Лекция № 3/2
Электронная подпись.

Учебные вопросы:

1. ФЗ «Об электронной подписи». Определение, технологии применения и основные принципы формирования ЭП.
2. Стандартные криптографические алгоритмы ЭП. Понятие сертификата ключа подписи и проверка его подлинности.
3. Системы электронного документооборота, используемые в профессиональной деятельности.

1. Федеральный закон «Об электронной подписи»

ФЕДЕРАЛЬНЫЙ ЗАКОН от 06.04.2011 № 63-ФЗ

«ОБ ЭЛЕКТРОННОЙ ПОДПИСИ»

(принят ГД ФС РФ 25.03.2011)

вступил в силу 08.04.2011

<u>электронная подпись</u> –

информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [1]**.**

Федеральный закон № 63-ФЗ «Об электронной подписи» регулирует отношения по вопросу использования электронных подписей при совершении гражданско - правовых сделок, исполнении государственных и муниципальных функций, оказании государственных и муниципальных услуг, совершении юридически значимых сделок.

[1] **Федеральный закон от 06.04.2011 № 63-ФЗ "Об электронной подписи"**

Федеральный закон направлен на устранение недостатков Федерального закона от

10 января 2002г. №1-ФЗ

«Об электронной цифровой подписи»,

а также на расширение сферы использования электронных подписей.

Федеральным законом регулируются отношения в области:

1. Использования электронных подписей при совершении гражданско-правовых сделок;
2. Оказании государственных и муниципальных услуг;
3. Исполнении государственных и муниципальных функций;
4. При совершении иных юридически значимых действий.

Федеральным законом определяется

1. **понятие электронной подписи**,

устанавливаются **её виды**, **требования** к средствам электронной подписи, с помощью которых создаются и проверяются:

- **электронная подпись**,
- **ключ электронной подписи**
- и **ключ проверки электронной подписи**

2. требования к **удостоверяющим центрам**, осуществляющим функции по

созданию и выдаче **сертификатов ключей** проверки электронных подписей

В пояснительной записке к **проекту закона об электронной подписи** была приведена неутешительная **статистика**, свидетельствующая о слабой распространенности ЭЦП в российском деловом обороте.

По состоянию на февраль 2007 г. в России было выдано около **200 000 сертификатов ключа ЭЦП**, что составляет лишь **0,2 %** от населения страны.

При этом отмечается, что **в Европе** за аналогичный период времени от введения в действие Директивы ЕС от 13.12.1999 N 1999/93/ЕС «**Об общих принципах электронных подписей**» (DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures) **усиленные электронные подписи** использовало около **70 %** населения

Федеральный закон «0б электронной подписи» (ЭП) пришел на смену Федеральному закону от 10 января 2002 года «0б электронно-цифровой подписи» (ЭЦП), который содержал слишком **серьезные требования** к ЭЦП

В частности, допускалось применение только одной технологии идентификации (**асимметричных электронных ключей подписи**), которая к тому же требовала обязательного наличия **сертификата** от **удостоверяющего центра**

Согласно положениям нового закона от **удостоверяющих центров не требуется лицензирования** - они могут пройти **аккредитацию** и то лишь на добровольной основе.

Аккредитацией будет заниматься назначенный правительством **уполномоченный орган**, он же организует работу корневого центра

Для **аккредитации** российское или иностранное **юридическое лицо** обязано обладать чистыми **активами** на сумму не менее **1 млн. руб**. и **финансовыми гарантиями** для выплат компенсаций пострадавшим клиентам в размере **1,5 млн. руб**., иметь не менее **двух IT-специалистов** с высшим профессиональным образованием и **пройти процедуру подтверждения в ФСБ**

определение

- **электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
- **средства электронной подписи** - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

виды электронных подписей

простая электронная подпись:
логины, пароли, коды подтверждения, адреса электронной почты и прочие средства идентификации

усиленная электронная подпись

квалифицированная

неквалифицированная

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

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

Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате **криптографического** преобразования информации с использованием **ключа** электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет **обнаружить факт внесения изменений** в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном **сертификате**;
- для создания и проверки электронной подписи используются **средства электронной подписи**, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Усиленная квалифицированная подпись имеет **сертификат** от **аккредитованного центра** и создана с помощью **подтвержденных ФСБ средств**

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

1) **обеспечивать конфиденциальность** ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;
2) **уведомлять** удостоверяющий **центр**, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

3) **не использовать** ключ электронной подписи при наличии оснований полагать, что **конфиденциальность** данного ключа **нарушена**;

4) **использовать** для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки **средства электронной подписи,** получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Условия признания электронных документов, подписанных электронной подписью

- Информация в электронной форме, подписанная **квалифицированной, простой, неквалифицированной** электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.
- Электронные подписи, созданные в соответствии с нормами права **иностранного государства** и международными стандартами, в Российской Федерации **признаются** электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона.

Соблюдены **два дополнительных** требования, помимо тех, которые предусмотрены для неквалифицированной подписи. В соответствии со ст. 12 нового Закона это возможно, если:

1) получен **квалифицированный сертификат**, в котором указывается ключ проверки такой электронной подписи;

2) для создания и проверки электронной подписи используются средства электронной подписи, **получившие подтверждение** соответствия требованиям, установленным в Законе об электронной подписи.

2. Стандартные криптографические алгоритмы ЭП.

- Содержимое любого документа (файла) представлено в компьютере как **последовательность байтов** и потому может быть однозначно описано определенным (очень длинным) числом или последовательностью нескольких более коротких чисел.
- Чтобы «укоротить» эту последовательность, не потеряв ее **уникальности**, применяют специальные математические алгоритмы, такие как контрольная сумма (control total) или **хеш-функция** (hash function).
- Если каждый байт файла умножить на его номер (позицию) в файле и полученные результаты суммировать, то получится более короткое, по сравнению с длиной файла, число.
- Изменение любого байта в исходном файле меняет итоговое число.

Хеш-функция определяется как уникальное число, полученное из исходного файла путем его «обсчета» с помощью сложного, но известного (открытого) алгоритма.

Как получается электронная цифровая подпись (ЭЦП)?

- С древних времен известен **криптографический** метод, позднее названный шифрованием с помощью **симметричного ключа**, при использовании которого для зашифровки и расшифровки служит один и тот же ключ (шифр, способ).

- Главной проблемой симметричного шифрования является **конфиденциальность** передачи ключа от отправителя к получателю.

- **Раскрытие ключа** в процессе передачи равносильно раскрытию документа и предоставлению злоумышленнику возможности его **подделать**.

- В 70-х гг. был изобретен алгоритм **асимметричного** шифрования.
- Зашифровывается документ одним ключом, а расшифровывается другим, причем по **первому** из них практически невозможно вычислить **второй**, и наоборот.
- Поэтому если отправитель зашифрует документ **секретным** ключом, а **публичный** ключ предоставит адресатам, то они смогут расшифровать документ, зашифрованный отправителем, и только им.

- Если получатель смог расшифровать значение хеш-функции, используя открытый ключ отправителя, то зашифровал это значение **именно отправитель (аутентификация)**.
- Если вычисленное и расшифрованное значения хеш-функции **совпадают**, то документ не был изменен **(идентификация).**
- Любое **искажение** (умышленное или неумышленное) документа в процессе передачи даст новое значение вычисляемой получателем хеш-функции, и программа проверки подписи сообщит, что подпись под документом **неверна**.

Новый Закон допускает получение электронной подписи, в частности, **юридическими лицами** или **государственными органами**, что не допускалось Законом об ЭЦП

В связи с этим в п. 3 ст. 14 **Закона об электронной подписи** специально оговаривается, что **при получении сертификата** ключа проверки электронной подписи юридического лица необходимо указывать, помимо наименования юридического лица - **владельца этого сертификата**, и **физическое лицо**, действующее от его имени на основании учредительных документов или доверенности.

Однако в этой же норме предусмотрены случаи, когда такие лица могут **не указываться**, и тогда единственным владельцем указанного сертификата будет юридическое лицо.

Такую подпись можно использовать **при оказании государственных** и **муниципальных услуг**, при исполнении **государственных** и **муниципальных функций**

Квалифицированный сертификат должен содержать следующую информацию:

1)уникальный **номер** квалифицированного сертификата, **даты начала** и **окончания** его действия;

2) **фамилия, имя и отчество владельца** квалифицированного сертификата (для физического лица) либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата (для юридического лица);

3) **страховой номер** индивидуального лицевого счета владельца квалифицированного сертификата (для физического лица) либо идентификационный номер налогоплательщика (ИНН) владельца квалифицированного сертификата - для юридического лица;

4) **ключ проверки** электронной подписи;

5) **наименования средств электронной подписи** и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в Законе об электронной подписи;

6) **наименование и место нахождения аккредитованного удостоверяющего центра**, который выдал квалифицированный сертификат, а также номер квалифицированного сертификата этого удостоверяющего центра;

7) **ограничения** использования квалифицированного сертификата (если установлены);

8) иная информация о владельце квалифицированного сертификата (по требованию заявителя).

В Законе об электронной подписи предусмотрено **разделение удостоверяющих центров** на **имеющие** и **не имеющие аккредитацию**.

Последние смогут выдавать только сертификаты ключа, а квалифицированные сертификаты будут выдавать исключительно аккредитованные удостоверяющие центры

Для получения **квалифицированной электронной подписи** необходимо обращаться в **аккредитованный удостоверяющий центр**

Удостоверяющим центром может быть **юридическое лицо** (в том числе и созданное по иностранному праву) или **индивидуальный предприниматель**. **Ограничений** относительно организационно-правовой формы такого юридического лица Закон об электронной подписи **не содержит**.

Сертификат ключа проверки электронной подписи

- Удостоверяющий центр осуществляет создание и выдачу сертификата ключа проверки электронной подписи на основании соглашения между **удостоверяющим** центром и **заявителем**.

Сертификат ключа проверки электронной подписи должен содержать следующую информацию:

1) даты начала и окончания срока его действия;

2) фамилия, имя и отчество (если имеется) - для физических лиц, наименование и место нахождения - для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;

3) ключ проверки электронной подписи;

4) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;

5) наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи;

6) иная информация, предусмотренная частью 2 статьи 17 настоящего Федерального закона, - для квалифицированного сертификата.

3. Системы электронного документооборота, используемые в профессиональной деятельности

Важную роль в системе электронного документооборота играет **администрация** системы.

Она обеспечивает:

- **контроль** за соблюдением абонентами единых **правил** работы,
- участвует в разборе **конфликтных** ситуаций,
- управляет **ключевой системой**
- поддерживает у всех абонентов **справочники** открытых **ключей** в актуальном состоянии.

Справочники меняются регулярно:

- при любом изменении списка участников,
- при замене каких-либо ключей.

Необходимость замены ключей возникает в случае:

- утраты ключа;
- повреждение ключа;
- увольнение сотрудника, имевшего доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) секретных ключей и др.

Если в системе предусмотрена возможность обмена электронными документами между абонентами напрямую, то **справочники** с перечнями открытых ключей должны быть у всех участников и **обновляться** одновременно.

Администрацию системы можно организовать на базе **сторонней фирмы**, располагающей:

- соответствующими службами,
- квалифицированными сотрудниками,
- необходимыми комплектами договоров,
- определенным опытом обслуживания таких систем.

Риск раскрытия конфиденциальной информации при этом **отсутствует**, поскольку секретными ключами участников администрация не обладает — она оперирует только справочниками открытых ключей.

Важно, чтобы генерация ключей (включая секретные) проводилась уполномоченными сотрудниками участников (пусть и на территории лицензированной администрации).

Электронный документооборот успешно применяется многими организациями.

Если **формат сообщений** сторонами изначально **не согласован** и не закреплен в специальном документе подписями и печатями, то может возникнуть **спор**.

И тогда подписанный и переданный файл не будет иметь юридического значения.

Условия проверки ЭЦП

- где проводится проверка,
- на каком аппаратном и программном обеспечении,
- кем,
- в какие сроки,
- а также какое решение принимается, если по каким-либо причинам эти условия не удается соблюсти

Согласно действующим положениям, электронные документы должны храниться столько же, сколько и бумажные — **5 лет**.

Хранение файлов на магнитных носителях в течение такого срока может привести к их **утрате**, поэтому рекомендуется формировать архивы электронных документов на компакт-дисках.

Одной из типичных ошибок организаторов систем ЭДО является архивное хранение документов **в зашифрованном виде**.

Считается, что если документы передаются по открытой сети зашифрованными (для обеспечения конфиденциальности), то и хранить их нужно так же.

Но тогда при физической утрате ключевой дискеты или невозможности считать с нее секретный ключ весь зашифрованный архив станет недоступным.

Кроме того, возникает необходимость либо хранить все секретные ключи за всю историю работы системы (регулярно проверяя их читаемость), либо вновь зашифровывать и перезаписывать архивы при каждой смене ключевых дискет.

В действительности после получения электронного документа адресатом потребность в шифровании отпадает.

Задачу защиты от несанкционированного доступа к документам в своей локальной сети каждый решает сам.