Электронный документооборот

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

Термины

- 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

- 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;
- Документооборот – это жизненный цикл документа начиная с момента создания или получения и заканчивая его исполнением и отправкой в архив.

Термины

- Электронный документооборот – это информационная система обеспечивающая жизненный цикл электронных документов и предоставляющая методы: создания, обработки, хранения, поиска, передачи и архивирования таких документов

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

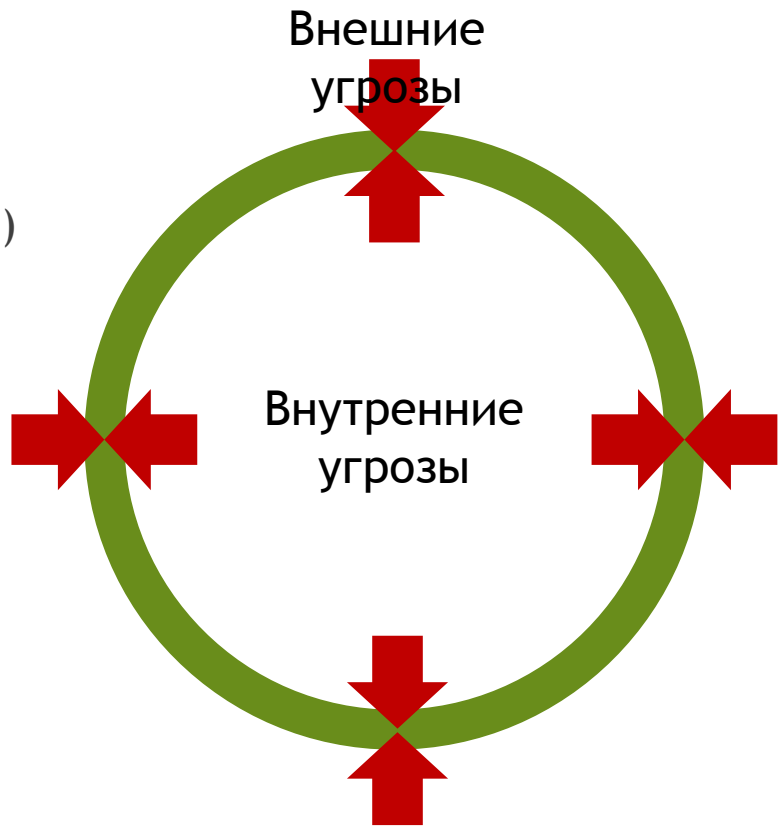
- Экономия времени
- Более адекватное использование физического пространства и техники
- Повышение прозрачности внутренней работы предприятия
- Ведение личной истории каждого файла и сопутствующей документации
- Больше гибкости в отношении физического местонахождения сотрудников
- Повышение безопасности информации и документов
- Снижение затрат на распечатку, почтовые марки, конверты и пересылку

Задачи систем электронного документооборота

- Обеспечение эффективного управления за счет автоматического контроля выполнения, прозрачности деятельности всей организации на всех уровнях.
- Поддержка системы контроля качества, соответствующей международным нормам.
- 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.

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

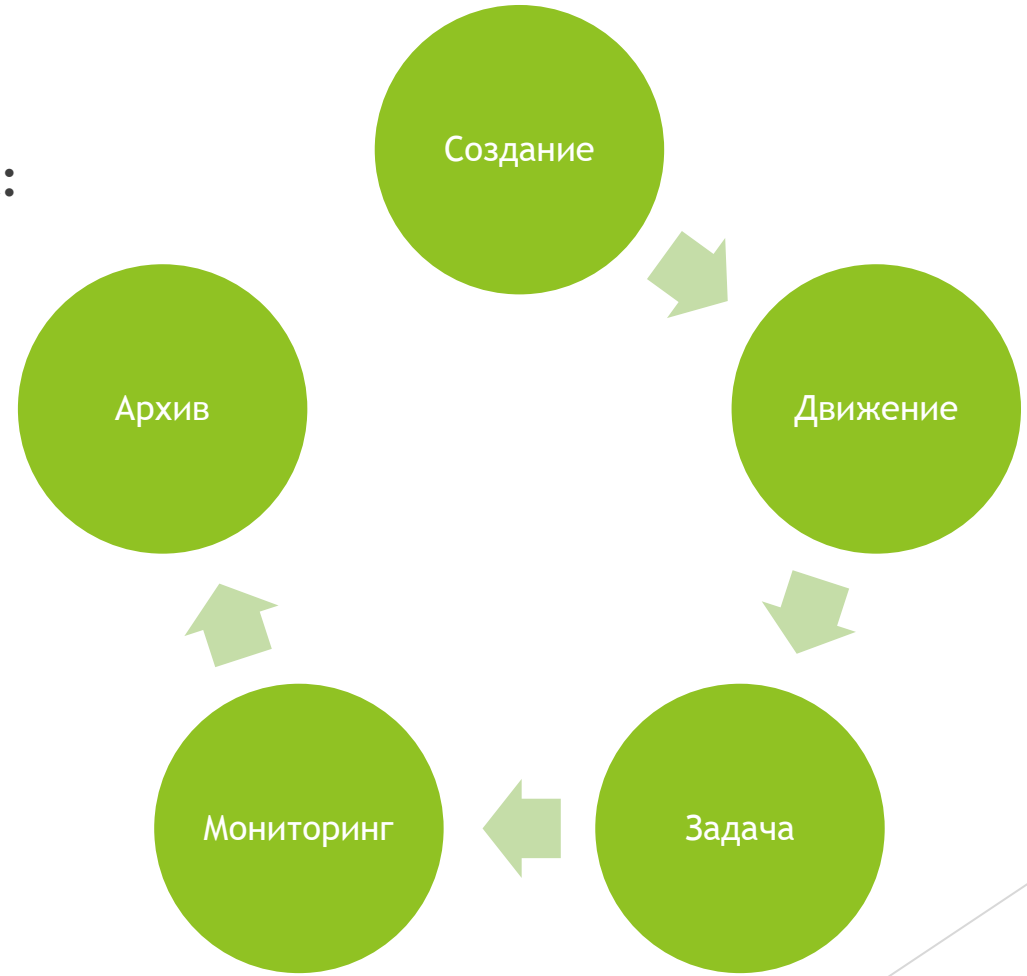
Золотой баланс в защите информации

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

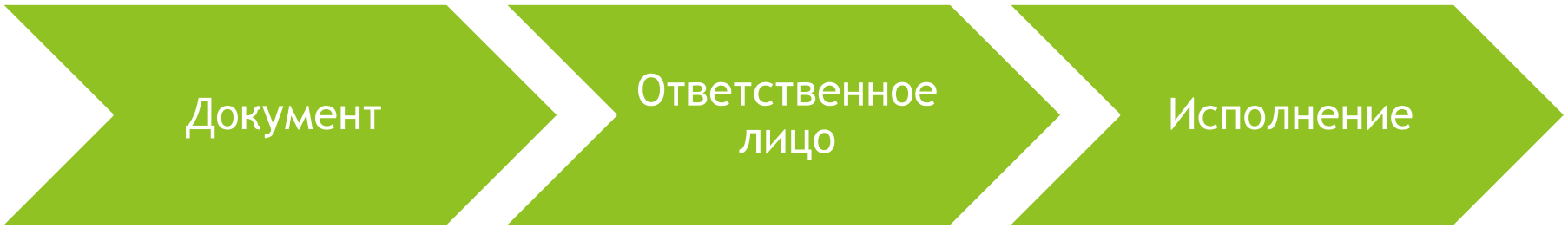
Входящий документ

Управление документами: движение

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

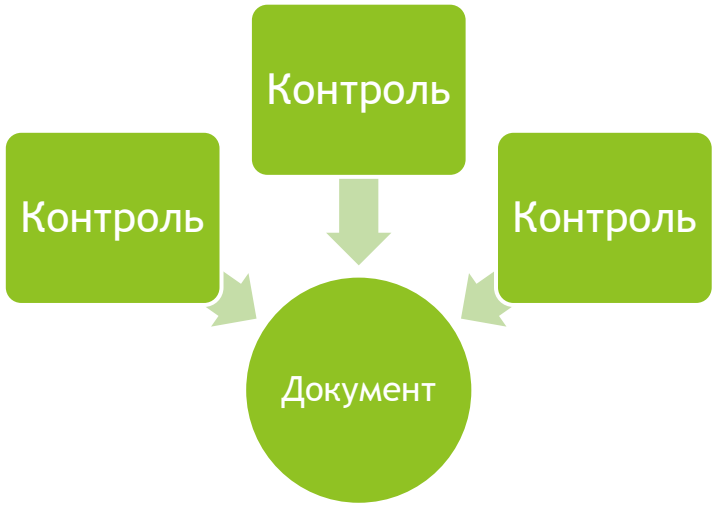
Управление документами: Задача

- 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

- 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

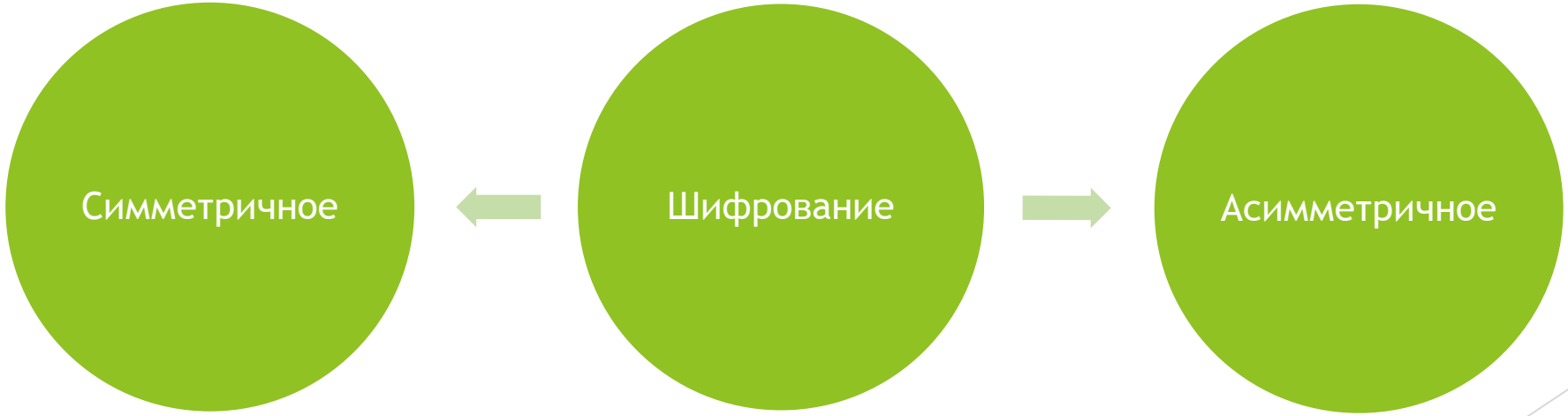
Электронно-цифровая подпись

- 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

Электронно-цифровая подпись

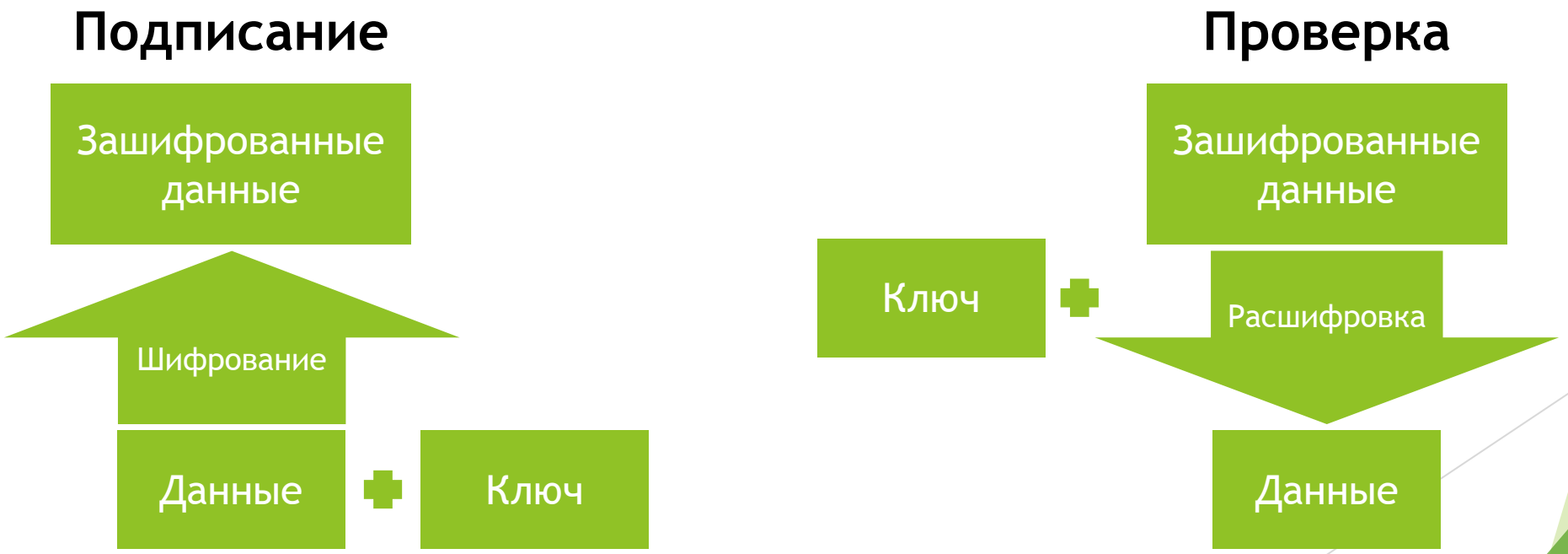
Электронно-цифровая подпись: ключ

- 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

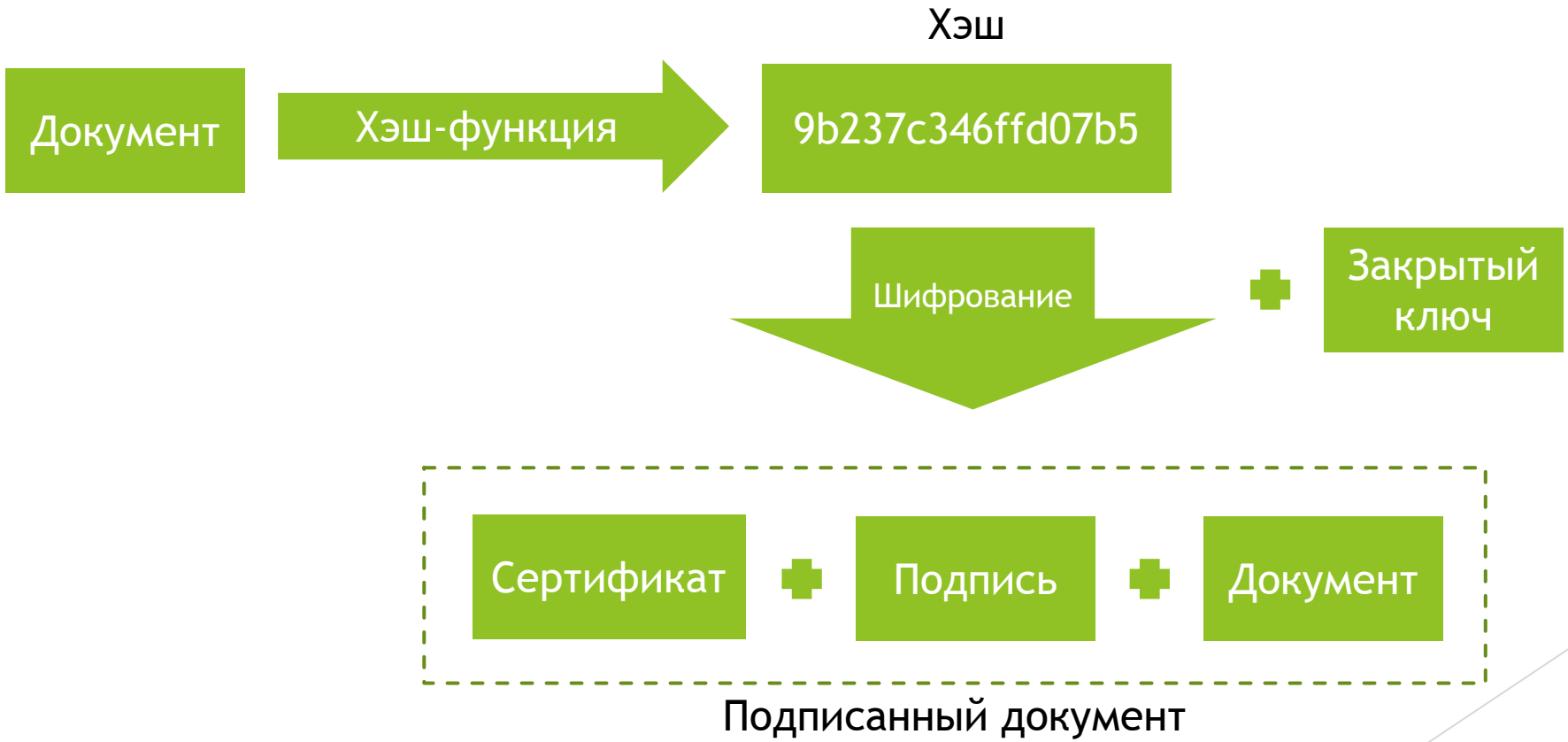
- Для подписи и проверки используется один ключ, из чего следует что после использования ключ компрометируется и необходимо генерировать новый ключ



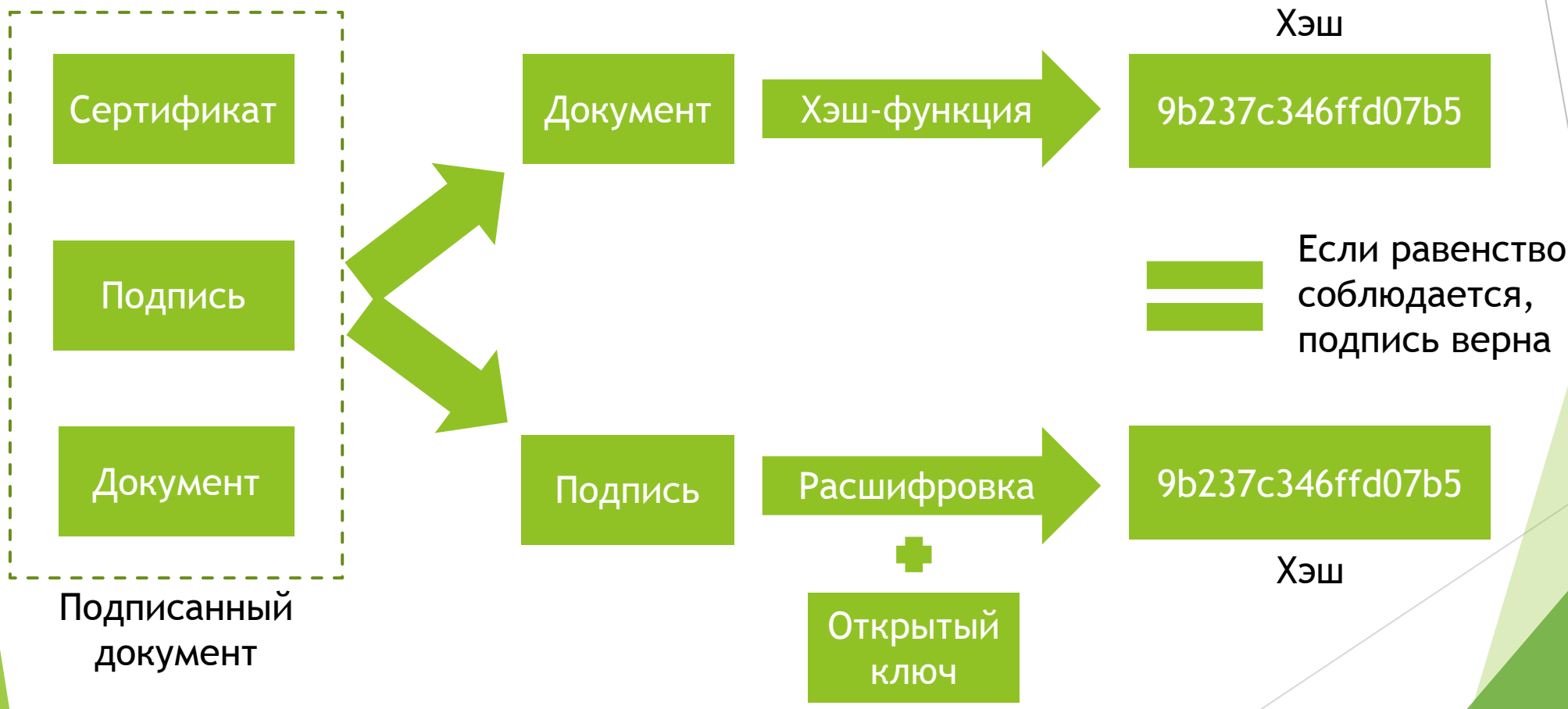
Электронно-цифровая подпись: асимметричный подход

- 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 вводных 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

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

- 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: сертификат

УДОСТОВЕРЯЮЩИЙ ЦЕНТР
ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ
Некоммерческое партнерство инновационной деятельности в социальной сфере
«МосГорУслуга»
111397, г.Москва, Зеленый проспект, д. 20

СЕРТИФИКАТ

КЛЮЧА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

№: 260E 41EB 0000 0000 092A

Владелец сертификата: Башков Владимир Анатольевич
Организация: ЗАО "Вимком Оптик ТС"
Действителен с: 2 февраля 2011 г. 14:05:00 UTC
Действителен до: 25 ноября 2011 г. 14:15:00 UTC

Сведения об отношениях:
Использование на электронных площадках отобранных для проведения аукционов в электронной форме
Юридическое лицо
Участник размещения заказа
Администратор организации
Уполномоченный специалист
Специалист с правом подписи контракта
Проверка подлинности клиента
Защищенная электронная почта

Открытый ключ ЭЦП:
0440 8ED8 967E DDA7 CAD8 0550 0666 E374 EBB8 E62A 2500 6816
EA08 1A6F 0196 261B 84F0 D930 7831 BD4C D123 FF86 5D69 AE2A
EEC4 C39A 6CBA C4F2 0721 DA13 E497 2FAE DC6F

Наименование СКЗИ: КриптоПро CSP
Ключевой контейнер: RaUser-eae995a3-bd90-4078-abf8-08bb3042430e
Ключевой носитель: ETOKEN_JAVA_00578e9c

Подпись владельца сертификата: _____
Получил: _____ (подпись) Кашкина Л.В. (ФИО)
По доверенности

Уполномоченное лицо УЦ: Хотченков А. И. _____

«МосГорУслуга» Уполномоченный центр электронной цифровой подписи

№ 0001820

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