

Электронный документооборот

Управление процессами: практика защиты информации, управления документами, архивирования, практика применения электронной цифровой подписи

Термины

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

- ▶ Электронный документ - 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
- ▶ Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

Термины

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

- ▶ Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
- ▶ Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
- ▶ Информация - сведения (сообщения, данные) независимо от формы их представления

Термины

- ▶ Документооборот - это жизненный цикл документа начиная с момента создания или получения и заканчивая его исполнением и отправкой в архив
- ▶ Электронный документооборот - это информационная система обеспечивающая жизненный цикл электронных документов и предоставляющая методы: создания, обработки, хранения, поиска, передачи и архивирования таких документов

Реквизиты документа

1. Герб
2. Эмблема
3. Товарный знак
4. Код формы документа
5. Наименование организации - автора документа
6. Наименование структурного подразделения - автора документа
7. Наименование должности лица - автора документа
8. Справочные данные об организации
9. Наименование вида документа
10. Дата документа
11. Регистрационный номер документа
12. Ссылка на регистрационный номер и дату поступившего документа
13. Место составления (издания) документа
14. Гриф ограничения доступа к документу
15. Адресат
16. Гриф утверждения документа
17. Заголовок к тексту
18. Текст документа
19. Отметка о приложении
20. Гриф согласования документа
21. Виза
22. Подпись
23. Отметка об электронной подписи
24. Печать
25. Отметка об исполнителе
26. Отметка о заверении копии
27. Отметка о поступлении документа
28. Резолюция
29. Отметка о контроле
30. Отметка о направлении документа в дело

Виды электронного документооборота

- ▶ Производственный документооборот
- ▶ Управленческий документооборот
- ▶ Архивное дело (совокупность процедур архивного документооборота)
- ▶ Кадровый документооборот (процедуры кадрового учета)
- ▶ Бухгалтерский документооборот
- ▶ Складской документооборот
- ▶ Секретное и конфиденциальное делопроизводство
- ▶ Технический и технологический документооборот

Преимущества электронного документооборота

- ▶ Централизованное, структурированное и систематизированное хранение документов в электронном архиве
- ▶ Сокращение расходов на печать, почтовую пересылку и хранение бумажных счетов-фактур
- ▶ Единообразный подход к процедурам формирования и обработки документа (регистрация, согласование и т.п.)
- ▶ Сокращение времени на доставку, регистрацию и согласование документов
- ▶ Быстрое подписания документов;
- ▶ Возможность круглосуточно в режиме онлайн осуществлять любые операции с документами: поиск, загрузку, печать, сверку, отклонение, а также отслеживать их движение;
- ▶ Быстрый поиск документов.

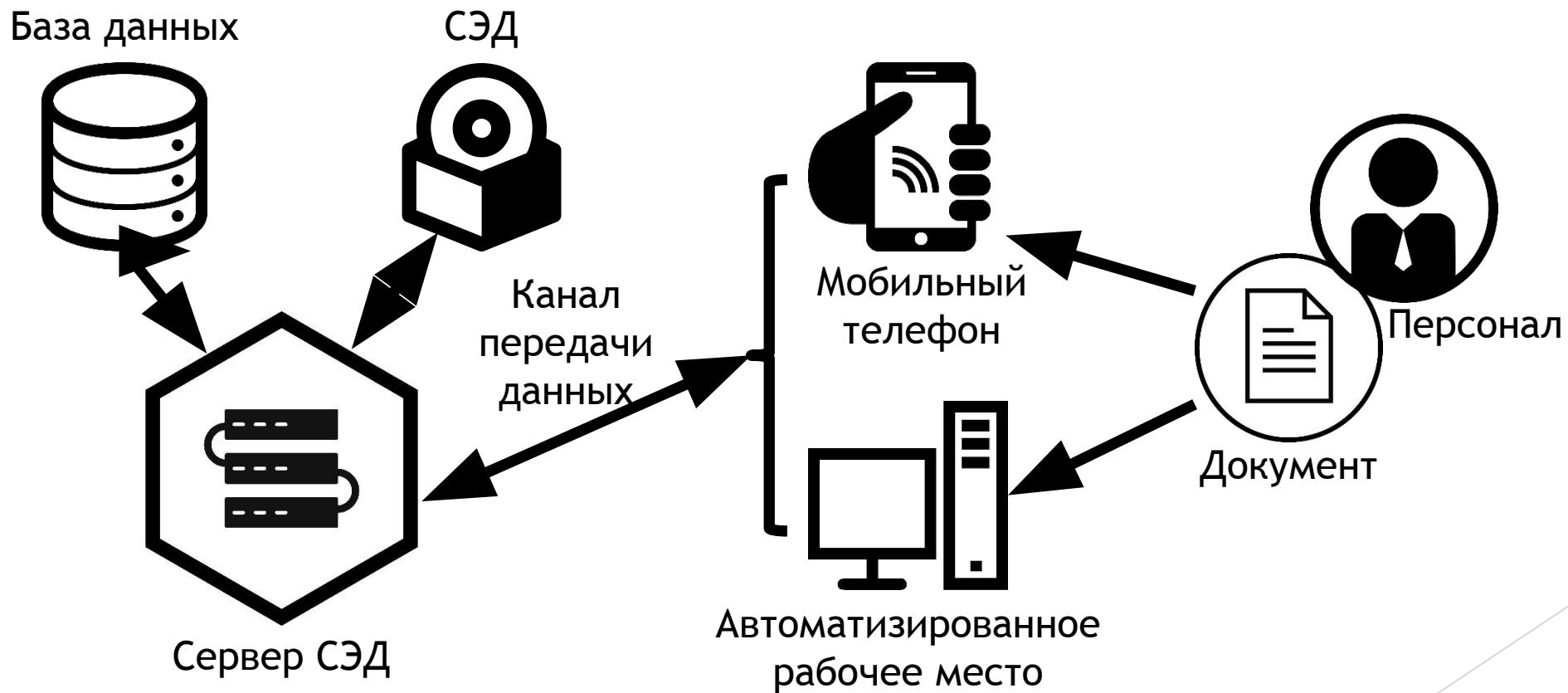
Задачи систем электронного документооборота

- ▶ Обеспечение эффективного управления за счет автоматического контроля выполнения, прозрачности деятельности всей организации на всех уровнях
- ▶ Поддержка эффективного накопления, управления и доступа к информации и знаниям. Обеспечение кадровой гибкости за счет большей формализации деятельности каждого сотрудника и возможности хранения всей предыстории его деятельности
- ▶ Протоколирование деятельности предприятия в целом (внутренние служебные расследования, анализ деятельности подразделений, выявление "горячих точек" в деятельности)
- ▶ Оптимизация бизнес-процессов и автоматизация механизма их выполнения и контроля
- ▶ Исключение бумажных документов из внутреннего оборота предприятия. Экономия ресурсов за счет сокращения издержек на управление потоками документов в организации
- ▶ Исключение необходимости или существенное упрощение и удешевление хранения бумажных документов за счет наличия оперативного электронного архива

Основные функции системы электронного документооборота

- ▶ Регистрация документов
- ▶ Контроль исполнения документов
- ▶ Контроль движения бумажного и электронного документа, ведение истории работы с документами
- ▶ Создание и редактирование реквизитов документов
- ▶ Формирование отчетов по документообороту предприятия
- ▶ Импорт документов из файловой системы и Интернета
- ▶ Создание документа прямо из системы на основе шаблона
- ▶ Работа с версиями документа, сложными многокомпонентными документами, вложениями
- ▶ Электронное распространение документов
- ▶ Работа с документами в папках
- ▶ Получение документов посредством сканирования и распознавания
- ▶ Уменьшением затрат на доступ к информации и обработку документов

Технология организации электронного документооборота



Технология организации электронного документооборота

- ▶ **Сервер СЭД:**
 - ▶ Локальный
 - ▶ Облачный
- ▶ **База данных:**
 - ▶ Amazon Aurora
 - ▶ PostgreSQL
 - ▶ MySQL
 - ▶ MariaDB
 - ▶ ORACLE
 - ▶ Microsoft SQL Server
- ▶ **СЭД:**
 - ▶ Directum
 - ▶ Elma
 - ▶ Docsvision
 - ▶ Дело
 - ▶ Тезис
 - ▶ 1С: Документооборот
 - ▶ Microsoft SharePoint
 - ▶ DirectumRX
 - ▶ NauDoc
 - ▶ Visary
- ▶ **Приложение для персонала:**
 - ▶ Прикладное
 - ▶ Мобильное приложение
 - ▶ Веб-приложение

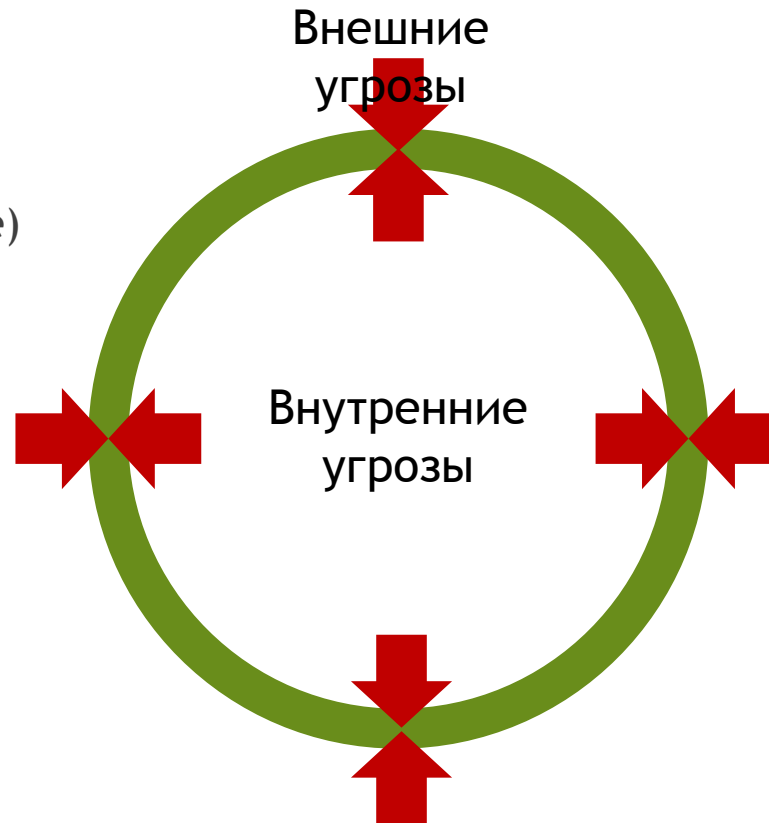
Защиты информации

- ▶ **Угрозы:**

- ▶ Внутренние (случайные, преднамеренные)
- ▶ Внешние (случайные, преднамеренные)

- ▶ **Основные угрозы для документа:**

- ▶ Копирование
- ▶ Изменение
- ▶ Удаление
- ▶ Порча



Комплексный подход к защите информации

- ▶ Механизмы защиты информации систем электронного документооборота (СЭД) реализуются на принципах комплексного подхода к организации защиты и учитывают разнообразие возможные угроз информационной безопасности СЭД



Золотой баланс в защите информации



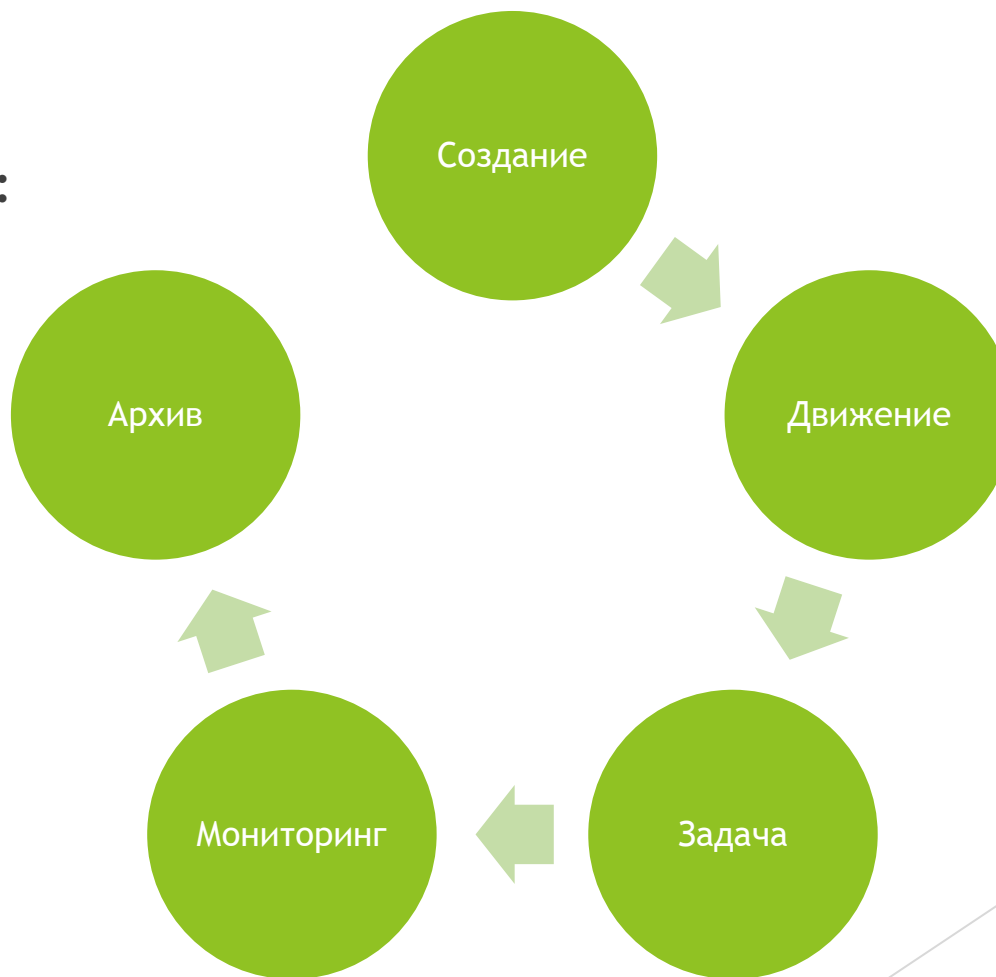
Защищенная СЭД

- ▶ **Для электронного документа должно обеспечиваться:**
 - ▶ Сохранность
 - ▶ Подлинность
 - ▶ Безопасный доступ
 - ▶ Протоколирование действий
- ▶ **Объекты защиты в СЭД:**
 - ▶ Аппаратное обеспечение - СВТ, серверы, элементы ЛВС и сетевое оборудование
 - ▶ Системные файлы, файлы базы данных при их обработке
 - ▶ Электронные документы

Управление документами

▶ Жизненный цикл документа:

- ▶ Создание и редактирование
- ▶ Движение
- ▶ Задача
- ▶ Мониторинг
- ▶ Архивное хранение



Управление документами: создание и редактирование

- ▶ Создаваемый в СЭД документ приобретает индивидуальную карточку учета, которая не может быть изменена или удалена. Только после сохранения документа в базе данных, его можно редактировать.



Новый
документ



Сканированный
документ



Входящий
документ

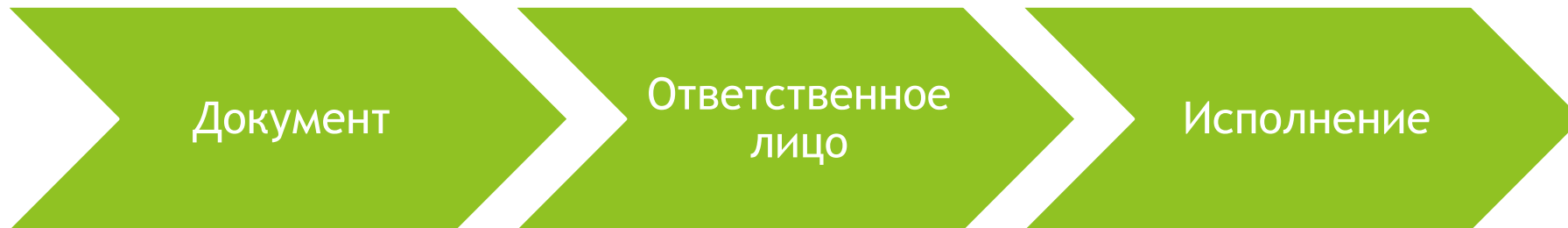
Управление документами: движение

- ▶ Документ направляется в работу к пользователям системы, которые могут проводить широкий спектр операций, таких как согласование, подпись, редактирование, ознакомление и др.



Управление документами: Задача

- ▶ Закрепление определенных задач за документом: обязывает ответственных лиц к строгому исполнению поручений в поставленный срок. Этот этап жизненного цикла должен обеспечиваться подсистемой контроля за выполнением задачи.



Управление документами: мониторинг

- ▶ Набор действий, обеспечивающих контроль над состоянием документа. Пользователь с соответствующими привилегиями должен в любой момент времени знать, в каком состоянии находится документ: редактируется, на подписи, на утверждении и т.д. Сюда же следует отнести функции подсистемы контроля за выполнением задачи.



Управление документами: архивное хранение

- ▶ Отработавшие все необходимые этапы документы перемещаются в электронный архив, где обеспечиваются функции хранения, поиска и доступа к документу в том случае, если он «может понадобиться» в дальнейшем.



Электронно-цифровая подпись

Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

- ▶ 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
- ▶ 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

Электронно-цифровая подпись

Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

- ▶ 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
- ▶ Удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей
- ▶ 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 электронно-цифровой подписи

Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

- ▶ Простая электронная подпись
- ▶ Неквалифицированная электронная подпись
- ▶ Квалифицированная электронная подпись

Простая электронная подпись

- ▶ Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
- ▶ Примеры:
 - ▶ Коды доступа из СМС
 - ▶ Коды на скретч-картах
 - ▶ Пары “логин-пароль” в личных кабинетах на сайтах и в электронной почте
 - ▶ Другое

Неквалифицированная электронная подпись

- ▶ 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
- ▶ Сама по себе усиленная неквалифицированная подпись – это не аналог собственноручной подписи. Она означает, что документ был подписан конкретным лицом и с тех пор не менялся. Но действует такая подпись обычно только совместно с соглашением о признании ее собственноручной. Правда, не везде, а только в документообороте с тем ведомством (организацией), с которым подписано такое соглашение.

Квалифицированная электронная подпись

- ▶ 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, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.
- ▶ Для формирования используются средства криптографической защиты информации, сертифицированные ФСБ РФ. Выдать такую подпись может только удостоверяющий центр, имеющий аккредитацию в Министерстве цифрового развития, связи и массовых коммуникаций РФ. Гарантом подлинности в этом случае становится квалифицированный сертификат ключа проверки электронной подписи, который предоставляет такой центр.

Квалифицированная электронная подпись

- ▶ Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Электронно-цифровая подпись: подходы шифрования

- ▶ Для генерации ключей существует два подхода шифрования:
 - ▶ Симметричное - состоит из одного ключа
 - ▶ Асимметричное - состоит из пары ключей, открытого и закрытого



Электронно-цифровая подпись: симметричный подход

- ▶ Для подписи и проверки используется один ключ, из чего следует что после использования ключ компрометируется и необходимо генерировать новый ключ

Подписание



Ключ

Ключ



Проверка



30

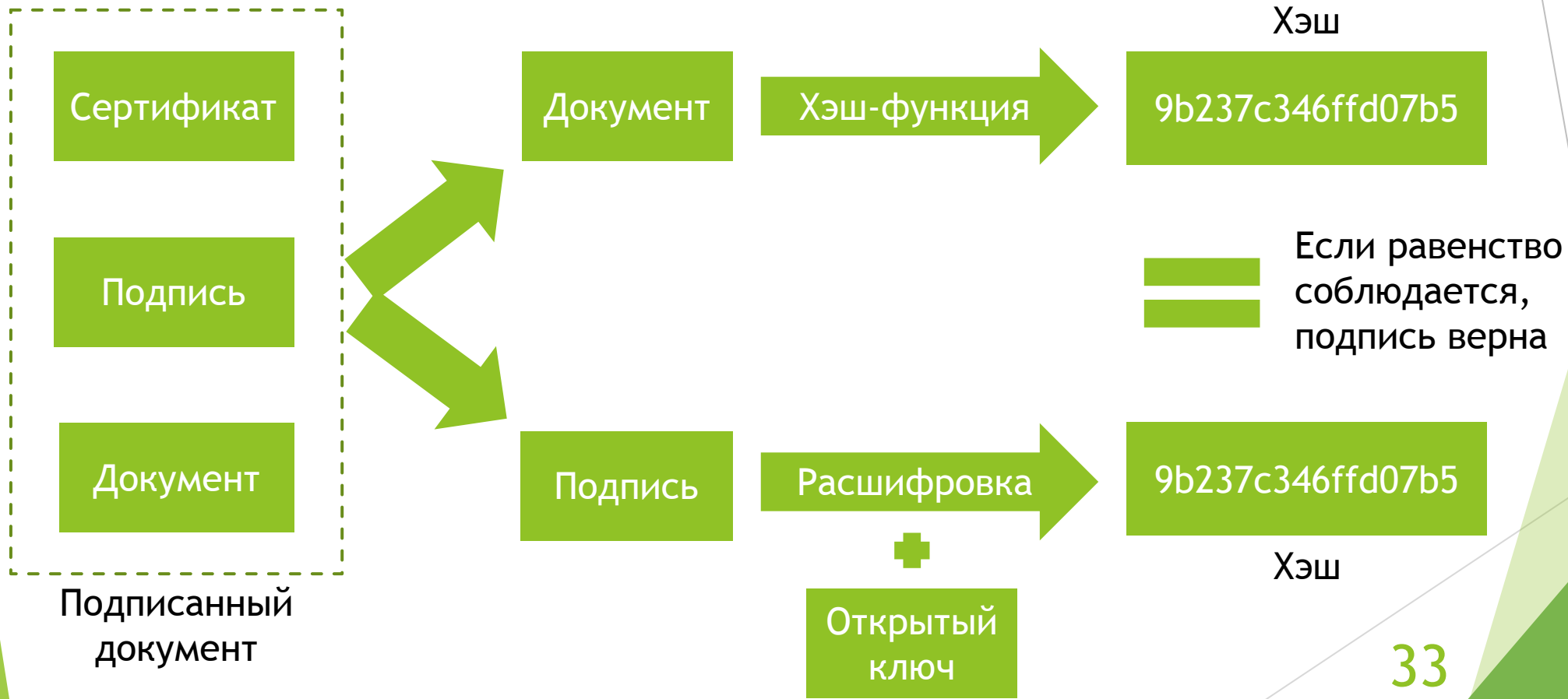
Электронно-цифровая подпись: асимметричный подход

- ▶ В асимметричном шифровании используется пара ключей (открытый и закрытый)
- ▶ Закрытый ключ используется для подписания документа и находится только у владельца
- ▶ Открытый ключ используется для проверки подписи и может свободно передаваться
- ▶ При использовании открытого ключа закрытый ключ не компрометируется, так как из открытого ключе нельзя вычислить закрытый ключ.

Электронно-цифровая подпись: асимметричный подход, подписание



Электронно-цифровая подпись: асимметричный подход, проверка



Электронно-цифровая подпись: алгоритмы шифрования

▶ Симметричные:

- ▶ ГОСТ 28147-89
- ▶ AES
- ▶ Blowfish
- ▶ CAST
- ▶ DES

▶ Асимметричные

- ▶ ГОСТ Р 34.12-2015
- ▶ RSA
- ▶ El-Gamal

Электронно-цифровая подпись: хэш-функция

- ▶ Это математический алгоритм, преобразовывающий произвольный массив данных в состоящую из букв и цифр строку фиксированной длины. Причем при условии использования того же типа хэша длина эта будет оставаться неизменной, вне зависимости от объема входных данных.
- ▶ Криптостойкой хэш-функция может быть только в том случае, если выполняются главные требования: стойкость к восстановлению хэшируемых данных и стойкость к коллизиям, то есть образованию из двух разных массивов данных двух одинаковых значений хэша.
- ▶ Интересно, что под данные требования формально не подпадает ни один из существующих алгоритмов, поскольку нахождение обратного хэшу значения — вопрос лишь вычислительных мощностей. По факту же в случае с некоторыми особо продвинутыми алгоритмами этот процесс может занимать чудовищно много времени.
- ▶ Алгоритмы хэширования: MD5, SHA1, SHA256, SHA384, SHA512, RIPE MD160

Электронно-цифровая подпись: хэш-функция

Используема хэш-функция: sha-1

Пример

• fda23dbe40cc5074768e2575454227551ef10067

ПРИМЕР

• 7a4a2d1bfa99b237c346ffd07b52699e3ec0c35d

Пример
длинного текста

• 86be731e7452f49bc6821f0648cf35b4a7a4a464

Системы счисления

Шестнадцатеричная	Десятичная	Восьмеричная	Двоичная			
0	0	0	0	0	0	0
1	1	1	0	0	0	1
2	2	2	0	0	1	0
3	3	3	0	0	1	1
4	4	4	0	1	0	0
5	5	5	0	1	0	1
6	6	6	0	1	1	0
7	7	7	0	1	1	1
8	8	10	1	0	0	0
9	9	11	1	0	0	1
A	10	12	1	0	1	0
B	11	13	1	0	1	1
C	12	14	1	1	0	0
D	13	15	1	1	0	1
E	14	16	1	1	1	0
F	15	17	1	1	1	1

Электронно-цифровая подпись: единицы измерения количества информации

- ▶ Бит = наименьшая единица измерения, может принимать значение: 0 или 1
- ▶ Байт = 8 бит
- ▶ Мегабайт = 1024 байт
- ▶ Гигабайт = 1024 мегабайт
- ▶ Терабайт = 1024 мегабайт



Электронно-цифровая подпись: сертификат

- ▶ Основное назначение сертификата ключа проверки электронной подписи – это подтверждение того, что электронная подпись принадлежит какому-то определенному лицу, так называемому владельцу электронной подписи
- ▶ Сертификат ключа проверки электронной подписи должен содержать следующую информацию:
 - ▶ уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата
 - ▶ 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
 - ▶ уникальный ключ проверки электронной подписи
 - ▶ наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи
 - ▶ наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи

Электронно-цифровая подпись: пример сертификата



Электронно-цифровая подпись: ГОСТЫ

**Электронная
подпись**

- ГОСТ Р 34.10-2012
- ГОСТ 34.10-2018

Хеш-функция

- ГОСТ Р 34.11-2012

Шифрование

- ГОСТ Р 34.12-2015
- ГОСТ 28147-89