Лекция #5

# Правовые основы информатики

# Структура лекции

- Понятие электронного документа
- Классификация электронных документов
- Электронный  документооборот
- Электронная подпись

# Введение

В современном бизнес-процессе активно распространяется электронный документооборот, и с его появлением все более актуальным становится вопрос о **легитимности** **средств фиксации** и **передачи** различной информации. Такие средства фиксации принято называть **цифровыми носителями**, а информацию, заключенную на них, - **электронными документами**.

Для более ясного представления понятия «электронный документ» обратимся к рассмотрению его предшественника – традиционного документа.

# Традиционный документ

Основной функцией традиционного документа является **удостоверение** некоторой информации.


Материальный носитель позволяет подтвердить **истинность информации**, содержащейся в документе (экспертиза по проверке подлинности документа)

**Оригинал** существует в ограниченном количестве экземпляров

Могут входить **данные** о времени, условиях и месте составления документа

Позволяет установить **аутентичность** (подлинность) документа

# Функции документа

- **Фиксация некоторой (содержательной) информации**
- **Фиксация лица, подписавшего документ**
- **Фиксация условий составления документа**
- **Доказательство в судебном разбирательстве**
- **Функция оригинала, обеспечиваемая его уникальностью**

# Юридически значимый документ

Государственный стандарт РФ ГОСТ Р 51141-98 "Делопроизводство и архивное дело. Термины и определения" дает следующее определение юридической силы документа (юридической значимости документа):

**«Юридическая сила документа – это свойство официального документа, сообщаемое ему действующим законодательством, компетенцией издавшего его органа и установленным порядком оформления»**

Юридическую значимость (силу) документу придают следующие условия:

- наличие в документе обязательных реквизитов и соблюдение правил отображения этих реквизитов,
- компетентность источника, то есть право автора создавать и подписывать документы такого рода,
- гарантия целостности и подлинности.


# Электронный документ

Согласно п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

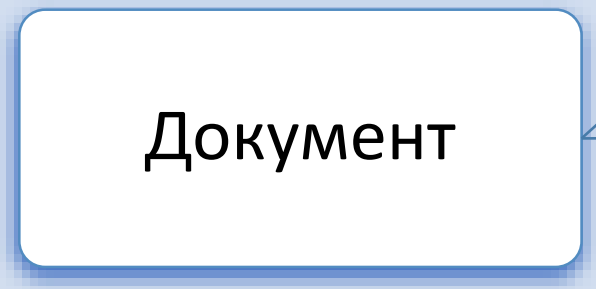
**Электронный документ** – это документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

# Свойства электронного документа

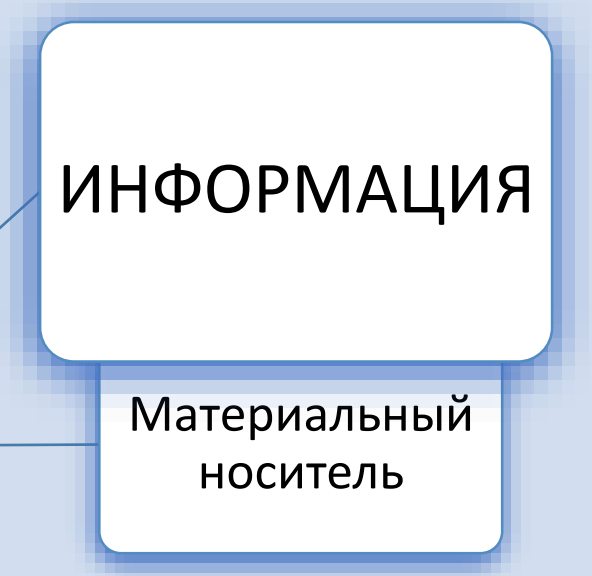
- **аутентичность** - свойство электронного документа, гарантирующее, что электронный документ идентичен заявленному;
- **достоверность** - свойство электронного документа, при котором содержание электронного документа является полным и точным представлением подтверждаемых операций, деятельности или фактов и которому можно доверять в последующих операциях или в последующей деятельности;
- **целостность** - состояние электронного документа, в который после его создания не вносились никакие изменения;
- **пригодность для использования** - свойство электронного документа, позволяющее его локализовать и воспроизвести в любой момент времени.

# Особенности электронного документа

Правовое понятие «электронный документ» неотделимо от традиционного понятия «документ» и должно обладать его свойствами



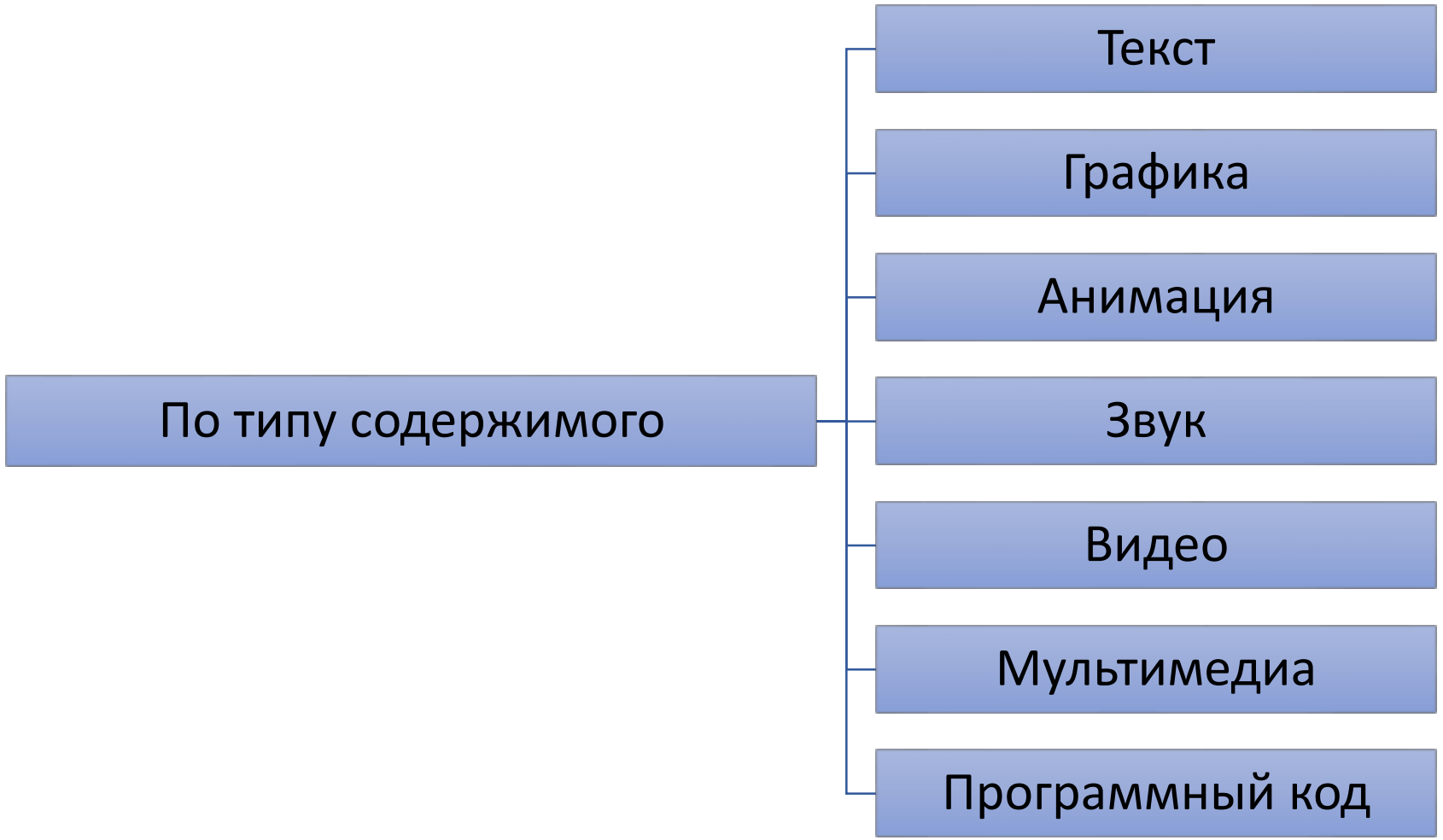

На первый план выходит свойство **информативности** документа, а не его объектно-материальный характер



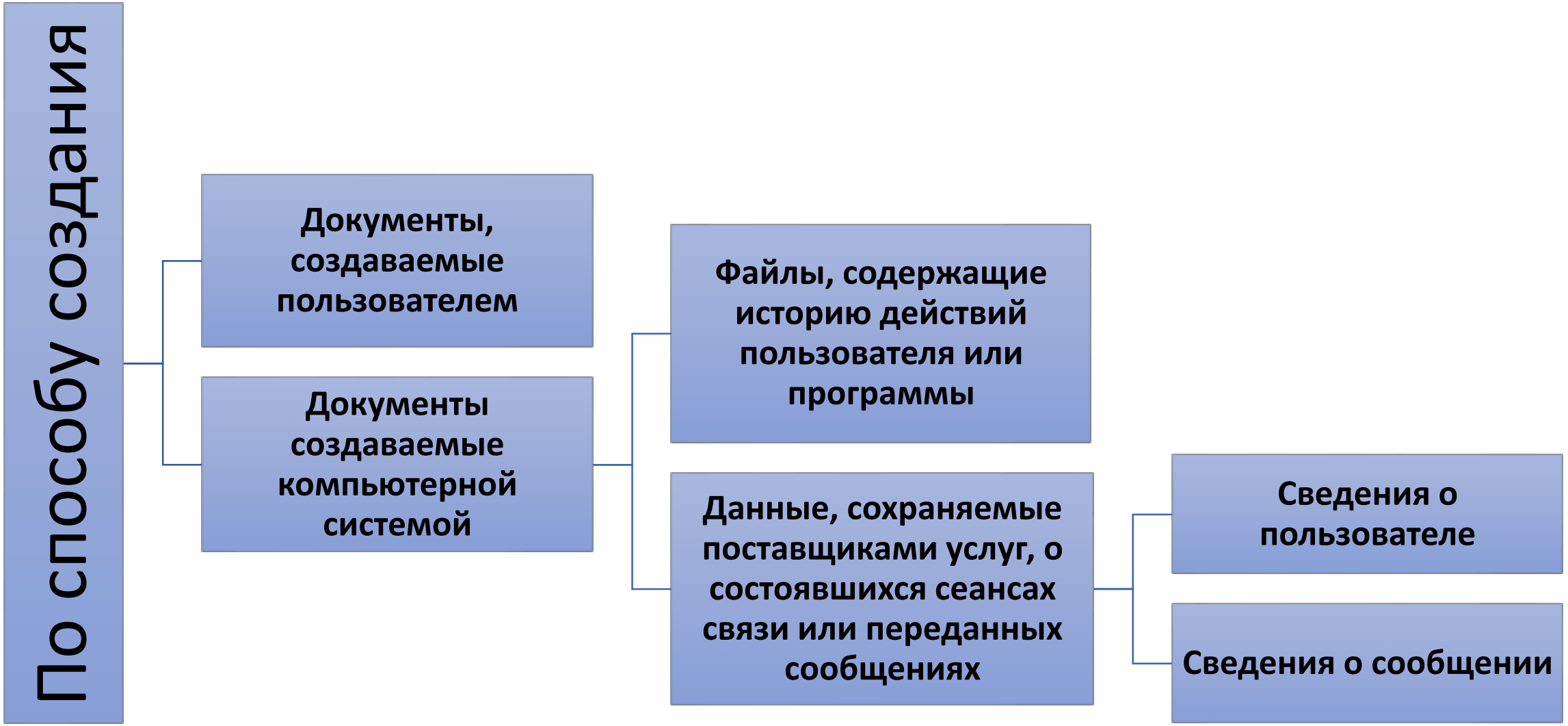

Электронный документ, отделимый от носителя, имеет две формы:
**активную** - обработка и передача,
**пассивную** - хранение.

Акцент смещается с носителя информации на саму информацию, и все действия с электронным документом оцениваются с точки зрения **информационной целостности** и **безопасности**

# Классификация электронных документов



# Классификация электронных документов



# Классификация электронных документов

## по виду материального носителя

### внешние запоминающие устройства

Электронные документы в форме файлов, хранящиеся на внешних запоминающих устройствах (жесткие диски, оптические диски, карты памяти и др.), существуют независимо от того, включен компьютер или нет

### оперативные запоминающие устройства

Электронные документы, зафиксированные в оперативных запоминающих устройствах компьютера или периферийных устройств (принтер, сканер), доступны только тогда, когда на модули устройства подается питание, отключение которого может привести к искажению либо полной потере информации

# Классификация электронных документов

## по форме восприятия

### МАТЕРИАЛЬНЫЕ

Документы, зафиксированные на электронном носителе, приобретают тем самым некую материальную форму и становятся доступными для прямого восприятия

### ВИРТУАЛЬНЫЕ

В виртуальной форме электронные документы существуют в виде «виртуальных следов», наличие которых можно объяснить самой природой электронной информации, которая легко копируется, передается, изменяется, блокируется

# Классификация электронных документов

## по степени защищенности

| **ОТКРЫТЫЕ** | **СКРЫТЫЕ** |
| --- | --- |
| документы, общедоступные для неограниченного числа лиц, имеющих доступ к компьютеру или к другому материальному носителю этих документов | Документы, к которым имеет доступ только ограниченный круг лиц |

# Классификация электронных документов

## по наличию электронной подписи

| **документы, имеющие электронную подпись** | **документы, не имеющие электронную подпись** |
| --- | --- |
| Электронная подпись позволяет идентифицировать лицо, подписавшее электронный документ, т.е. является доказательством подтверждения авторства и осуществляет контроль целостности документа. | Подлинность документов, не имеющих электронную подпись, часто приходится доказывать криминалистам с помощью специальных технических средств. |

# Первые системы электронного документооборота

Первые системы электронного документооборота появились в **банковской сфере**.

Одна из таких систем, **SWIFT** (Society for World Wide Interbank Financial Telecommunications – Всемирное общество межбанковских финансовых телекоммуникаций) функционирует с 1970-х годов.

# Преимущества электронного документооборота

| Прозрачность бизнес-процессов | Повышение исполнительской дисциплины | Сокращение затрат времени руководителей и сотрудников |
| --- | --- | --- |
| Система обеспечивает возможность отслеживания этапов выполнения бизнес-процессов, что делает всю деятельность в организации абсолютно прозрачной и контролируемой | По статистике 20% полученных заданий не выполняются ответственными за них работниками. Предоставляя полный контроль всех этапов работ для руководства, ЭД напрямую влияет на исполнительскую дисциплину сотрудников | Использование системы сокращает временные затраты практически на все рутинные операции с документами (создание, поиск, согласование и т.д.). Кроме того, происходит ускорение документооборота и, как следствие, всех процессов в организации |

# Преимущества электронного документооборота

| Обеспечение конфиденциальности информации | Выполнение требований стандартов ISO 9000 | Легкость внедрения инноваций и обучения |
| --- | --- | --- |
| В отличие от традиционного «бумажного» документооборота, система ЭД обеспечивает доступ к документам строго в соответствии с назначенными правами пользователей, все действия над документом (чтение, изменение, подписание), протоколируются | Постановка менеджмента качества в настоящее время стала одной из приоритетных задач, решаемых российскими компаниями. Одно из требований к системе менеджмента качества (СМК) – это прозрачно поставленный документооборот и информационное взаимодействие. | Благодаря системе оповещения, построенной на базе ЭД можно быстро довести новые правила работы до всех сотрудников. Сокращаются сроки обучения новых сотрудников за счет возможности быстрого поиска необходимой для работы информации (положений, инструкций и т.п.). |

# Преимущества электронного документооборота

| Электронный архив | Развитие корпоративной культуры | Рост конкурентных преимуществ |
| --- | --- | --- |
| Хранение текстов документов в электронном виде позволяет реализовывать полнотекстовый поиск, что открывает принципиально новые возможности при ведении информационно-справочной работы | Оптимизация взаимодействия сотрудников и развитие горизонтальных связей приводят к сплочению команды. В то же время возрастает ответственность каждого сотрудника за качественное выполнение выданного ему задания | Повышается скорость и качество работы организаций за счет ускорения движения информационных потоков и четкого контроля всех процессов. |

# Юридический аспект электронного документооборота

С юридической точки зрения понятие электронного документооборота отличается от понятия электронного обмена данными.

В основе ЭД лежит легитимность (процессуальная допустимость и доказательственная сила) электронных документов.

Наряду с совершенствованием информационных технологий важную роль в процессе создания инфраструктуры электронного документооборота играет его законодательная поддержка, суть которой состоит в придании данным, создаваемым и передаваемым электронным способом, **юридического статуса документа**.

# Юридическая сила документов, подписанных электронной подписью

В 2002 году был принят Федеральный закон № 1-ФЗ "Об электронной цифровой подписи", который приравнял документы в электронном виде, подписанные электронной цифровой подписью, к документам на бумаге, подписанным сторонами договора (утратил силу с 1 июля 2013 года).

Именно этот закон позволил участникам гражданско-правовых отношений обмениваться электронными договорами, актами, накладными и иными документами и установил условия, при выполнении которых эти документы равнозначны аналогичным на бумажных носителях.

# Федеральный закон от 06.04.2011 № 63-ФЗ "Об электронной подписи"

С 8 апреля 2011 года действует **Федеральный закон от 06.04.2011 № 63-ФЗ "Об электронной подписи"** (далее - Закон № 63-ФЗ), который определяет порядок получения и использования электронной подписи и обязанности участников обмена электронными документами.

Данным законом регулируются отношения в области использования электронных подписей при совершении

- гражданско-правовых сделок,
- оказании государственных и муниципальных услуг,
- исполнении государственных и муниципальных функций,
- при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами

# Определение электронной подписи

**Электронная подпись (ЭП)** – это 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 (пп. 1 ст. 2 Закона № 63-ФЗ).

# Определение электронной подписи

Фактически электронная подпись представляет собой **реквизит электронного документа**, который позволяет установить отсутствие искажения информации в электронном документе с момента формирования ЭП и проверить принадлежность подписи владельцу сертификата ключа ЭП.

Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа ЭП.

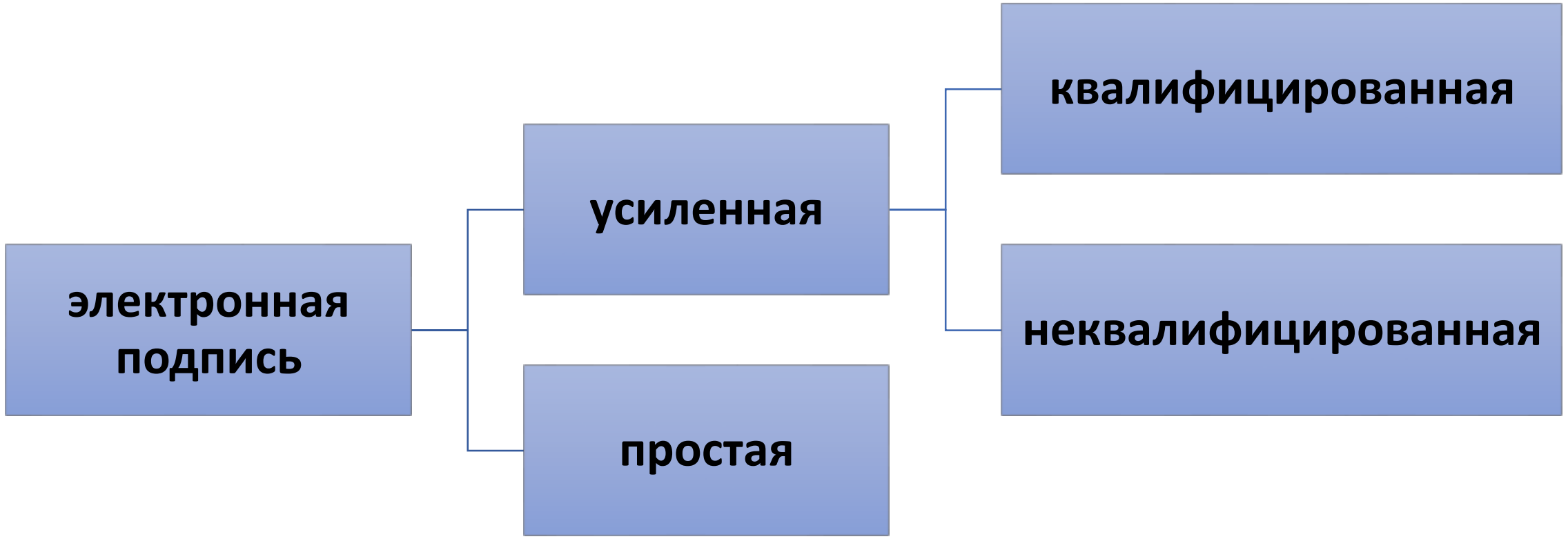
# Принципы использования электронной подписи

1) **право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению**, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) **возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств**, позволяющих выполнить требования Федерального закона об ЭП применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

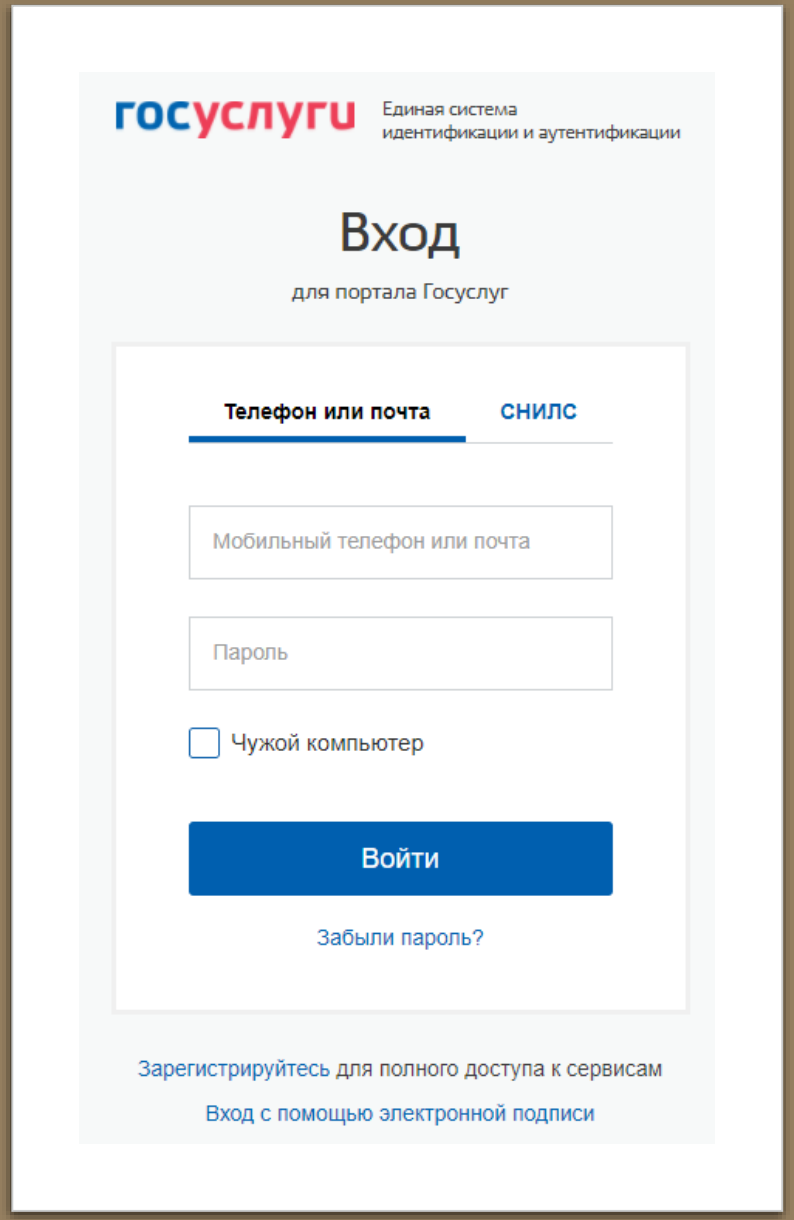
# Виды электронной подписи



# Простая электронная подпись

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

Важной особенностью простой электронной подписи является отсутствие возможности проверить документ на предмет наличия изменений с момента подписания.



# Применение простой электронной подписи

Предназначена для подписания гражданами электронных сообщений, направляемых в государственный орган, орган местного самоуправления или должностному лицу.

Для того чтобы электронный документ, подписанный этой подписью, признавался равнозначным бумажному документу, подписанному собственноручно, необходимо выполнение определенных условий, предусмотренных Законом об ЭП.

Кроме того, условия признания и порядок проверки этой подписи устанавливаются нормативными правовыми актами, принимаемыми в соответствии с федеральными законами, или соглашением между участниками обмена.

Документы, требующие печати, не могут быть подписаны простой ЭП.

# Усиленная электронная подпись

Целям определения лица, подписавшего электронный документ, а также обнаружения факта внесения изменений в документ после его подписания служит усиленная электронная подпись.

Именно эта подпись (в двух видах — неквалифицированная и квалифицированная) является аналогом прежней электронной цифровой подписи (согласно Федеральному закону № 1-ФЗ "Об электронной цифровой подписи«)

# Усиленная неквалифицированная электронная подпись

Неквалифицированной электронной подписью является электронная подпись, которая:

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

# Применение неквалифицированной электронной подписи

Усиленная неквалифицированная ЭП создается с помощью специальных программных средств (средств электронной подписи). Данная подпись позволяет определить лицо, подписавшее документ, и защитить его от несанкционированного изменения.

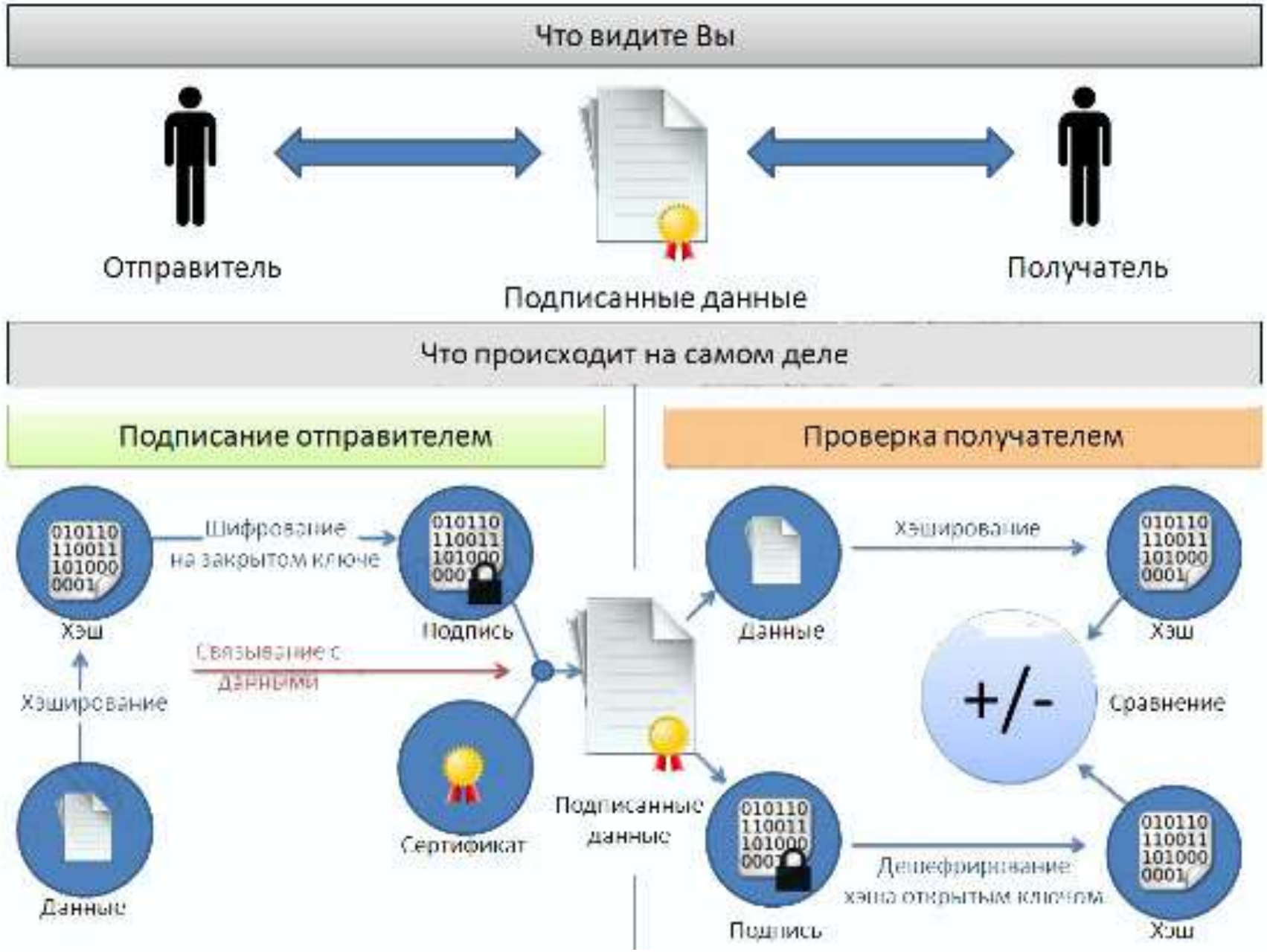
Данная подпись выдается удостоверяющим центром и признается равнозначной собственноручной подписи в случаях, определенных законодательством или соглашением сторон.

Неквалифицированной ЭП можно подписывать документы, которые в бумажном виде заверяются печатью.

# Ключи и средства электронной подписи

Составляющими и связанными понятиями с электронной подписью являются:

- **ключ электронной подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи;
- **ключ проверки электронной подписи** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи
- **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


Что видите Вы
Отправитель
Подписанные данные
Получатель
Что происходит на самом деле
Подписание отправителем
Проверка получателем
Шифрование на закрытом ключе
Хэш
Подпись
Связывание с данными
Хэширование
Данные
Сертификат
Подписанные данные
Данные
Хэширование
Хэш
+/-
Сравнение
Дешефрирование хэша открытым ключом
Подпись
Хэш

# Квалифицированная электронная подпись

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

1) ключ проверки электронной подписи указан в **квалифицированном сертификате**;
2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом об ЭП.

# Квалифицированная электронная подпись

Усиленная квалифицированная электронная подпись должна обязательно иметь сертификат аккредитованного Удостоверяющего центра.

Эта подпись заменяет бумажные документы во всех случаях, за исключением тех, когда закон требует наличия исключительно документа на бумаге.

С помощью таких подписей возможно организовать юридически значимый электронный документооборот с партнерскими компаниями, органами государственной власти и внебюджетными фондами.

# Возможные сферы применения квалифицированной электронной подписи

**Электронная отчетность**

В контролирующие органы и внебюджетные фонды, ФНС, ПФР, ФСС, Росстат

**Электронные торги**

на федеральных и коммерческих торговых площадках

**Счет-фактуры в электронном виде**

**Обмен документами между организациями** (договоры, акты)

**Арбитражный процесс**

# Подмена открытых ключей для создания ложного канала связи

Открытый ключ (ключ проверки электронной подписи) доступен каждому из партнеров владельца закрытого ключа (ключа электронной подписи)

# Решение проблемы подмены ключей

Одним из основополагающих моментов использования электронной подписи для установления подлинности, целостности и аутентичности документов, хранимых, обрабатываемых и передаваемых с помощью информационных и телекоммуникационных систем, является подтверждение принадлежности открытого ключа ЭП конкретному лицу посредством выдачи сертификата ключа подписи.

Вводится дополнительная сторона, **удостоверяющая** принадлежность открытого ключа конкретному юридическому или физическому лицу.

# Решение проблемы подмены ключей

Вопросы: кто именно имеет право удостоверять открытые ключи, когда и как, — в законодательстве различных государств решаются по-разному. В частности, это может быть:

- государственный орган
- организация, уполномоченная государством для ведения данной деятельности.

Возможно, что для внутреннего документооборота предприятия эту функцию можно поручить лицу, назначенному руководством, а для документооборота внутри ведомства — уполномоченному подразделению.

# Решение проблемы подмены ключей

На практике сертификация открытых ключей выполняется следующим образом.

- Лицо (юридическое или физическое), создавшее себе пару ключей (открытый и закрытый) с помощью средства ЭП, должно обратиться в орган, уполномоченный выполнить сертификацию - **удостоверяющий центр**.
- **Удостоверяющий центр** проверяет принадлежность открытого ключа заявителю и удостоверяет этот факт добавлением к открытому ключу своей подписи, завизированной собственным закрытым ключом.
- Любой партнер, желающий вступить в контакт с владельцем открытого ключа, может прочитать удостоверяющую запись с помощью открытого ключа удостоверяющего центра. Если целостность этой записи не нарушена, то он может использовать открытый ключ партнера для связи с ним.

# Удостоверяющий центр

- **Удостоверяющий центр** - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом
- **Аккредитация удостоверяющего центра** - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона «Об электронной подписи»

# Аккредитованный удостоверяющий центр

**Аккредитованный удостоверяющий центр** для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему **головным удостоверяющим центром**, функции которого осуществляет уполномоченный федеральный орган.

Аккредитованному удостоверяющему центру **запрещается** использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

# Сертификаты ключа проверки электронной подписи

- **сертификат ключа проверки электронной подписи** - электронный документ или документ на бумажном носителе, выданные **удостоверяющим центром** либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи
- **квалифицированный сертификат ключа проверки электронной подписи** - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный **аккредитованным удостоверяющим центром** либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи

Следует четко понимать, что **удостоверяющий центр** заверяет только факт принадлежности открытого ключа конкретному лицу или организации.

Наличие полноценного сертификата открытого ключа говорит о том, что ключ можно использовать для удостоверения личности партнера в договорных отношениях.

Но законность этих отношений удостоверяющим центром не подтверждается!

# Требования к удостоверяющему центру

К удостоверяющим центрам предъявляются особые требования. Это обусловлено тем, что участники электронного документооборота не могут проверить корректность осуществления подобными организациями своих функций.

В части экономического обоснования возможности удостоверяющего центра нести гражданскую ответственность за ненадлежащее исполнение своих обязанностей необходимо выделить три критерия:

- наличие собственного минимально установленного капитала, выраженного в абсолютной сумме;
- подтверждение этой суммы банковской гарантией;
- наличие страховки

# Инфраструктура открытых ключей (PKI — Public Key Infrastructure)

Достаточно трудной представляется задача практического создания в нашей стране инфраструктуры открытых ключей (PKI — Public Key Infrastructure) в системах электронного документооборота и электронной торговли.

Термин «инфраструктура открытых ключей» включает в себя полный комплекс программно-аппаратных средств, а также организационно-технических мероприятий, необходимых для использования открытых ключей.

Основным компонентом инфраструктуры является собственно система удостоверяющих центров.

# Системы сертификации

В настоящее время распространение получили две структурные модели системы сертификации — централизованная и децентрализованная.

**Централизованная модель** имеет иерархический характер и наиболее соответствует потребностям служебного документооборота.

**Децентрализованная модель** имеет сетевой характер и может использоваться, например, в гражданском электронном документообороте.

# Централизованная модель сертификации

В основе централизованной модели сертификации находится один уполномоченный орган сертификации. Такой орган называется **корневым удостоверяющим центром** (**корневым центром сертификации**).

Если чисто технически корневой центр не может обеспечить все запросы на выдачу и проверку сертификатов, поступающие от юридических и физических лиц, то он может сертифицировать другие дополнительные органы, называемые **доверенными удостоверяющими центрами** (**доверенными центрами сертификации**).

Доверенные центры тоже могут удостоверять чужие открытые ключи своими открытыми ключами, но при этом их открытые ключи тоже нуждаются в удостоверении. Их удостоверяет своим закрытым ключом вышестоящий центр сертификации.

# Алгоритм проверки ЭП при централизованной модели сертификации

Таким образом, участник электронного документооборота, получивший откуда-то открытый ключ неизвестного партнера, может:

1. установить наличие сертификата, удостоверенного электронной подписью удостоверяющего центра;
2. проверить действительность подписи центра сертификации в вышестоящем удостоверяющем центре;
3. если вышестоящий центр тоже является не корневым, а доверенным, то и его подпись можно проверить в вышестоящем центре, и так далее, пока проверка не дойдет до корневого удостоверяющего центра.

# Сетевая модель сертификации

Сетевая модель сертификации основана на **взаимных договоренностях сторон**, которые будут иметь правовое значение, только если прямо отражены в двусторонних договорах.

Два юридических или физических лица, вступающих в электронные коммерческие взаимоотношения, могут сами взаимно заверить друг другу открытые ключи, если обменяются ими при личной встрече с предъявлением друг другу учредительных документов или удостоверений личности (для физических лиц).

В этом случае у них нет оснований сомневаться в истинной принадлежности открытых ключей.

# Сетевая модель сертификации

Однако электронная коммерция строится исходя из того факта, что участники не нуждаются в очной встрече.

В этом случае две стороны могут договориться о том, что им взаимно заверит ключи **третья сторона**, которую они выберут сами.

В результате возникает сложная структура, в которой все участники связаны, с одной стороны, двусторонними договорными отношениями, а с другой стороны, еще и выполняют функции заверителей для своих традиционных партнеров.

С точки зрения отдельного коммерсанта доверие к его открытому ключу будет тем выше, чем большее количество сертификатов он получит от прочих участников рынка.

Ссылка на тест