароль на ключевой контейнер можно в настройках КриптоПро вкладка «Сервис», кнопка «Изменить пароль».

2. Использование ключей и сертификатов на компьютере

Для того, чтобы воспользоваться личными ключами и сертификатами пользователя в различных приложениях на другом компьютере, необходимо на этом компьютере установить пользовательский сертификат в локальный справочник и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

В окне модуля управления КрптоПро CSP перейдите на вкладку **Сервис**.

Если сертификат пользователя интегрирован в ключевой контейнер, то нажмите кнопку **«Просмотреть сертификаты в контейнере»** и следуйте указаниям мастера. Ключевой носитель, содержащий личный ключ и сертификат, при этом должен быть вставлен в соответствующее устройство считывания. Если на ключевом носителе содержится сертификат, его содержание будет отображено в стандартном окне просмотра сертификатов. Нажмите кнопку «**Установить сертификат»** для его переноса с ключевого носителя в локальный справочник.

Если сертификат пользователя находиться на ключевом носителе в виде отдельного файла, то воспользуйтесь мастером **«Установить личный сертификат».**

Менеджмент сертификатов на локальном компьютере

В ОС MS Windows присутствуют встроенные средства управления сертификатами открытых ключей (добавление, удаление, перенос, просмотр и пр.) такие как менеджер сертификатов (реализовано начиная с MS Windows 95) и консоль управления сертификатами (начиная с MS Windows 2000).

Установить сертификаты из файлов (тип файлов .cer и .p7b) можно выбрав в контекстном меню файла пункт **Установить сертификат**.

Для запуска приложения «**Менеджер сертификатов»** нужно открыть **Свойства обозревателя** (в панели управления или в Internet Explorer), вкладка **Содержание**, кнопка **Сертификаты**. Менеджер отображает содержимое хранилищ сертификатов, доступных для данного пользователя и позволяет выполнять различные операции с сертификатами.

Для формирования **консоли управления сертификатами** создайте пустую консоль (команда **mmc**), добавьте в консоль оснастку управления сертификатами (меню **Консоль** -> **Добавить или удалить оснастку** -> кнопка **Добавить** -> оснастка **Сертификаты**). Консоль позволяет управлять сертификатами в хранилищах доступных для локального компьютера и/или пользователя. Отображаются все хранилища сертификатов присутствующие в ОС.

Функции ЭЦП и шифрования в MS Outlook Express

Программное обеспечение Outlook Express версии 5.0 и выше полностью поддерживает Инфраструктуру Открытых Ключей для обеспечения конфиденциальности, целостности авторства почтовых сообщений, передаваемых по протоколам SMTP, IMAP, POP3. Для этих целей Outlook Express использует функции CryptoAPI 2.0 и сертификаты открытых ключей X.509. В качестве формата защищенных сообщений используется формат, описанный в рекомендациях Secure Multipurpose Internet Mail Extensions (S/MIME).

1. Конфигурация Outlook Express

Для создания или редактирования учетных записей электронной почты выберите **Сервис**, **Учетные записи** и нажмите на закладку **Почта**. Для создания новой учетной записи нажмите **Добавить**, **Почта**. Для редактирования учетной записи в списке учетных записей, выберите ту, которую необходимо настроить и нажмите кнопку **Свойства**. Для настройки использования ЭЦП выберите закладку **Безопасность** в отображаемом диалоге. Отображаемый диалог позволяет пользователю указать свои личные сертификаты, которые будут использоваться при выборе личных ключей пользователя для формирования электронной цифровой подписи и расшифрования входящих сообщений. В диалоге выбора сертификат отображаются только сертификаты, имеющие совпадающий адрес электронной почты и разращенные для защиты электронной почты.

В меню **Сервис**, **Параметры** на вкладке **Безопасность** можно включить режимы автоматического шифрования и ЭЦП каждого сообщения. Если эти режимы не включены, опции шифрования и подписи нужно будет включать для каждого отправляемого сообщения. Кнопка **Дополнительно** вызывает окно с настройками отправки и проверки сертификатов.

2. Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **Создать сообщение** или выберите пункт меню **Файл, Создать, Сообщение**. Заполните необходимые поля письма. Для отправки сообщения в подписанном виде проверьте что кнопка **Подписать**

нажата и виден признак подписанного сообщения в правой части экрана. Нажмите кнопку **Отправить.**

3. Шифрование сообщений

Для шифрования сообщений в адрес других пользователей необходимо предварительно произвести обмен сертификатами. Для этого обычно достаточно переслать подписанное сообщение в адрес требуемого абонента (сообщение посылается вместе с сертификатом отправителя). После получения сообщения и проверки электронной цифровой подписи производится добавление (автоматическое или нет) адресата отправителя и его сертификата в адресную книгу.

Для отправки зашифрованного сообщения в окне создания сообщения нажмите кнопку **Шифрование,** появиться признак шифрованного сообщения в правой части экрана. Шифрованное сообщение можно подписать ЭЦП нажав кнопку **Подписать**.

Удостоверяющий центр КриптоПро

Основные компоненты программно-аппаратного комплекса Удостоверяющий центр КриптоПро:

- Центр сертификации (ЦС)
- Центр регистрации (ЦР)
- Автоматизированное рабочее место (АРМ) администратора
- АРМ пользователя

Центр сертификации предназначен для формирования сертификатов открытых ключей пользователей и администраторов Удостоверяющего центра, списков отозванных сертификатов, хранения эталонной базы сертификатов и списков отозванных сертификатов. ЦС взаимодействует только с Центром регистрации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

Центр регистрации предназначен для хранения регистрационных данных пользователей, запросов на сертификаты и сертификаты пользователей, предоставления интерфейса взаимодействия пользователей и Удостоверяющего центра. ЦР взаимодействует с ЦС по отдельному сегменту локальной сети с использованием защищенного сетевого протокола. Взаимодействие пользователей с Удостоверяющим центром обеспечивается за счет использование АРМ пользователя, предоставляемого ЦР пользователю.

Компонент **АРМ Администратора ЦР** предназначен для выполнения организационно-технических мероприятий, связанных с регистрацией пользователей, формированием служебных ключей и сертификатов пользователей и управления Центром регистрации. АРМ администратора взаимодействует с Центром регистрации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

Компонент **АРМ пользователя ЦР** представляет собой WEB-приложение, размещенное на сервере ЦР, и предназначено для выполнения организационно-технических мероприятий, связанных с управлением личной ключевой информацией и сертификатами, такими как формирование служебных ключей и сертификатов, отзыв сертификатов, установка списка отозванных сертификатов. АРМ пользователя функционирует в ОС Microsoft Windows 95 и выше (с установленным MS IE 5.0 и выше). АРМ пользователя взаимодействует с Центром регистрации по протоколу HTTP(S).

1. Процесс взаимодействия пользователей с УЦ

Процесс регистрации пользователей в УЦ предусматривает централизованное изготовление служебных (закрытых) ключей и сертификатов пользователей администратором безопасности. Служебные ключи предназначены для подтверждения подлинности пользователя при формировании им рабочих закрытых ключей и передаче запроса на сертификат в Центр регистрации УЦ. Запрос на сертификат от пользователя будет обработан Центром регистрации только в случае, если он подписан служебным ключом или действующим закрытым ключом пользователя.

После процесса регистрации пользователи с использованием служебных ключей и сертификатов должны получить сформировать рабочие ключи и получить рабочие сертификаты. Рабочие ключи предназначены для формирования ЭЦП, выполнения операций шифрования сообщений, аутентификации пользователя при его взаимодействии с ЦР и плановой смене ключей.

Перед началом работы с АРМ пользователя ЦР необходимо установить сертификат УЦ (цепочку сертификатов от коревого УЦ до данного УЦ) и личный сертификат с ключевого носителя, полученного от администратора ЦР.

Для запуска и работы с АРМ пользователя необходимо открыть окно браузера MS Internet Explorer и перейти по адресу нахождения ЦР.

Для аутентификации пользователя на ЦР и получения доступа к АРМ пользователя необходимо в процессе запуска выбрать сертификат пользователя, по которому будет выполняться процедура аутентификации. Данный выбор происходит в окне проверки подлинности клиента приложения MS IE.

АРМ пользователя представляет собой окно браузера MS IE, содержащего кнопки сервисных функций (создание запроса на новый сертификат пользователя, получение сертификата УЦ, получение списка отозванных сертификатов, поиск по базе сертификатов), а также списков (в виде таблиц) личных сертификатов, запросов на сертификаты и запросы на отзыв сертификатов.

Для формирования запроса на новый сертификат нажмите ссылку «Новый сертификат», выберите тип сертификата и нажмите кнопку «Отправить». Сгенерируйте ключи. Для этого в соответствии с запросами ПО АРМ пользователя выберите необходимый тип ключевого носителя, установите пароль (ПИН-код) на создаваемый ключевой контейнер, проинициализируйте генератор случайных чисел (путем нажатия клавиш на клавиатуре или движением указателя мышки в окне инициализации). В результате выполнения данных действий в окне АРМ, в таблице запросов на сертификаты появиться новая строка с информацией о сформированном запросе. Столбец «Статус» данной таблицы содержит текущее состояние обработки данного запроса на Центре регистрации. Завершение обработки запроса на сертификат и наличие возможности установить выпущенный сертификат, свидетельствует установление статуса запроса на сертификат в состояние «Установить». Установите сертификат, нажав ссылку «Установить».

ГЛАВА 5. ТИПОВЫЕ ЗАДАНИЯ ЛАБОРАТОРНЫХ И ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Задание 1

1. Установите сертификат удостоверяющего центра и личный служебный сертификат с ключевого носителя.
2. С помощью средств менеджмента сертификатов определите, в какие хранилища были установлены сертификаты.
3. В свойствах установленных сертификатов найдите полную информацию о субъектах – владельцах сертификатов, сроках действия сертификатов, информацию об издателях и области применения сертификатов.
4. Используя модуль управления «Крипто-Про CSP» измените пароль на личный ключевой контейнер служебных ключей.
5. Подключитесь к центру регистрации УЦ, адрес ЦР получите у лаборанта. По средствам АРМ пользователя ЦР запросите новый сертификат и установите его в систему. В свойствах сертификата найдите значения полей срок действия и область применения сертификата.
6. По средствам АРМ пользователя ЦР отзовите служебный сертификат. Отключитесь от ЦР и произведите попытку повторного подключения с авторизацией по служебному сертификату. Результат поясните.
7. Удалите служебный сертификат из локального хранилища.
8. Определите дату выпуска последнего списка отозванных сертификатов УЦ и дату следующего выпуска.
9. С помощью АРМ пользователя ЦР найдите в реестре сертификатов УЦ сертификат пользователя, полученный студентами соседнего рабочего места. Параметры поиска поясните.

Задание 2

На основе ПО MS Outlook Express организуйте простую систему защищенного электронного документооборота с ЭЦП.

1. Нарисуйте схему движения документов с пояснениями по стадиям. На этапах использования ЭЦП и шифрования поясните применение открытых, закрытых ключей и сертификатов открытых ключей.
2. Создайте в MS Outlook Express учетную запись пользователя в соответствии с данными указанными в личном сертификате открытых ключей, адрес почтового сервера получите у лаборанта.
3. Настройте MS Outlook Express для использования средств ЭЦП и шифрования.
4. Выполните обмен подписанными и зашифрованными сообщениями (документами) с несколькими пользователями.

Задание 3

Цель задания: изучить особенности реализации конкретной системы защищенного электронного документооборота с ЭЦП и получить навыки практической работы с такого рода системами.

1. Получите у лаборанта необходимые методические материалы.
2. Составьте схему движения документов. Укажите этапы использования ЭЦП и шифрования, поясните применение открытых, закрытых ключей и сертификатов открытых ключей на соответствующих этапах.
3. При необходимости настройте программное обеспечение в соответствии с методическими рекомендациями.
4. Проведите сеанс работы в системе с прохождением всех этапов движения документа.
5. В соответствии с методическими рекомендациями выполните дополнительные практические задания.

ГЛАВА 6. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ПО ТЕМАТИКЕ

Выдержки из нормативных документов.

информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих ин формационные процессы;

электронный документ - документ, в котором информация представлена в электронно-цифровой форме;

электронная цифровая подпись - 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;

владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

ключевой документ - физический носитель, содержащий ключевую информацию

ключевой носитель - физический носитель, предназначенный для размещения на нем ключевой информации дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.);

средства криптографической защиты информации (СКЗИ) - аппаратные, программные или аппаратно-программные средства, выполняющие какую-либо из следующих функций: реализация криптографического преобразования информации; изготовление и распределение ключевых документов.

орган криптографической защиты - организация (или ее структурное подразделение) обладающая лицензией ФСБ (ФАПСИ) на предоставление услуг конфиденциальной связи с использованием СКЗИ.

компрометация криптоключей - хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА ПО ТЕМЕ

1. Гайдамакин Н.А. - Автоматизированные информационные системы, базы и банки данных. - М.: Гелиос АРВ, 2002. – 367с.
2. Информационные технологии в бизнесе: Энцикл. - СПб. и др.: Питер, 2002. - 1120 с.
3. Петров В.Н. - Информационные системы: Учеб. пособия для студентов вузов. - СПб. и др.: Питер, 2003. - 688 с.
4. Ященко В.В. - Введение в криптографию: Новые математические дисциплины. - СПб. и др.: МЦНМО; Питер, 2001. - 288с.
5. Горбатов В.С. - Основы технологии PKI. - М.: Горячая линия-Телеком, 2004. - 248с.
6. Леонтьев К.Б. - Комментарий к Федеральному Закону "Об электронной цифровой подписи" (постатейный). - М.: Проспект : ТК Велби, 2003. - 64 с.