

Электронный документооборот.

Лекция № 2

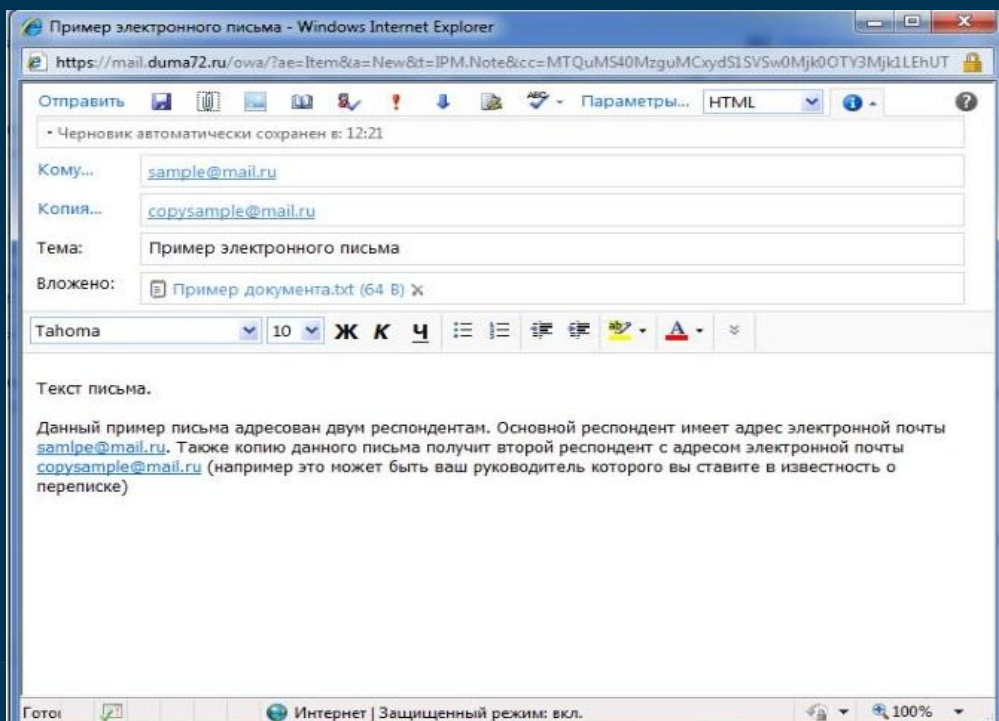
Основные понятия

Электронное сообщение

В связи со значительной распространенностью электронного документооборота (ЭДО) необходимо определить следующие понятия:

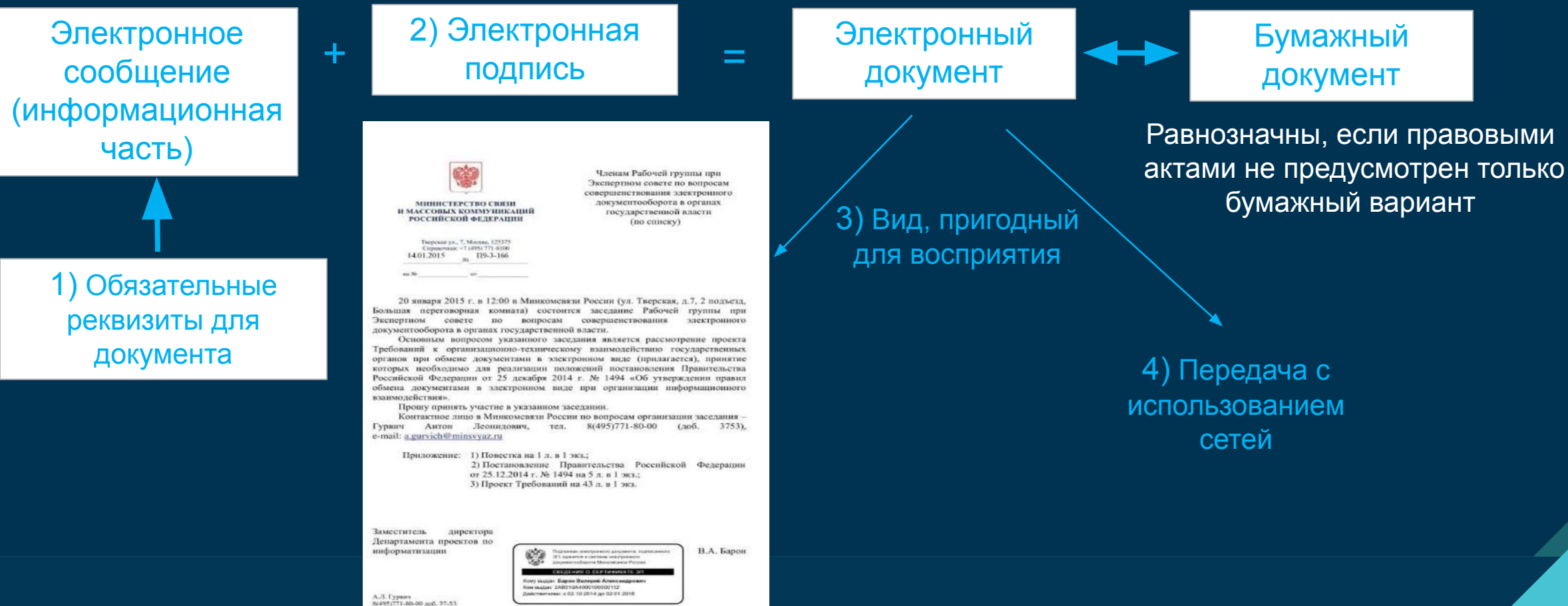
Электронное сообщение – информация, переданная или полученная пользователем с использованием информационно-телекоммуникационной сети (ЛВС или Интернет).

Электронное сообщение \neq электронный документ



Понятие об электронном документе

Электронный документ – это аналог текстового документа, содержащий все необходимые реквизиты, представленный в электронной форме в виде, пригодном для восприятия человеком и подписанный электронной подписью.



Понятие об электронном документе

Свойства электронного документа (ЭД):

- ❑ **достоверность** – состояние ЭД, при котором его содержание является полным и точным представлением фактов, операций или деятельности и которому можно доверять в последующем;
- ❑ **целостность** – состояние ЭД, заключающееся в его неизменности после создания;
- ❑ **аутентичность** – свойство, гарантирующее, что ЭД идентичен заявленному;
- ❑ **пригодность для использования** – свойство, позволяющее воспроизвести ЭД в любой момент времени.

Понятие об электронном документе

Состав электронного документа

Реквизиты формы:
аналогичны реквизитам бумажных документов

Метаданные файла ЭД:

- описательные;
- структурные;
- административные;
- идентификационные

Юридическая сила электронного документа

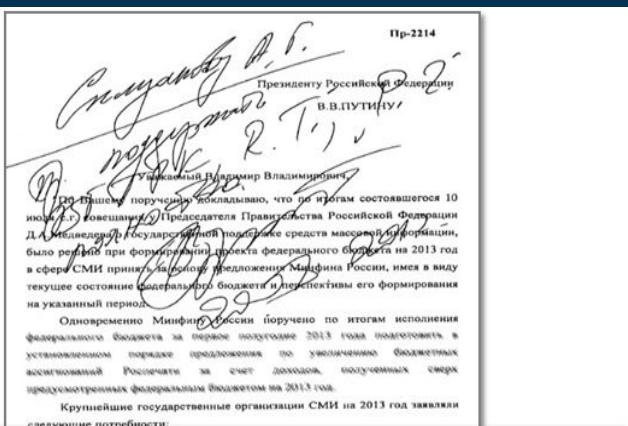
Электронный документ обладает юридической силой при соблюдении следующих условий:

- 1) **Соответствие нормативным документам:** если в нормативном документе нет прямого указания, что документ составляется только на бумаге, значит его можно публиковать в виде ЭД.
- 2) **Содержание и форма:** форма ЭД должна соответствовать форме бумажных документов, а содержание – не противоречить законодательству РФ.
- 3) **Порядок передачи:** передача ЭД без перевода их в бумажную форму возможна только с использованием систем электронного документооборота; для этого организации подписывают соглашение об использовании электронного документооборота. Передача электронных документов в надзорные органы (ФНС и пр.) также осуществляется с использованием определенного порядка, при нарушении которого ЭД теряет свою юридическую значимость.
- 4) **Подписи:** ЭД получает юридическую значимость при его подписании электронной подписью (Федеральный закон «Об электронной подписи» № 63-ФЗ).

Методы защиты электронного документа

1) **Маркировка:** метод защиты, направленный на обнаружение нарушителя:

- Простая маркировка: добавление малозаметной метки (например, точка или прозрачный пробел), уникальной для каждого экземпляра ЭД;
- Программная маркировка – программно-аппаратный комплекс, позволяющий при воспроизведении документа изменять интервалы или кегль шрифта.



2) **Доступ по электронному ключу:** расшифровка документа возможна только при наличии у пользователя физического ключа для расшифровки документа.

3) **Система управления правами доступа** - список типичных ограничений прав:

- Чтение, изменение, печать;
- Срок действия документа;
- Запрет пересылки электронного письма;
- Запрет печати электронного письма.

4) **Комбинированные методы защиты:** предоставление доступа по паролю, отправляемому на мобильный телефон; привязка к уникальному материальному носителю; управление правами доступа в режиме реального времени.

ВГТРК – 19 980 млн.рублей;

АО "ТВ Новости" (Russia Today) – 11 211 млн. рублей;

ФГУП "РИА Новости" – 3 469 млн. рублей;

ФГУП "ИТАР-ТАСС" – 1 370 млн. рублей;

ФГУП ВГТРК "Голос России" – 4 725 млн. рублей;

ФГБУ "Редакция "Российской газеты" – 4 941 млн. рублей.

С уважением,

Первый заместитель Руководителя
Администрации Президента
Российской Федерации

А.Громов

Электронная подпись: основные понятия

Электронная подпись (ЭП) – реквизит электронного документа, предназначенный для его защиты от подделки и полученный в результате криптографического преобразования информации, позволяющий идентифицировать владельца сертификата ключа подписи, а также установить искажение информации в электронном документе.

Использование ЭП регулируется Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Виды ЭП:

- Простая;
- Усиленная:
 - неквалифицированная;
 - квалифицированная.

Электронная подпись

Простая ЭП

Это ЭП, которая подтверждает ее формирование определенным лицом посредством использования кодов, паролей или иных средств. Ключом ЭП являются коды, пароли или их сочетание.

Виды простой ЭП:

- 1) ПЭП в виде присоединяемой к электронному документу информации – представляет собой набор данных генерируемых программой совместно с пользователем или по его команде и присоединяемой к документу. *Пример* – создание ПЭП в MS Office для подтверждения авторства документа.
- 2) ПЭП, созданная при помощи средств прохождения авторизации в ИС (логин/пароль; логин/пароль/код, отправляемый на телефон пользователя). *Пример* – авторизация в любой СЭД или на портале «Госуслуги».

Использование ПЭП:

- Ведомства и учреждения: доступ к сервисам госучреждений (портал nalog.ru, «Госуслуги» – возможно подавать заявления и запрашивать информацию, но не осуществлять документооборот); выполнения различных операций с документами во внутренних СЭД (создание, согласование).
- Финансовые организации: системы «клиент-банк», если клиент физлицо.
- Страховые компании.

Юридическая значимость ПЭП:

В случаях, установленных законодательством или по соглашению участников. При этом должны предусматриваться: правила определения лица по его ПЭП (например по логину/паролю); соблюдение конфиденциальности ключа ПЭП.

Электронная подпись

Усиленная ЭП

Это ЭП, которая создается с помощью криптографических преобразований и хеш-функций, позволяет однозначно определить автора и факт внесения изменений в ЭД.

Алгоритм подписания и проверки усиленной ЭП:

- 1) Генерация ключевой пары: с помощью алгоритма генерации ключа выбирается пара «закрытый – открытый ключ».
- 2) Формирование подписи: вычисление хэш-суммы документа; шифрование хэш-суммы закрытым ключом (полученная при преобразовании информация фактически и является ЭП документа).
- 3) Передача документа и ЭП.
- 4) Проверка (верификация) подписи: для данного документа с помощью открытого ключа определяется действительность подписи:
 - Вычисление хэш-суммы документа с помощью функции, использованной на шаге 3;
 - Расшифровка ЭП с помощью открытого ключа пользователя;
 - Сравнение полученных хэш-сумм.

Результатом сравнения является определение факта целостности документа (хэш-суммы равны) или нарушение целостности (не равны).

Условия использования усиленной ЭП:

- Верификация ЭП открытым ключом, соответствующим тому закрытому ключу, который использовался при подписании.
- Не имея закрытого ключа, выполняется условие вычислительной сложности создания ЭП.

Электронная подпись

Квалифицированная усиленная ЭП

ЭП, создаваемая с использованием алгоритмов шифрования и выдаваемая в удостоверяющем центре, имеющим аккредитацию ФСБ и Минсвязи.

Владелец КЭП получает ключи ЭП, специальное ПО, сертификат ЭП, в котором указываются:

- 1) Уникальный номер сертификата для проверки ЭП, даты начала и окончания действия сертификата;
- 2) ФИО или наименование владельца ЭП;
- 3) Уникальный ключ проверки ЭП;
- 4) Наименование используемого средства ЭП и наименование удостоверяющего центра.



Основные сведения:

- закрытый ключ ЭП – называется ключом ЭП, а открытый – ключом проверки ЭП;
- документ, подписанный с помощью КЭП = собственноручно подписанному документу;
- проверку целостности и авторства документа можно запросом сертификата в УЦ или на портале «Госуслуги»;
- срок действия сертификата ключа – 1 год, при этом действие привязанных к нему подписей не ограничено, сам сертификат можно продлить.

Электронная подпись

Неквалифицированная усиленная ЭП

ЭП, создаваемая с использованием алгоритмов шифрования; однако выпуск такой ЭП возможен не только УЦ, но и внутри организации или на устройстве пользователя, при этом сертификат ЭП не является необходимым, ключ проверки может распространяться любым удобным способом.

Юридическая сила неквалифицированной ЭП признается только в случаях, оговоренных законом, или по соглашению сторон.

Юридическая сила электронной подписи

Юридическая сила различных видов ЭП при использовании в сферах деятельности:

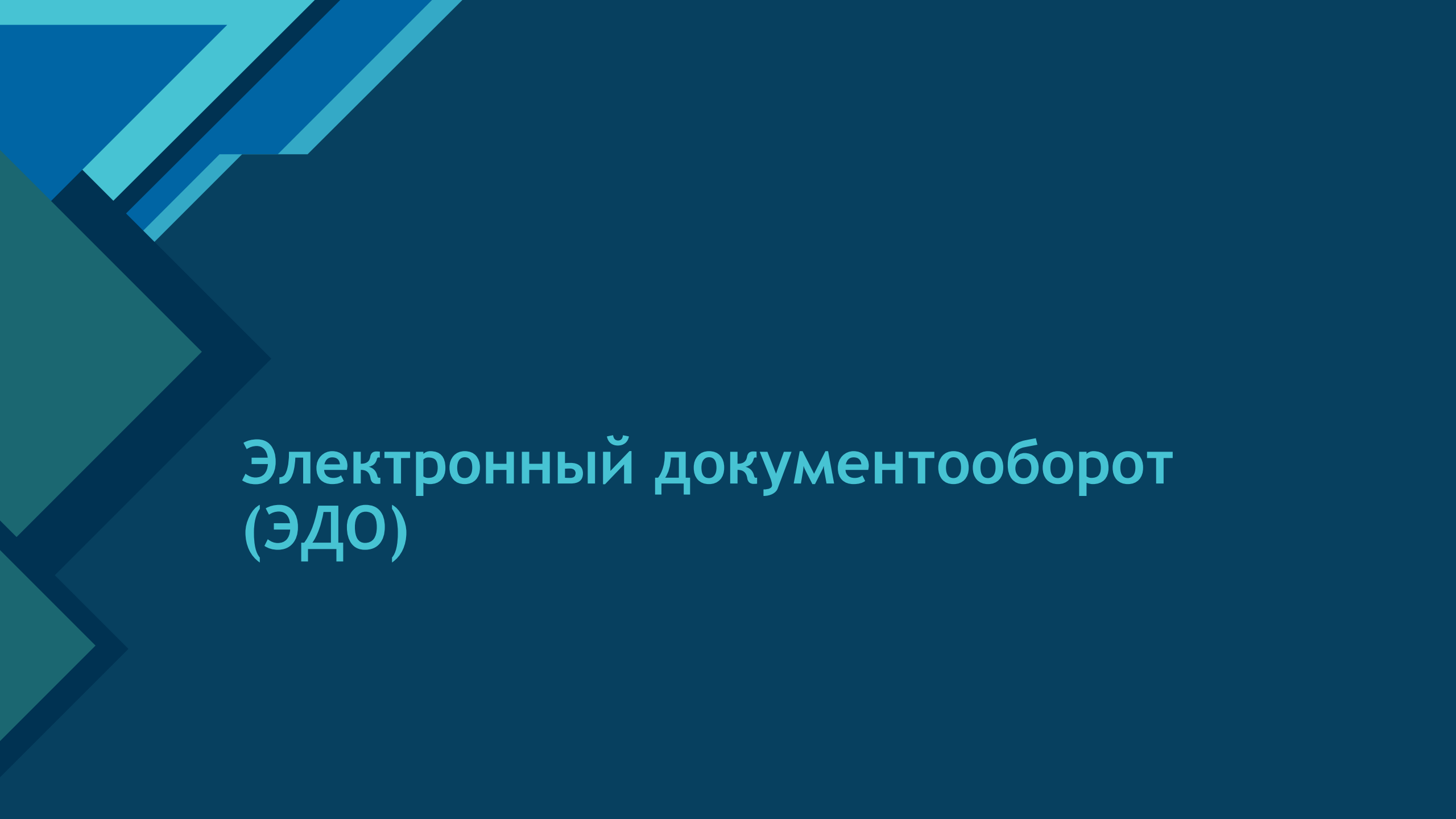
Сфера деятельности	КЭП	НЭП	ПЭП
1) Электронный документооборот: <ul style="list-style-type: none">▪ Внутренний▪ Межкорпоративный (кроме гос.органов)	+	Соглашение сторон	Соглашение сторон
2) Отчетность для контролирующих органов (ФНС, ПФ РФ)	+	На официальном портале (nalog.ru)	-
3) Органы исполнительной власти	+		
4) Электронные торги	+	-	-
5) Арбитражный суд	+	-	-

Атаки на электронную подпись

Классы атак на ЭП:

- 1) Взлом закрытого ключа: нахождение секретного ключа пользователя и полный взлом алгоритма шифрования.
- 2) Универсальная подделка: поиск алгоритма, аналогичного алгоритму генерации ЭП, что позволяет подделывать ЭП для любого документа.
- 3) Селективная подделка: подделка ЭП только под выбранным сообщением – либо подбор произвольных данных в служебных полях, либо подмена одного документа с одинаковой подписью другим.
- 4) Экзистенциальная подделка: подделка ЭП для одного случайно выбранного документа из совокупности.
- 5) Социальные атаки: кража закрытого ключа у собственника или подписание самим собственником документа злоумышленника с помощью обмана.

Современные алгоритмы шифрования позволяют значительно уменьшить вероятность атак на ЭП при условии сохранности ключа ЭП, а при его утере – сообщение в УЦ.



Электронный документооборот (ЭДО)

Электронный документооборот

Электронный документооборот (ЭДО) - система процессов по обработке документов в электронном виде без их фиксации на бумажном носителе.

ЭДО регламентирован :

- Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ.
- Отраслевыми документами, содержащими положения о работе с ЭДО в различных сферах деятельности: рекомендации и приказы Росархива и пр.

Система электронного документооборота

Система электронного документооборота (СЭДО, EDMS-Electronic Document Management Systems) - информационная система (или соответствующее программное обеспечение), позволяющее организовать работу с ЭДО в полном жизненном цикле документа, а также взаимодействие между сотрудниками по вопросам документооборота.

Функционал СЭДО :

- 1) Управление документами (создание, контроль версий, выписка/возврат, безопасность, группировка).
- 2) Совместная работа над документами общего доступа.
- 3) Сканирование и управление образами бумажных документов.
- 4) Принципами организации для поддержки бизнес-процессов, маршрутизации документов, назначения рабочих задач и контроля их выполнения.

СЭДО, поддерживающая три и более из приведенных функций, относится к комплексной.

Виды СЭДО

По реализуемым функциям СЭО делятся на:

- 1) Системы делопроизводства.
- 2) **Электронные архивы**: система структурированного хранения ЭД, обеспечивающие сохранность и доступность данных.
Основной функционал:
 - Прием на хранение ЭД и сопутствующее оформление дел на основе передачи документов из других ИС или их оцифровки;
 - Управление хранящейся документацией;
 - Поиск по номенклатурам, атрибутам и по тексту;
 - Учет выдачи оригиналов документов и дел.
- 3) **Workflow-системы** – система, позволяющая координировать выполнение и контроль появляющихся в организации задач, назначая их индивидуально исполнителям или рабочим группам.
- 4) **Комплексные (ЕСМ) системы** – системы управления различными по структуре и содержащимся данным документами, а также их хранение, обработка, доставка, разграничение прав доступа к информации.

Роуминг в СЭДО

Роуминг в ЭДО имеет значение только между организациями, обменивающимися ЭД и подключенными к разным операторам ЭДО.

Роуминг может быть реализован:

- через роумингового оператора;
- напрямую с каждым оператором ЭДО.



Алгоритм работы внешнего ЭДО с роумингом:

- Отправитель генерирует электронный документ в собственной СЭД или в сервисе, непосредственно предоставляемым оператором, указывая в нем данные контрагента;
- Оператор 1 взаимодействует с оператором 2, обеспечивая возможность передачи ЭД;
- Получатель принимает ЭД либо в сервисе, либо в собственной СЭД, подключенной к сервису;
- Оператор фиксирует данные о документе.

Угрозы безопасности в СЭДО

Угрозы в СЭДО классически подразделяются на угрозы К-Ц-Д (конфиденциальности, целостности и доступности). Как и других ИС угрозам подвержены следующие элементы: **рабочие места; каналы связи и БД (серверная часть).**

Угрозы конфиденциальности:

- ❑ **НСД к рабочим местам:** физический доступ к рабочим станциям, когда злоумышленник имеет данные для идентификации и аутентификации в СЭДО с пользовательскими или административными правами.
- ❑ **НСД к серверу ОС, СЭДО или БД СЭДО:** получение частичного или полного контроля над системой, а также доступа к обрабатываемым документам.
- ❑ **НСД через канал связи между элементами системы:** реализация атаки с целью перехвата пакетов между сервером и рабочими станциями.

Угрозы целостности направлены на:

- ❑ **ЭД и их резервные копии.**
- ❑ **серверы ОС и СЭДО или БД СЭДО:** при соответствующем администрировании не являются критичными.

Угрозы нарушения доступности связаны с ошибками в настройке системы, разграничении прав доступа. Нарушение доступности как итог может привести к остановке бизнес-процессов всей организации.

Разграничение прав доступа в СЭДО

Разрешительная система управления доступом основывается на предоставлении пользователю такого объема конфиденциальной информации, который необходим для выполнения его обязанностей.

Требования к системе управления доступом в СЭДО:

- передаваемая КИ должна полностью соответствовать функциональным обязанностям сотрудника;
- критерий доступа к КИ – только служебная необходимость;
- исключение возможности НСД к конфиденциальным документам при любых условиях;
- состав лиц, управляющих доступом четко определен и задокументирован;
- исключение несанкционированного управления доступом;
- создание необходимых условий работы с КИ в соответствующих помещениях;
- организована и регламентирована работа всех категорий пользователей с КИ.



Технические и программные средства защиты конфиденциальных данных

Пути несанкционированного доступа

- дистанционное фотографирование;
- перехват электромагнитных излучений;
- хищение носителей информации;
- считывание данных;
- копирование носителей информации;
- маскировка под зарегистрированного пользователя путем хищения паролей и других реквизитов доступа;
- использование вредоносных программ;
- несанкционированное подключение к аппаратуре или линиям связи ЛВС;
- вывод из строя механизмов защиты.

Виды каналов утечки информации

Канал утечки информации – это совокупность источников информации, материального носителя или среды распространения сигнала, несущего эту информацию, и средства выделения информации из сигнала или носителя.

- 1) Электромагнитный канал: связан с возникновением электромагнитного поля, образующегося при протекании электрического тока в средствах обработки информации. В близкорасположенных проводных линиях электромагнитное поле может индуцировать токи (т.н. наводки).
- 2) Канал несанкционированного копирования.
- 3) Канал несанкционированного доступа.

Основные каналы утечки информации

Просмотр печатаемого текста



Несанкционированный доступ к HDD (хищение паролей, использование вредоносных программ)

Просмотр изображения на мониторе

Утечки по электромагнитному каналу: наводка на специальную аппаратуру; утечки через линии связи между ПЭВМ; передача информации вмонтированными устройствами

Несанкционированное копирование носителей

Хищение носителей или документов

Средства и способы защиты конфиденциальной информации

Физические

Устройства и системы, препятствующие доступу к защищаемой информации (электронно-механическое оборудование охранной сигнализации; замки на дверях; решетки на окнах).

Препятствие

Способ, физически преграждающий путь злоумышленнику к защищаемой информации (на территорию и в помещения с носителями информации).

Технические средства

Аппаратные

Устройства, встраиваемые в аппаратуру или сопрягаемые с аппаратурой по стандартному интерфейсу.

Управление доступом

Способ защиты, заключающийся в регулировании использования всех ресурсов системы (технических, программных средств, элементов данных).

- идентификация пользователей;
- проверка полномочий (проверка соответствия времени суток, дня недели и запрашиваемых ресурсов установленному регламенту);
- разрешение в пределах установленного регламента;
- регистрация обращений к защищаемым ресурсам;
- реагирование при несанкционированных действиях

Средства и способы защиты конфиденциальной информации

Программные средства

Программы, выполняющие функции защиты информации

Маскировка
(кодирование информации)

Способ, подразумевающий криптографическую обработку защищаемой информации

Организационные средства

Мероприятия, осуществляемые при создании и эксплуатации систем обработки информации для ее защиты

Регламентация

Средства и способы защиты конфиденциальной информации



Способы защиты информации от утечек

Способы защиты от утечек по электромагнитному каналу

Принципиально различают 2 способа защиты:

- 1) Постановка **активных помех** – использование **генераторов электромагнитного шума**



- 2) Пассивная защита – **экранирование помещения** **отражающими материалами** (сталь, алюминий с заземлением) **электромагнитное излучение**

Способы защиты информации от утечек

Идентификация и аутентификация

Идентификация - процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта. Для выполнения процедуры идентификации в информационной системе субъекту предварительно должен быть назначен соответствующий идентификатор. Идентификация эквивалентна сообщению «своего имени».

Аутентификация - процедура проверки подлинности, подлинность идентифицированного субъекта может быть подтверждена:

- Тем, что пользователь знает (пароль, личный идентификационный номер, криптографический ключ);
- Тем, чем пользователь владеет (личная карточка);
- Тем, что является частью его самого (биометрические признаки, отпечатки пальцев, голос);
- Информация, однозначно ассоциированная с ним (GPS-координаты).

Способы защиты информации от утечек

Идентификация и аутентификация

Наиболее распространенный способ аутентификации – **парольная защита**. У данного способа существуют недостатки: перехват при передаче по линиям электронной связи, хищение, ввод методом подбора.

Способы повышения надежности парольной защиты:

- Наложение технических ограничений (пароль должен не быть слишком коротким, содержать буквы, цифры, знаки пунктуации);
- Управление сроком действия паролей, их периодическая смена;
- Ограничение доступа к файлу паролей;
- Ограничение числа неудачных попыток входа в систему (затруднение метода перебора);
- Использование программных генераторов паролей.

Способы защиты информации от утечек

Управление доступом

Средства управления доступом позволяют контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими ресурсами).

Контроль прав доступа производится разными компонентами программной среды – ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных посредническим программным обеспечением.

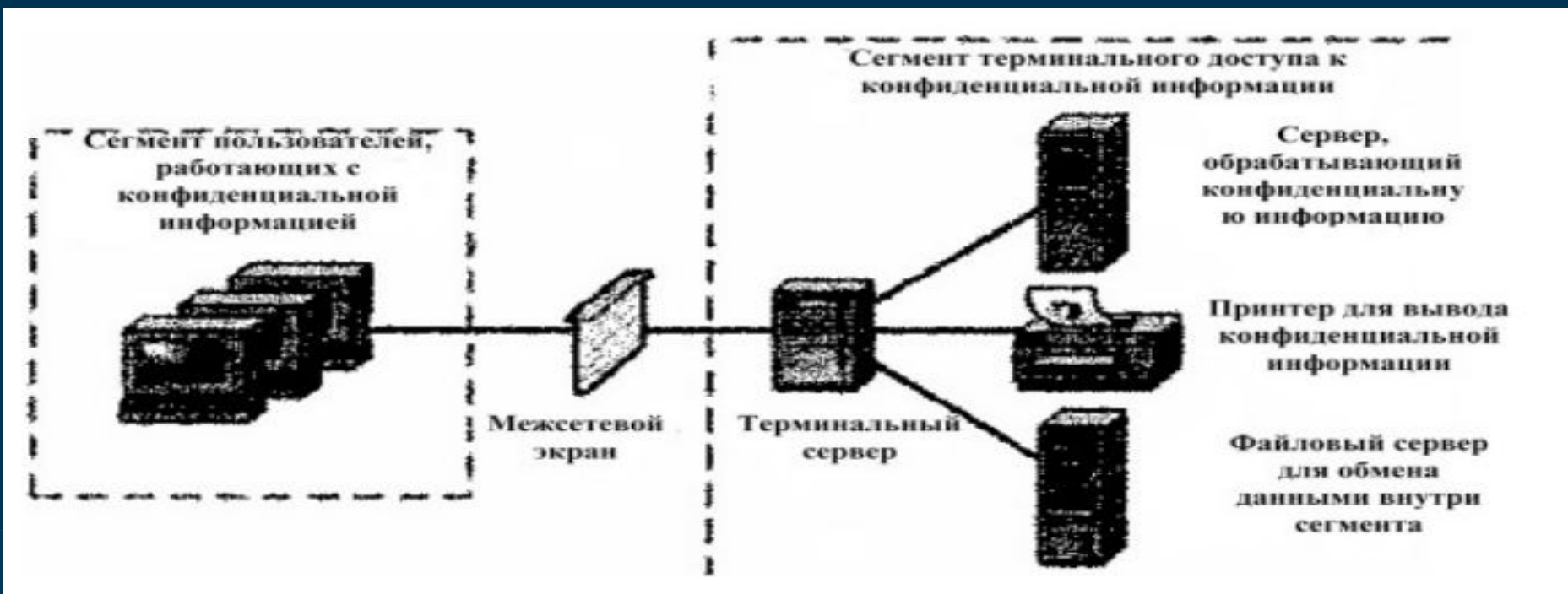
При предоставлении доступа анализируется следующая информация:

- Идентификатор субъекта (идентификатор пользователя, адрес компьютера);
- Атрибуты субъекта (метка безопасности, группа пользователя);
- Место действия (надежный узел сети);
- Время действия (большинство действий целесообразно разрешать в рабочее время).

Способы защиты информации от утечек

Выделенный сегмент терминального доступа

Суть – организация доступа к конфиденциальной информации через промежуточные терминальные серверы: пользователь подключается к терминальному серверу, на котором установлены приложения для работы с конфиденциальной информацией. После этого пользователь в терминальной сессии запускает эти приложения и работает с ними так, будто они установлены на его рабочей станции. То есть пользователь получает только графическое отображение информации, хранящейся на терминальном сервере.



Способы защиты информации от утечек

Протоколирование и аудит

Протоколирование – сбор и накопление событий, происходящих в информационной системе организации: внешних (вызваны действием других сервисов); внутренние (вызваны действием самого сервиса) и клиентские (вызваны действием пользователей и администраторов).

Аудит – анализ накопленной информации, проводимый оперативно или периодически.

Протоколирование и аудит позволяют:

- Обеспечить подотчетность пользователей и администраторов (как средство сдерживания – если пользователь знает, что все его действия фиксируются, то вероятность несанкционированных действий с его стороны ниже);
- Обеспечить возможность реконструкции последовательности событий (выявление уязвимостей в защите сервисов);
- Обнаружить попытки нарушения информационной безопасности;
- Получить информацию для выявления и анализа проблем.

Способы защиты информации от утечек

Средства криптографической защиты

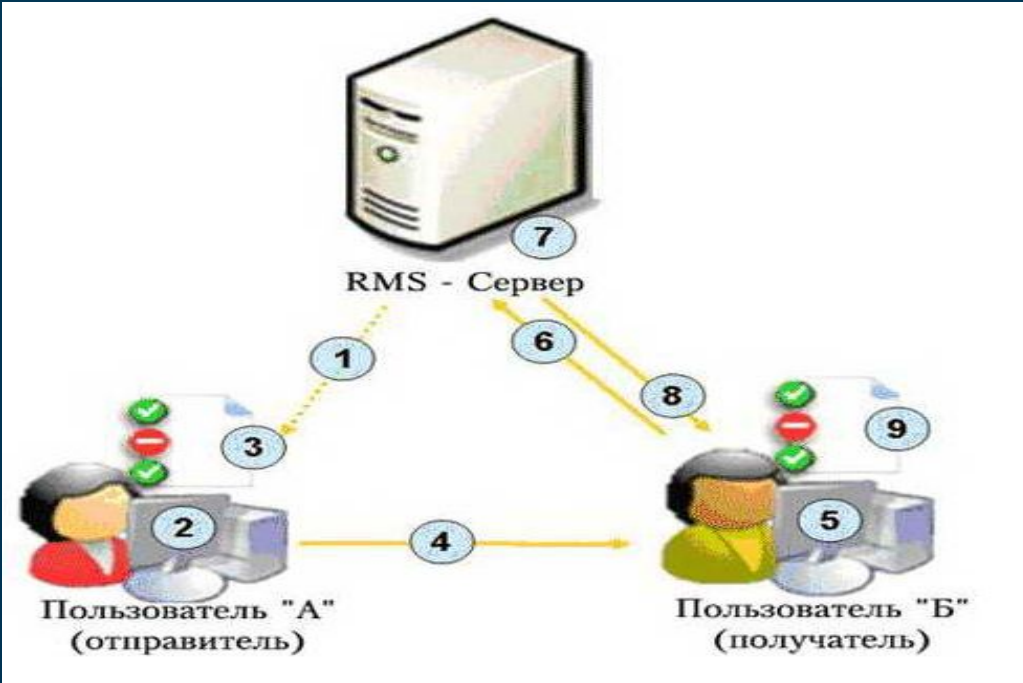
Криптографические средства обеспечивают шифрование конфиденциальных данных, хранящихся на жестких дисках или других носителях. При этом ключ, необходимый для декодирования зашифрованной информации, хранится отдельно, на внешнем носителе (USB-носитель, ключ Touch Memory).

Одним из практических решений криптографической защиты является технология **RMS** (Windows Rights Management Services). Суть ее заключается в том, что вся конфиденциальная информация хранится и передается в зашифрованном виде, а ее дешифрование возможно только на тех компьютерах и теми пользователями, которые имеют на это права.

Способы защиты информации от утечек

Windows Rights Management Services

Общий алгоритм работы RMS:



- (1) Загрузка с RMS-сервера ключа, который будет использоваться для шифрования КИ.
- (2) Формирование пользователем А КД с помощью приложения, поддерживающего функции RMS (например, Microsoft Word); формирование тем же пользователем списка разрешенных субъектов и операций над документом; информация записывается в XML-файл.
- (3) Шифрование документа с помощью случайно сгенерированного сеансового ключа, формируемого на основе открытого ключа (этап 1), расшифровка возможна только через RMS-сервер, хранящий ключ.

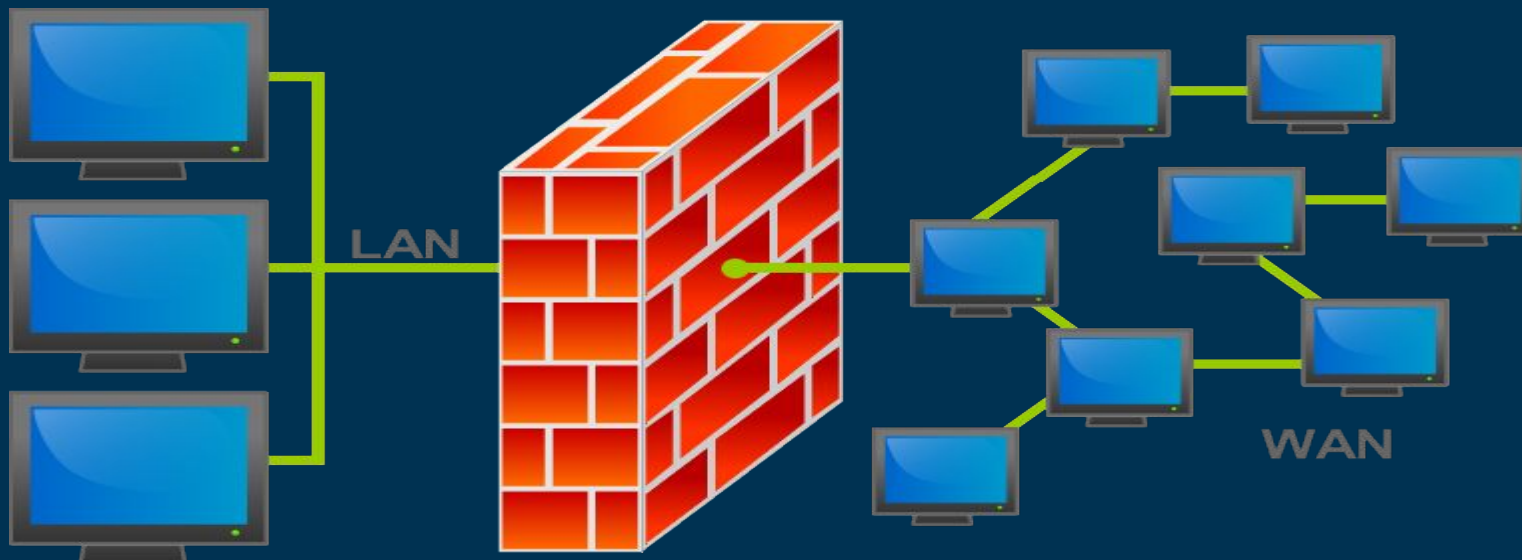
- (4) Отправка пользователю Б зашифрованного КД вместе с XML-файлом.
- (5) Открытие документа пользователем Б, для чего отправляется запрос на сервер;(6) .
- (7) Проверка прав доступа пользователю Б к КД в соответствии с XML-файлом. При этом из XML-файла извлекается ключ, дешифруется и формируется новый на основе открытого ключа пользователя Б.
- (8) RMS-сервер отправляет пользователю Б новый XML-файл, на основе которого КД открывается (9).

Способы защиты информации от утечек

Экранирование

Экран средство ограничения доступа клиентов из одного множества к серверам из другого множества. Экран контролирует все информационные потоки между множествами систем; осуществляет протоколирование информационных обменов.

Для экрана определены понятия «внутри»/ «снаружи», при этом задача экранирования – защита внутренней области от внешней. Кроме этого, экранирование дает возможность контролировать информационные потоки, направляемые во внешнюю область.



**Экран как средство
разграничения доступа**

Способы защиты информации от утечек

Экранирование

Экран также можно представлять как последовательность фильтров. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран.



Экран как последовательность фильтров

Способы защиты информации от утечек

Средства контентного анализа исходящих пакетов

Средства контентного анализа предоставляют возможность обработки исходящего сетевого трафика, отправляемого за границы контролируемой зоны с целью выявления возможной утечки КИ. Используются, как правило, для анализа исходящего почтового и web-трафика.

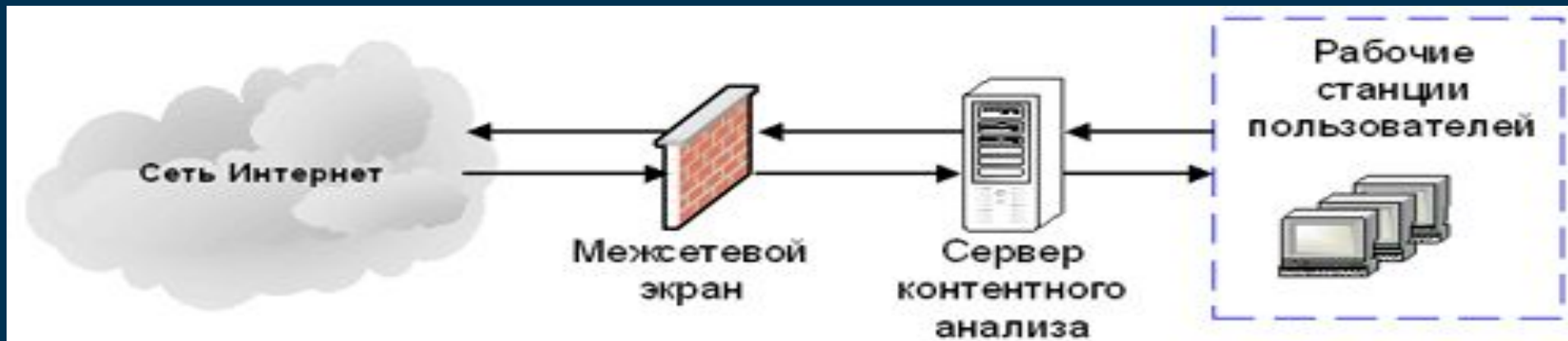


Схема установки средств анализа исходящего трафика

При анализе исходящих сообщений они обрабатываются в соответствии с заданными служебными полями, содержащими критерии анализа, которые задаются администратором (ключевые слова — «конфиденциально», «служебная тайна»). Метод практически не работает, если отправлять информацию в зашифрованном виде или передавать другими способами, кроме текста (например, аудио).

Способы защиты информации от утечек

Системы активного мониторинга рабочих станций

Системы активного мониторинга представляют собой программные комплексы, предназначенные для выявления несанкционированных действий пользователей – попыткой передачи КИ.



Блок-схема системы мониторинга

Способы защиты информации от утечек

Системы активного мониторинга рабочих станций

Системы активного мониторинга состоит из следующих компонентов:

- Модули-датчики – устанавливаются на рабочие станции пользователей, собирают информацию о регистрируемых событиях;
- модуль анализа данных – выявляют несанкционированные действия пользователя;
- модуль реагирования на выявленные несанкционированные действия;
- модуль хранения результатов;
- модуль управления компонентами системы.

Системы активного мониторинга состоит из следующих компонентов устанавливаются на рабочие станции, обрабатывающие КИ. Настройки датчиков системы позволяют не только контролировать действия пользователя, но и ограничивать определенные действия – копирование на внешний носитель, вывод на печать.

Программные продукты, используемые для защиты КИ

Классы продуктов для защиты КИ

Управление правами доступа к информации в масштабах предприятия (Enterprise Rights Management, ERM)

Защищают информацию от несанкционированного доступа.

Microsoft RMS

Выявление и предотвращение утечек конфиденциальных данных (Information Leakage Detection and Prevention, ILD&P)

Защищают информацию от утечки, уничтожения и искажения при легальном к ней доступе.

InfoWatch Enterprise Solution

Программные продукты, используемые для защиты КИ

InfoWatch Enterprise Solution

Архитектура программного решения носит распределенный характер и включает следующие программные компоненты:

- Web Monitor (IWM)
- Mail Monitor (IMM)
- Net Monitor (INM)
- Device Monitor (IDM).

IWM и IMM – сетевые фильтры, контролирующие трафик по web- и электронной почте (отсекают утечку через e-mail, чаты, форумы).

INM / IDM контролируют оборот КИ на уровне рабочих станций. INM следит за действиями в средах Office и Adobe, контролирует вывод документов на печать, работу с буфером обмена и файловые операции; IDM управляет доступом к коммуникационным портам (CD, USB, Floppy, Wi-Fi и т.п.)

Программные продукты, используемые для защиты КИ

InfoWatch Enterprise Solution

Принцип использования IES – конфиденциальная информация не должна покидать периметр корпоративной сети. При внедрении создается специальная база контентной фильтрации, соответствующая специфике бизнес-профиля компании. Используя эту базу в качестве эталона, фильтры IES выявляют конфиденциальную информацию и препятствуют ее выходу за защищаемый периметр.

Спасибо!