Тема 6. Защита информации в электронном документообороте

Цели:

- формирование представления об электронной подписи и защите электронных документов с ее помощью.

Задачи:

- познакомиться с принципами формирования электронной подписи;
- рассмотреть порядок работы с ключами электронной подписи;
- изучить правовые аспекты применения электронной подписи.

Вопросы темы:

1. Электронная цифровая подпись в системах автоматизации делопроизводства и документооборота. Основные понятия.
2. Принципы формирования ЭЦП. Функции хэширования.
3. Работа с ключами.
4. Правовые аспекты применения электронной подписи.
5. Новые формы электронной подписи.

Теоретический материал

Вопрос 1. Электронная цифровая подпись в системах автоматизации делопроизводства и документооборота. Основные понятия.

В современном, оснащенном компьютерами предприятии, документы создаются и перемещаются в электронном виде. Даже входящие документы, зачастую переводятся на этапе их регистрации в электронную форму. Бумажный текст сканируется, получается электронный графический образ документа, который затем автоматически преобразовывается в текстовый файл. Дальнейшая рассылка документа идет уже в электронной форме (рисунок 21).

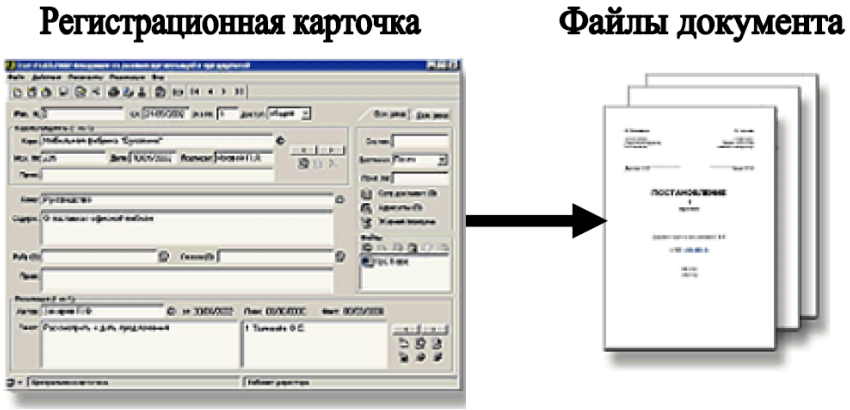

Рис. 21. Структура электронного документа

При этом необходимость подписания документов остается. Ведь перевод документов в другую форму, сам по себе не изменяет сложившихся методов управления организацией. Документы адресуются людям, и подписи на документах ставятся для будущих читателей этих документов. А цель подписи одна - удостоверить, что именно этот документ подписан именно этим человеком. Когда мы получаем подписанный бумажный документ, то мы видим подпись человека на этом документе и вряд ли задумываемся о том, что его содержимое могло быть изменено.

Но то, что очевидно при работе с бумажными документами, становится совершенно неочевидным при работе с их электронными аналогами. В документе или в его описании, называемом регистрационной карточкой, есть информация о том, кто и когда подписал документ. Но потенциальный читатель документа хочет быть уверен, что документ подписал именно этот человек, и с момента подписания документа, его содержание не изменилось. То есть, этот документ - подлинник, поэтому ему можно доверять, как доверяют бумажному документу. Данную задачу и решает ЭЦП – электронная цифровая подпись, которая является аналогом собственноручной подписи человека для электронных документов. Более того, ЭЦП может служить аналогом всякого рода печатей и штампов организации.

Электронная цифровая подпись - средство, позволяющее на основе криптографических методов надежно установить авторство и подлинность документа.

Защита данных с помощью криптографических преобразований (преобразование данных шифрованием) - одно из возможных решений проблемы их безопасности.

Криптография предполагает наличие трех компонент: данных, ключа связи и криптографического преобразования.

При шифровании исходными данными будет сообщение, а результирующими - зашифрованное сообщение. При расшифровке они меняются местами.

Ключ - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных. В данном случае термин «ключ» означает уникальный битовый шаблон. Считается, что правила криптографического преобразования известны всем, но, не зная ключа, с помощью которого пользователь закрыл смысл сообщения, требуется потратить невообразимо много усилий на восстановление текста сообщения. Длина ключа, согласно ГОСТ 28147- 89, равна 256 бит.

Вопрос 2. Принципы формирования ЭЦП. Функция хеширования.

При построении цифровой подписи вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между документом, секретным и общедоступным ключами, а также цифровой подписью. Невозможность подделки электронной цифровой подписи опирается на очень большой объем необходимых математических вычислений.

Мероприятия по защите ключа цифровой подписи от несанкционированного использования и подмены должны охватывать весь его жизненный цикл, включая генерацию, распределение, хранение, использование и выведение из действия.

Создание (генерация) ключей цифровой подписи может производиться владельцем самостоятельно или осуществляться специальным уполномоченным органом.

Каждый из этих подходов имеет свои преимущества и недостатки. При централизованной генерации ключей легче обеспечить их качество за счет использования аппаратных датчиков случайных чисел и более надежного контроля за применяемыми программно-аппаратными средствами. Недостатком является потенциальная возможность доступа к закрытому ключу цифровой подписи лиц, осуществляющих его генерацию и запись на носитель информации. Присутствие владельца ключа при его генерации и формировании ключевых носителей позволяет проконтролировать только действия оператора. Внутренние процессы, происходящие в программно-аппаратном комплексе, при этом контролю не поддаются, что не позволяет гарантировать конфиденциальность изготовленных закрытых ключей.

Самостоятельная генерация ключей их владельцем позволяет избежать доступа к закрытому ключу посторонних. Однако проблемы обеспечения качества генерируемых ключей в этом случае ему необходимо решать самостоятельно. Место генерации также существенным образом влияет на организацию распределения ключей.

Каждый абонент, обладающий правом подписи, самостоятельно на отдельном ПК формирует два ключа подписи: секретный и открытый.

Секретный (закрытый) ключ используется для выработки подписи. Только секретный ключ гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего. Каждый пользователь системы цифровой подписи должен обеспечить сохранение в тайне своего секретного ключа.

Открытый ключ вычисляется как значение некоторой функции от секретного, но знание открытого ключа не дает возможности определить секретный ключ. Открытый ключ может быть опубликован и используется для проверки подлинности документа и цифровой подписи, а также для

предупреждения мошенничества со стороны заверяющего в виде отказа его от подписи документа.

Открытым ключом можно пользоваться только в том случае, если известны его подлинность и авторство, которые подтверждаются сертификатом «центра». Поэтому во избежание попыток подделки или внесения искажений обмен и хранение открытых ключей должны осуществляться в защищенном виде. Для этого при обмене открытыми ключами можно использовать секретный канал связи или в открытом канале связи средства электронной цифровой подписи, а при работе с системами криптографической защиты информации (СКЗИ) необходимо контролировать целостность справочника открытых ключей.

Таким образом, каждому пользователю, обладающему правом подписи, необходимо иметь лишь один секретный ключ и справочник регистрационных записей открытых ключей абонентов сети. Если пользователь не обладает правом подписи, но в процессе работы ему необходимо проверять подписи, проставленные под документами, он должен иметь лишь справочник открытых ключей.

Для формирования справочника существует несколько возможностей. Например, список открытых ключей может формироваться в «центре» (под «центром» понимается выделенный пользователь, обладающий особыми полномочиями), которому доверяют все пользователи системы. «Центр» получает готовую регистрационную карточку открытого ключа абонента, формирует справочник открытых ключей, рассылает готовый справочник абонентам сети и контролирует его целостность и истинность.

Электронная цифровая подпись может быть реализована на базе асимметричного криптографического алгоритма согласно ГОСТ Р 34.10-94. Электронная цифровая подпись вырабатывается на основе текста документа, требующего заверения, и секретного ключа. Согласно стандарту документ «сжимают» с помощью функции хэширования (ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хеширования»).

Однонаправленная хэш-функция получает на входе сообщение переменной длины и преобразует его в хэш-значение фиксированной длины (256 бит согласно ГОСТ Р 34.11-94). Значение хэш-функции сложным образом зависит от документа, но не позволяет восстановить сам документ. Хэш-функция чувствительна к всевозможным изменениям в тексте. Кроме того, для данной функции нельзя вычислить, какие два исходные сообщения могут генерировать одно и то же хэш-значение, поскольку хэш-значения двух 256-битовых документов могут совпасть в одном из 2^{256} (10^{77}) случаев. Далее, к полученному хэш-значению применяется некоторое математическое преобразование и получается собственно подпись документа.

При проверке подписи проверяющий должен располагать открытым ключом абонента, поставившего подпись. Проверяющий должен быть

полностью уверен в его подлинности, которая подтверждается сертификатом «центра».

Процедура проверки подписи состоит из вычисления хэш-значения документа и проверки некоторых соотношений, связывающих хэш-значение документа, подпись под этим документом и открытый ключ подписавшего абонента. Документ считается подлинным, а подпись - правильной, если эти соотношения выполняются. В противном случае документ считается измененным, и подпись под ним - недействительной.

Для разрешения споров между отправителем и получателем информации, связанных с возможностью искажения ключа проверки подписи (открытого ключа подписи), достоверная копия этого ключа может выдаваться третьей стороне (арбитру) и применяться им при возникновении конфликта. Предъявляя контролеру открытый ключ - значение некоторой функции, вычисляемое с помощью секретного ключа, пользователь косвенным образом доказывает, что обладает секретным. Наличие у абонента секретного ключа не позволяет ему самому сменить свой номер в сети или выработать подпись под номером другого абонента.

Вопрос 3. Работа с ключами.

Распределение ключей. При распределении ключей цифровой подписи решаются следующие задачи:

- доставка владельцу закрытого ключа способом, исключающим его компрометацию;
- доставка открытого ключа получателям ЭД способом, исключающим его подмену.

Необходимость решения первой задачи возникает в случае централизованной генерации ключей. Ключи могут выдаваться владельцам лично, передаваться через третьих лиц на носителях информации или пересылаться по закрытым каналам связи.

Наиболее безопасным вариантом является выдача ключей лично владельцам на месте их генерации и формирования ключевых носителей. В тех случаях, когда это невозможно по каким-либо причинам, доставка ключей владельцу может осуществляться курьером, с помощью почтовой связи, через представителя организации, имеющего соответствующую доверенность, или по каналам закрытой связи.

Если генерация ключей осуществляется владельцем самостоятельно, то остается решить задачу доставки открытого ключа получателям ЭД. Открытую часть ключа нет необходимости держать в секрете. Собственно поэтому она и называется открытой. Однако это не означает, что в процессе доставки ей ничего не угрожает. Подмена открытого ключа цифровой

подписи позволит злоумышленнику подделывать цифровые подписи, проверяемые с помощью этого ключа.

В качестве дополнительного элемента защиты открытого ключа от подмены может использоваться заверенный владельцем ключа документ на бумажном носителе, по своему содержанию аналогичный цифровому сертификату. В подлинности открытого ключа, полученного в электронном виде, можно убедиться, сверив его с отрытым ключом, содержащимся в заверенном документе на бумажном носителе.

Хранение и использование ключей. При хранении и использовании ключей цифровой подписи рекомендуется соблюдать следующие общие правила:

1. Все ключевые носители должны быть промаркированы и зарегистрированы.
2. Вне времени использования съемные ключевые носители должны помещаться в надежные хранилища: запирающиеся металлические шкафы или сейфы.
3. На несъемных носителях информации ключи должны храниться в зашифрованном виде.
4. Аппаратные и программные средства, используемые при работе с ключевыми носителями и осуществляющие криптографические операции, должны быть защищены.
5. Владельцам ключей должно быть запрещено:
    - передавать ключевые носители лицам, к ним не допущенным;
    - выводить закрытые ключи на монитор или принтер;
    - помещать ключевой носитель в устройства считывания/записи аппаратных средств, не предназначенных для их использования;
    - оставлять ключевой носитель без присмотра;
    - записывать на ключевой носитель посторонние данные.

Наиболее часто в качестве ключевых носителей используются дискеты, элементы Touch Memory, устройства, подключаемые через USB-порт - USB-токены, и смарт-карточки.

Основным преимуществом использования дискет в качестве ключевых носителей является их низкая стоимость и отсутствие расходов на приобретение дополнительного оборудования. К недостаткам можно отнести легкость несанкционированного копирования, быстрый износ, уязвимость к внешним воздействиям (магнитным полям, пыли, температурным воздействиям и т. п.).

Элементы Touch Memory являются более дорогими носителями по сравнению с дискетами. Для чтения/записи требуется специальный считыватель, подключаемый к последовательному порту компьютера. Учитывая, что для копирования информации также необходимо иметь считыватель и специальное программное обеспечение, это несколько

снижает риск несанкционированного копирования. Надежность хранения информации и устойчивость к внешним воздействиям у Touch Memory значительно выше, чем у дискет. Элементы Touch Memory сохраняют работоспособность в температурном диапазоне от –20 до +70°С. Имеется защита от статического электричества. При ношении элементов Touch Memory в специальном держателе на связке с обычными ключами от механических дверных замков риск потери информации остается незначительным.

Одним из самых надежных считается хранение ключей на смарт-картах и в специальных высокозащищенных USB-токенах, в которых пары ключей генерируются аппаратно, и ключи подписания (закрытые ключи) никогда не покидают устройство и не могут быть извлечены или перехвачены.

Смарт-карточки — один из наиболее перспективных носителей информации для ключей цифровой подписи. Они могут использоваться как в качестве обычных носителей, так и в качестве устройства, совмещающего функции хранения ключевой информации с функциями вычисления цифровой подписи. Простановка цифровой подписи в этом случае производится по следующей схеме:

1) владелец ключа принимает решение подписать ЭД, находящийся в памяти компьютера;

2) в компьютере производится вычисление хеш-кода ЭД;

3) запрашивается ПИН-код для доступа к закрытому ключу;

4) вычисленный хеш-код и ПИН-код передаются в смарт-карточку;

5) если введен правильный ПИН-код, то для полученного хеш-кода вычисляется цифровая подпись с использованием закрытого ключа;

6) вычисленная цифровая подпись передается в компьютер и связывается с подписанным ЭД.

При таком способе применения закрытый ключ цифровой подписи не будет покидать смарт-карточку, что позволяет значительно повысить его защищенность от несанкционированного копирования. Защита от несанкционированного использования обеспечивается с помощью ПИН-кода. В случае неправильного ввода ПИН-кода цифровая подпись не вычисляется или выдается случайная последовательность чисел в качестве цифровой подписи.

Выведение ключей из действия. При разработке процедуры выведения из действия ключей цифровой подписи следует учитывать, что срок действия и процедура уничтожения закрытого и открытого ключей не совпадают.

Срок действия закрытого ключа цифровой подписи — это период времени, в течение которого допускается использование этого ключа для

подписания ЭД. Данный срок должен быть явно указан в документах, определяющих принадлежность ключа владельцу.

На продолжительность устанавливаемого срока действия закрытого ключа оказывают влияние следующие основные факторы:

1) возможность появления в будущем новых методов криптоанализа и осуществления качественных прорывов в области вычислительной техники, которые могут привести к преодолению криптографической защиты;

2) снижение стойкости криптосистемы за счет накопления материала для криптоанализа при многократном использовании одного и того же ключа;

3) возрастание вероятности компрометации ключа при длительном использовании и хранении.

Провести объективный учет влияния перечисленных факторов довольно сложно. Обычно производители криптографических средств рекомендуют ограничивать период действия закрытого ключа одним годом. Однако в некоторых приложениях назначение столь короткого срока действия будет вести к неоправданно большим расходам. В частности, для ключей, используемых для подписи цифровых сертификатов, рекомендуется устанавливать срок действия не менее пяти лет.

Вопрос 4. Некоторые правовые аспекты применения ЭЦП.

Описанные выше возможности применения ЭЦП могут использоваться в корпоративных информационных системах. Статья 17 Закона «Об электронной цифровой подписи» предоставляет возможность непосредственно владельцам системы или ее участникам решать самостоятельно вопросы, связанные с порядком ведения действующих и отозванных сертификатов ключей подписей и использования подписей. При этом регламент получения, использования и отзыва подписей, а также разрешение возможных конфликтов применения ЭЦП является внутренним делом участников корпоративной системы и может решаться их внутренними нормативными документами.

ЭЦП широко использовались и до принятия закона, например в банковских сферах. Требования закона к использованию ЭЦП в сфере государственного управления (статья 16) предполагают наличие развитой инфраструктуры обеспечения применения ЭЦП и, в том числе, наличие удостоверяющих центров сертификации с «материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей» (статья 8).

Создание такой инфраструктуры требует значительного времени. До 2010 года, положения, провозглашенные в статье 1 закона, - «создание правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе», были чисто декларативными. Потребовался значительный объем практического применения, в первую очередь в сферах государственной и налоговой отчетности, чтобы закон смог работать в полную силу. ЭЦП начинает реально применяться в повседневной деятельности предприятий, пускай даже на первых порах со значительно меньшими функциональными возможностями, чем это декларировано законом. Сфера применения ЭЦП постоянно расширяется. Большой толчок к активному использованию электронной подписи дало принятие нового Федерального закона «Об электронной подписи». В настоящее время ЭП наиболее активно используется в таких областях, как сдача отчетности в электронном виде, электронные государственные закупки, системы «Клиент-банк» и «Интернет-банк», электронный документооборот государственных и муниципальных органов власти.

Вопрос 5. Новые формы электронной подписи.

Новый Федеральный закон «Об электронной подписи», принятый 6 апреля 2011, определяет три вида электронной подписи:

1. простая электронная подпись;
2. усиленная неквалифицированная электронная подпись;
3. усиленная квалифицированная электронная подпись.

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной электронной подписью является электронная подпись, получаемая в результате криптографического преобразования информации с использованием ключа электронной подписи и средств электронной подписи и позволяющая определить лицо, подписавшее электронный документ, и обнаружить факт внесения изменений в электронный документ после момента его подписания.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи, кроме того имеется ключ проверки электронной подписи, указанный в квалифицированном сертификате и для создания и проверки электронной подписи используются средства электронной подписи,

получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения должны предусматривать порядок проверки электронной подписи.

Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

Электронный документ считается подписанным простой электронной подписью если она содержится в самом электронном документе и ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ. При этом соглашения, подписанные между участниками электронного взаимодействия, должны содержать правила определения лица, подписывающего электронный документ, а также обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

Использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны строго соблюдать конфиденциальность процесса проставления электронной подписи и обеспечивать конфиденциальность ключей.

При создании электронной подписи средства электронной подписи должны показывать подписывающему лицу содержание подписываемой информации, создавать электронную подпись только после подтверждения операции по созданию электронной подписи и однозначно показывать, что электронная подпись создана. При проверке электронной подписи средства электронной подписи должны показывать содержание подписанного электронного документа, информацию о внесении изменений в подписанный электронной подписью электронный документ, определять лицо, с использованием ключа электронной подписи которого подписаны электронные документы. Эти требования не применяются к средствам электронной подписи, используемым для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Существуют различные средства проставления электронной подписи на документе. Например, немецкий сберегательный банк Berliner Sparkasse использует способ интеграции рукописных подписей в электронный документооборот. В отделениях сбербанка клиенты подписывают документы посредством перьевого планшета для подписей (signature tablet) «SignPad eSignio», используя программное обеспечение SignDoc компании Softpro. Подпись фиксируется на дисплее SignPad и моментально оцифровывается. В сочетании с индивидуальными биометрическими характеристиками электронная подпись создается в момент подписания документа. SignPad eSignio позволяет зафиксировать и статичную картинку подписи и динамические (биометрические) сигналы подписывающего лица. Индивидуальные показатели силы нажима, ритма и скорости письма помогают сохранить уникальные характеристики фиксируемой подписи. Подпись, зафиксированная на SignPad, уникальна и ее фактически невозможно подделать. Подлинность и надежность документов защищены посредством полной интеграции инструмента фиксации подписи (SignPad) и программного обеспечения (SignDoc). В процессе фиксации программа связывает подпись с содержанием документа, шифрует их и генерирует надежные параметры, позволяющие обнаружить любые попытки использования подписанного документа посторонними лицами. Далее подпись и содержание документа сохраняются в закодированном виде.

Вопросы для самопроверки:

1. Что такое ключ?
2. Какие бывают ключи?
3. Зачем нужна защита информации?
4. Что такое ЭЦП?
5. Как проставляется ЭЦП?
6. Что такое хеширование?
7. Кто является владельцем закрытого ключа?
8. Кто является владельцем открытого ключа?
9. Какие существуют носители ключей?
10. Какие существуют виды электронной подписи?

Литература по теме:

Основная литература:

1. Кузнецов И. Н. Документационное обеспечение управления. Учебник для вузов.- Юрайт-Издат, 2010.

2. Рогожин М. Ю. «Документационное обеспечение управления: учебно-практическое пособие» - Издательство: Проспект, 2010.

Нормативно-правовые акты:

1. Федеральный закон от 10 января 2002 г. N 1-ФЗ «Об электронной цифровой подписи». // www.base.garant.ru/184059/

2. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». // www.consultant.ru/document/cons_doc_LAW_112701/

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». www.graph.document.kremlin.ru/page.aspx?1;878565

4. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хеширования». www.vsegost.com/Catalog/96/9658.shtml

5. ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». www.vsegost.com/Catalog/11/11287.shtml

Статьи:

1. Электронная подпись на STU-500//независимый портал о СЭД. http://www.doc-online.ru/a_id/321

2. Наталья Храмцовская. «Три вида электронной подписи вместо ЭЦП: что изменится для пользователей?». https://ecm-journal.ru/docs/Tri-vida-ehlektronnojj-podpisi-vmesto-EhCP-chto-izmenitsja-dlja-polzovatelejj.aspx