

КРАСНОДАРСКИЙ УНИВЕРСИТЕТ МВД РОССИИ  
КРЫМСКИЙ ФИЛИАЛ  
Кафедра оперативно-разыскной деятельности и специальной техники

Учебно-наглядное пособие

Дисциплина: Делопроизводство и режим секретности в органах внутренних дел  
специальность 40.05.01 Правовое обеспечение национальной безопасности  
Специализация Уголовно-правовая  
Профиль образовательной программы – Предварительное следствие  
в органах внутренних дел

Тема № 6  
«Сервис электронного документооборота ИСОД МВД России»

Обсуждено и одобрено  
на заседании кафедры,  
протокол № 28  
от 26 июля 2023 г.

Подготовил:  
старший преподаватель кафедры,  
подполковник полиции

В.А. Зоз

Симферополь  
2023

## Цели лекции:

1. Образовательная – охарактеризовать понятие ИСОД МВД России, прикладных сервисов, сервиса электронного документооборота ИСОД МВД России, объяснить порядок применения средств электронной подписи, организацию защиты информации в ИСОД обучающимся профиля образовательной программы – Предварительное следствие в органах внутренних дел.
2. Методическая – активизировать познавательную деятельность обучающихся на учебном занятии в процессе работы с учебным наглядным пособием.
3. Развивающая – сформировать у обучающихся знания в области работы ИСОД МВД России, сервиса электронного документооборота ИСОД МВД России.
4. Воспитательная - воспитать чувство ответственности при осуществлении профессиональной деятельности, в части использования ИСОД МВД России, прикладных сервисов и сервиса электронного документооборота (ПК-15/4).

## План лекции

### Введение

1. Основные понятия ИСОД МВД России.
  2. Защита информации в ИСОД МВД России.
  3. Применение средств электронной подписи в ОВД.
  4. Основные положения о СЭД МВД России
- Заключение(выводы)

## Список использованной литературы

а) нормативные правовые акты:

1. Конституция Российской Федерации (с учетом последних изменений) // ИПО «Гарант». – URL: <http://www.garant.ru>.
2. Об информации, информационных технологиях и о защите информации: федер. Закон от 27 июля 2006 г. №149-ФЗ (с учетом последних изменений) // ИПО «Гарант». – URL: <http://www.garant.ru>.
3. Об утверждении Перечня документов, образующихся в деятельности МВД РФ, с указанием сроков хранения, создания, хранение и использование которых осуществляется в форме электронных документов: приказ МВД России от 31 мая 2011 года № 600 (с учетом последних изменений) // ИПО «Гарант». – URL: <http://www.garant.ru>.

б) основная литература

1. . Организация работы подразделений делопроизводства и режима [Текст]: учебно-практическое пособие / сост. С. О. Бевз . - Краснодар : Краснодарский ун-т МВД России, 2022. - 166 с.
2. Информационные технологии управления и организация защиты информации [Электронный ресурс] : учебник / В. В. Баранов, И. В. Горошко, В. Н. Лебедев, В. Ф. Макаров [и др.]} . - М. : Академия управления МВД России, 2018. - 456 с.
3. Применение современных инфокоммуникационных технологий в управлении деятельностью подразделений органов внутренних дел: учебно-практическое пособие [Электронный ресурс] : учебное пособие / К. М. Бондарь, А. В. Рыбак, П. П. Скрипко} . - Электрон. текстовые дан. - М. : ДГСК МВД России, 2018

# **1. Основные понятия ИСОД МВД России**

# ИСОД МВД России –

единая система информационно-  
аналитического обеспечения  
деятельности МВД России

# «Должностное лицо - техническая Система - должностное лицо»

Принятое решение любого должностного лица в рамках служебной компетенции для придания ему юридической силы удостоверяется электронной подписью и чётко фиксируется во времени, а также сохраняется весь последующий механизм его исполнения с возможностью контроля соответствующими субъектами

# Цель ИСОД МВД России заключается:

в повышении уровня информационно-аналитического обеспечения деятельности МВД России, выражающаяся в обеспечении сотрудникам основных направлений деятельности ОВД и в соответствии со служебной компетенцией возможности использования:

- увеличенного количества видов актуальной структурированной информации в электронной форме, одновременно доступной с автоматизированных рабочих мест (АРМ), и обеспечении быстрого поиска необходимой информации

# Цель ИСОД МВД России заключается:

в повышении уровня информационно-аналитического обеспечения деятельности МВД России, выражающаяся в обеспечении сотрудникам основных направлений деятельности ОВД и в соответствии со служебной компетенцией возможности использования:

- обобщённых актуальных данных при принятии управленческих решений.

# Задачей ИСОД является

автоматизация основных видов деятельности сотрудников подразделений МВД России, которая призвана:

- интегрировать информационные ресурсы МВД России на основе единых информационных банков данных
- создать единую систему централизованной обработки данных для информационно-аналитической поддержки деятельности подразделений МВД России
- предоставить возможность ведомственного электронного обмена информацией и внешнего электронного взаимодействия подразделений МВД России с органами государственной власти

# Задачей ИСОД является

автоматизация основных видов деятельности сотрудников подразделений МВД России, которая призвана:

- создать подсистему обеспечения информационно-аналитической деятельности оперативно-технических подразделений МВД России
- обеспечить предоставление государственных услуг в электронном виде и развитие соответствующих информационных систем, интегрируя их с компонентами инфраструктуры электронного правительства
- совершенствовать профессиональную подготовку и переподготовку в области информационных технологий

## Концепция построения ИСОД:

реализация сервис-ориентированной архитектуры для создания системы автоматизации прикладных задач ИСОД.

использование технологии «облачных вычислений» – технологии обеспечения повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов

построение централизованной схемы инфраструктуры на базе центров обработки данных (ЦОД) единого, масштабируемого, программно-аппаратного решения на всех уровнях структурной организации ОВД

максимальное использование имеющихся в ОВД программно-технических комплексов обеспечения деятельности (ПТК), развертывание на их основе типового, масштабируемого решения для обеспечения деятельности ОВД в составе системы прикладных задач ИСОД

# Облачные вычисления –

при обработке информации компьютерные ресурсы (то есть вычислительные мощности, программное обеспечение, данные) предоставляются пользователю в режиме реального времени как распределённый в вычислительной сети сервис (так называемый онлайн Net-сервис)

*Основными элементами ИСОД МВД России являются:*

- ИМТС – интегрированная мультисервисная телекоммуникационная сеть;
- ЦОД (центр обработки данных) и ПТК (программно-технический комплекс);
- ЕЦЭ – единый центр эксплуатации сервисов ИСОД;
- ПОИБ – подсистема обеспечения информационной безопасности;
- сервисы повседневной деятельности;
- сервисы оперативно-служебной деятельности.

*Интегрированная телекоммуникационная сеть предоставляет доступ сотрудникам органов внутренних дел к услугам специальных федеральных информационно-телекоммуникационных систем, автоматизированных банков данных на базе унифицированных программно-технических комплексов информационно-аналитических и экспертно-криминалистических центров органов внутренних дел.*



Центр  
обработки  
данных



Кустовой  
программно-  
технический  
комплекс



Программно-  
технический  
комплекс

***В подсистему обеспечения информационной безопасности (ПОИБ) входят:***

- криптографическая защита каналов связи;
- антивирусная система;
- сервис СУДИС;
- средства защиты от несанкционированного доступа;
- аппаратные идентификаторы rutoken, крипто-про;
- комплекс организационных мер.

# АРМ ИСОД МВД России



# ***Сервис управления доступом к информационным системам***

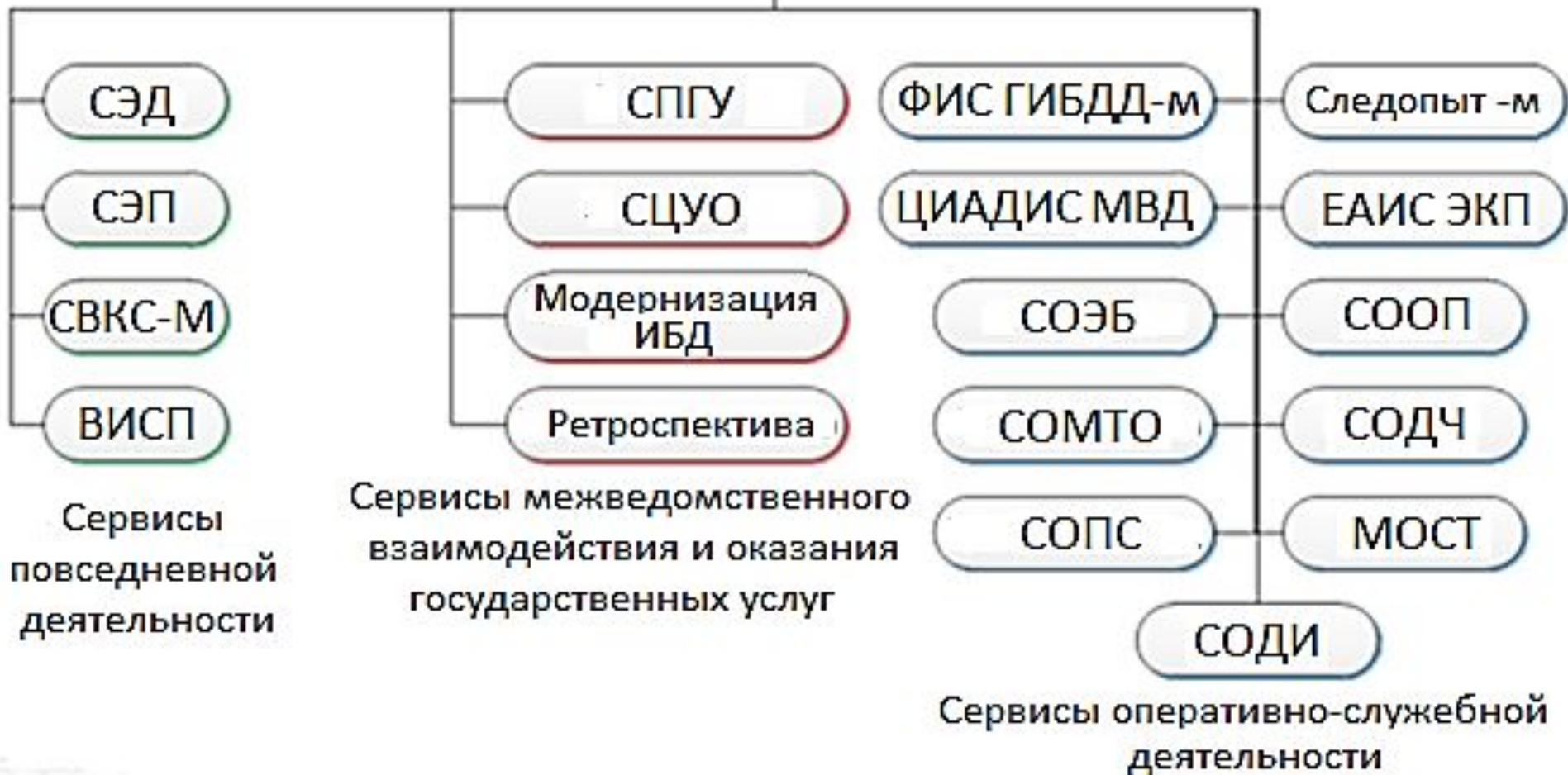
## ***обеспечивает:***

- управление доступом пользователей в систему;
- управление доступом пользователей к сервисам ИСОД;
- единую точку входа в сервисы ИСОД;
- регистрацию событий безопасности.

## **позволяет:**

- организовать контроль пользователей, имеющих доступ к сервисам ИСОД;
- обеспечить доступ к ресурсам по электронной подписи.

# СУДИС



## *Ведомственный информационно-справочный портал МВД России (ВИСП) обеспечивает:*

- доступ сотрудников к внутренней ведомственной информации, связанной с ИСОД МВД России;
- доступ сотрудников к сведениям об организационно-штатной структуре МВД России;
- доступ сотрудников к адресно-телефонному справочнику МВД России;
- информирование сотрудников о мероприятиях, связанных с ИСОД МВД России.

# Ведомственный информационно-справочный портал МВД России (ВИСП)



# Сервисы обеспечения охраны общественного порядка (СООП)



# Сервисы обеспечения деятельности дежурных частей (СОДЧ)



## ***Вывод:***

ИСОД МВД России является эволюционным развитием Единой информационно-телекоммуникационной системы ОВД (ЕИТКС ОВД) и представляет собой сегмент глобальной общегосударственной информационно-телекоммуникационной системы (электронного правительства) на более высоком технологическом уровне и направлена на обеспечение реализации в системе МВД России государственной политики Российской Федерации в области информатизации, связи и технической защиты информации

## **2. Защита информации в ИСОД МВД России**

Приказ МВД России от 24.12.2015 № 1228  
"Об утверждении Правил организации доступа к  
информационно-телекоммуникационной сети  
"Интернет" в органах внутренних дел Российской  
Федерации"

В ИСОД МВД России достигается унификация используемых программно-технических решений и приведение архитектуры основных автоматизированных информационных систем в соответствие современным требованиям к доступности и надежности.

# Механизмы защиты информации в ИСОД МВД России

## МЕХАНИЗМЫ ЗАЩИТЫ ОТ НСД

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПРИ ПОПЫТКАХ ДОСТУПА К РЕСУРСАМ

РАЗГРАНИЧЕНИЕ ДОСТУПА К РЕСУРСАМ И СЕРВИСАМ

КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНЫХ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

ПРОТОКОЛИРОВАНИЕ СОБЫТИЙ БЕЗОПАСНОСТИ

## АНТИВИРУСНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ

УСТАНОВКА КОМПЛЕКТА ПРОГРАММ АНТИВИРУСНОЙ ЗАЩИТЫ

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ КОМПОНЕНТОВ АНТИВИРУСНОЙ ЗАЩИТЫ

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ АНТИВИРУСНОЙ ПОЛИТИКОЙ И ПАРАМЕТРАМИ АНТИВИРУСНОГО КОНТРОЛЯ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ СОТРУДНИКОВ И СЕРВЕРОВ

## КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ЗАЩИТЫ

ШИФРОВАНИЕ И ИМИТОЗАЩИТА ДАННЫХ

ЭЛЕКТРОННАЯ ПОДПИСЬ

КОНТРОЛЬ ЦЕЛОСТНОСТИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

## МЕХАНИЗМЫ ЗАЩИТЫ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

УСТАНОВКА МЕЖСЕТЕВЫХ ЭКРАНОВ

ОБНАРУЖЕНИЕ АТАК

ФИЛЬТРАЦИЯ СЕТЕВОГО ТРАФИКА

# VPN (Virtual Protected Network) -

это совокупность локальных сетей и отдельных компьютеров, объединенных в единую виртуальную защищенную сеть, с целью обеспечения:

- конфиденциальности;
- целостности;
- аутентичности данных.

# Основные компоненты защищенной сети ViPNet :



ViPNet Administrator. Выполняет функции создания, настройки, модификации и управления защищенной VPN-сетью



ViPNet Coordinator. VPN-сервер с интегрированными персональным и межсетевым экранами, выполняет работу NAT и проху, является защищенным почтовым сервером, а также туннельным сервером для создания защищенных соединений между незащищенными компьютерами



ViPNet Client. Модуль предназначен для защиты отдельных компьютеров. Устанавливается на компьютер каждого VPN-пользователя, обеспечивает защищенное соединение с другими пользователями и защиту самого компьютера от сетевых атак

## ***ViPNet Client -***

это программное обеспечение, выполняющее задачу защиты локального компьютера.

Включает в себя следующие компоненты:

- 1. Персональный сетевой экран*** - средство защиты от несанкционированных попыток получить доступ к компьютеру извне.
- 2. Шифратор трафика*** - средство защиты информации криптографическими методами.

**ВЫВОД:** Для обеспечения защиты информации в ИСОД МВД России создана подсистема обеспечения информационной безопасности, которая включает в себя средства защиты инфраструктуры, средства защиты сервисов и средства защиты автоматизированных рабочих мест.

В целях ограничения доступа к информационным ресурсам ИСОД МВД России определены требования по обеспечению безопасности информации для контура обработки информации, составляющей государственную тайну, и контура обработки информации ограниченного доступа, не составляющей государственную тайну. Определены требования по обеспечению безопасности информации при доступе к информационным ресурсам ИСОД МВД России с использованием мобильных устройств. Разработаны организационные и технические меры, составляющие комплексную и взаимоувязанную подсистему обеспечения информационной безопасности ИСОД МВД России.

## **4. Применение средств электронной подписи в ОВД**

Отношения в области использования электронных подписей регулируются Федеральным законом от 06.04.2011 № 63-ФЗ (Изм. от 24.02.2021 № 20-ФЗ) «Об электронной подписи».

Под электронной подписью (ЭП) понимается

реквизит электронного документа, защищенный от подделки, полученный в результате криптографического преобразования информации с использованием личного ключа ЭП, позволяющий установить обладателя электронной цифровой подписи, а также отсутствие утраты, искажения или подделки содержащейся в электронном документе информации.

## Использование электронной подписи позволяет решать следующие задачи:

Контроль целостности передаваемого документа

- при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему

Защита от изменений (подделки) документа

- гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев

Невозможность отказа от авторства

- так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом

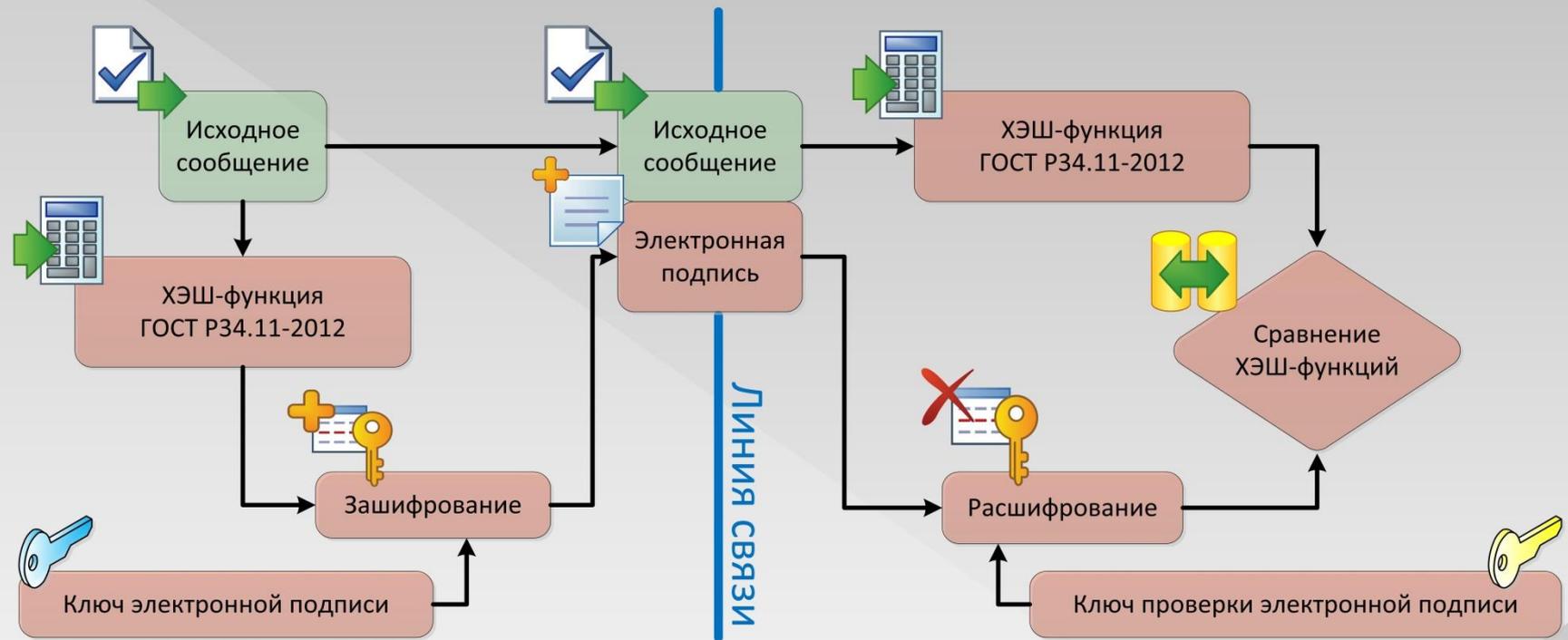
Доказательное подтверждение авторства документа

- так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство подписи под документом.

Существуют два сертифицированных алгоритма, определяющих порядок выработки и проверки электронной подписи, закрепленных в государственных стандартах:

- ГОСТ Р 34.10-2012 описывает алгоритмы формирования и проверки электронной цифровой подписи.
- ГОСТ Р 34.11-2012 определяет алгоритм и процедуру вычисления хэш-функции для последовательности символов.

# СХЕМА ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ



Электронная подпись (ЭП) - 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 (ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи»).

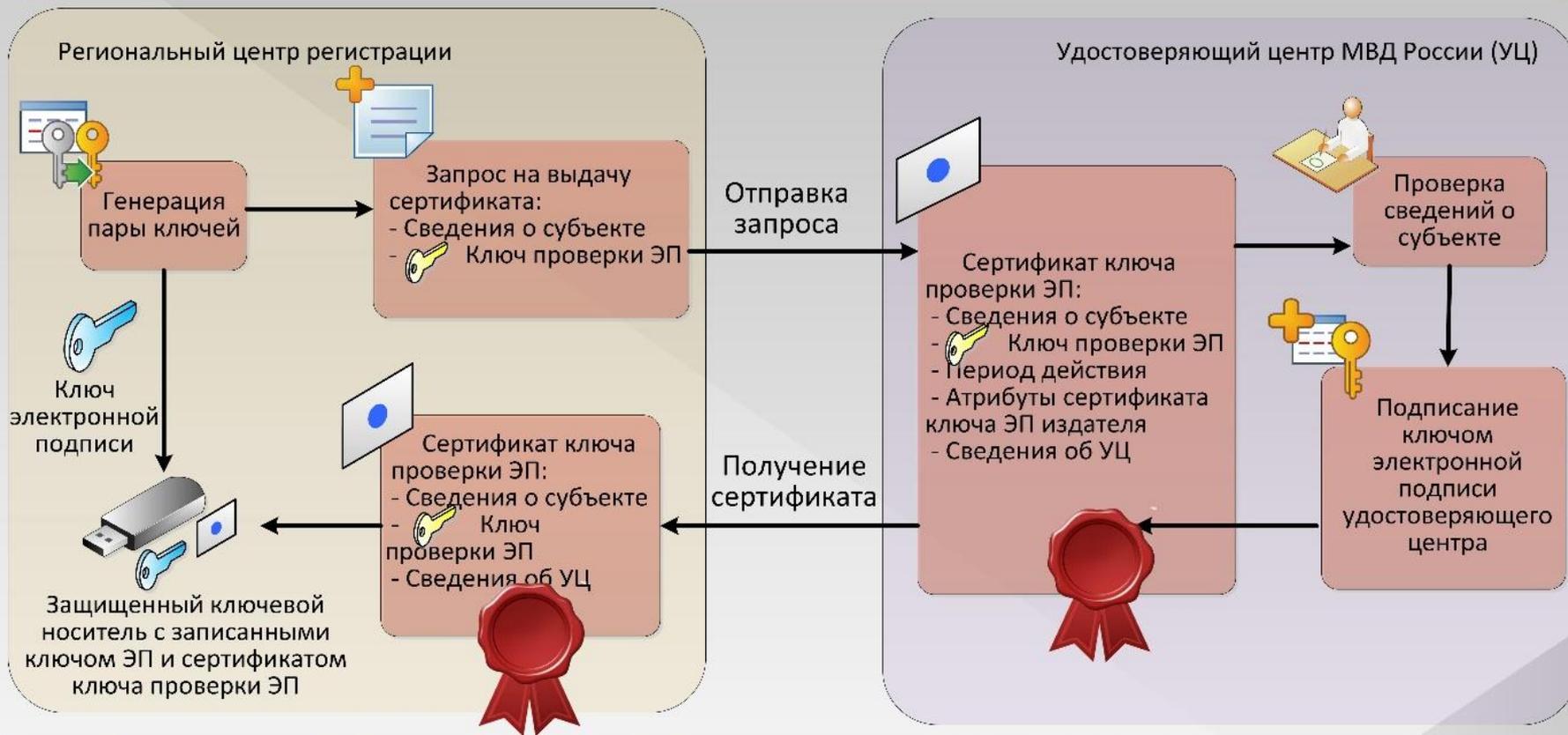
Электронная подпись — реквизит электронного документа, вырабатываемый с помощью закрытого ключа и проверяемый с помощью соответствующего открытого ключа. Она свидетельствует о целостности подписанного документа и что выработавший ее субъект знает закрытый ключ. Неотрекаемость от подписи гарантируется тем, что правильно подписать документ можно, только владея закрытым ключом.

# Сертификат ключа проверки электронной подписи

–

это 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.

# СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ



Служит для связывания ключа проверки ЭП с субъектом, правомерно владеющим соответствующим ключом ЭП. Без такой верификации злоумышленник может выдать себя за любого субъекта, подменив ключ проверки ЭП.

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 .

## Удостоверяющий центр (УЦ) –

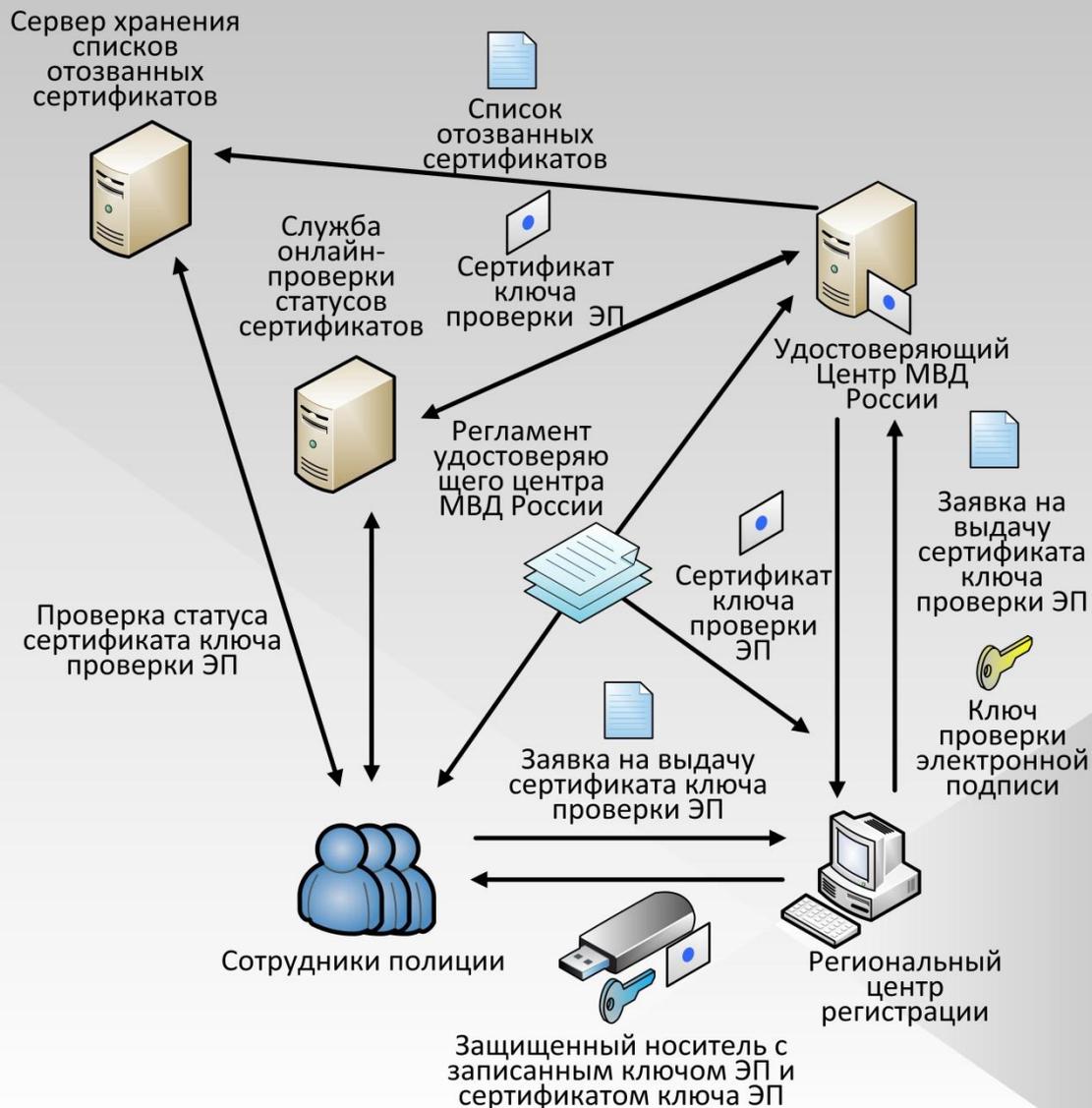
юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

# СИСТЕМА УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ МВД РОССИИ

Система удостоверяющих центров органов внутренних дел Российской Федерации (СУЦ ОВД) – автоматизированная система, предназначенная для реализации возможностей средств электронной подписи в подразделениях системы МВД России.

Удостоверяющий центр МВД России – подразделение, входящее в состав ФКУ «ГЦСиЗИ МВД России», на которое возложены функции удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и приказом МВД России от 28 мая 2013 г. № 294 «О вводе в эксплуатацию Системы удостоверяющих центров органов внутренних дел Российской Федерации».

Удостоверяющий центр МВД России осуществляет деятельность по созданию и управлению сертификатами ключей проверки электронной подписи сотрудников МВД России на территории Российской Федерации.



# Основные процедуры процесса регистрации ЭП

- передача в региональный центр регистрации заявки на издание сертификата ключа подписи, согласованной с уполномоченными руководящими сотрудниками подразделений ОВД
- проверка оператором автоматизированного рабочего места центра регистрации (АРМ ЦР) в соответствии с Регламентом УЦ данных, содержащихся в заявке
- регистрация пользователя в УЦ оператором АРМ ЦР
- издание (выпуск и публикация) сертификата ключа подписи

# Электронные идентификаторы, используемые в МВД России

*Ключевой носитель* – отчуждаемый физический носитель, содержащий один или несколько ключей электронной подписи, а при необходимости и иную контрольную, служебную и технологическую информацию.



ПСКЗИ ШИПКА



eToken



JaCarta



Rutoken

В соответствии с Регламентом Удостоверяющего центра МВД России допускается применять в качестве ключевых носителей устройства типа eToken, JaCarta, Rutoken и Шипка, сертифицированные ФСТЭК России.

# Перечень компонентов и программного обеспечения, которые необходимы для работы с электронной подписью

Крипто ПРО CSP (<http://www.cryptopro.ru>)

Драйвер носителя ключа

RuToken (<http://www.rutoken.ru>)

eToken (<http://www.aladdin-rd.ru>)

Прикладное ПО для работы с электронной подписью  
(в зависимости от конкретной службы ОВД)

Список отзыва удостоверяющего центра  
(<http://www.ucmvd.ru>)

Личный сертификат  
(хранится на полученном в УЦ защищенном носителе)

**ВЫВОД:** Под электронной подписью (ЭП) понимается реквизит электронного документа, защищенный от подделки, полученный в результате криптографического преобразования информации с использованием личного ключа ЭП, позволяющий установить обладателя электронной цифровой подписи, а также отсутствие утраты, искажения или подделки содержащейся в электронном документе информации. Проверяется ЭП при помощи открытого ключа.

**Вопрос 4. Основные положения ОСЭД  
МВД России**

Порядок работы с электронными документами утвержден приказом МВД России от 20 июня 2012 года №615 «Об утверждении инструкции по делопроизводству в ОВД РФ».

Согласно данному приказу электронный документ должен быть оформлен по общим правилам делопроизводства и иметь реквизиты, установленные для аналогичного документа на бумажном носителе, за исключением оттиска печати и изображения государственного герба РФ.

Обеспечение правовых условий для использования электронной подписи в электронных документах, при соблюдении которых электронная подпись признается юридически равнозначной собственноручной подписи человека в документы на бумажной носителе, осуществляется федеральным законом от 6 апреля 2011 года №63-ФЗ «Об электронной подписи». Данным законом устанавливаются права и обязанности обладателя электронной подписи. Владельцем сертификата ключа подписи (обладателем электронной подписи) является физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи.

*Состав электронных документов, образующихся в системе электронного документооборота, определяется приказом МВД России от 31 мая 2011 года №600 «Об утверждении Перечня документов, образующихся в деятельности ОВД РФ, с указанием сроков хранения, создания, хранения и использование которых осуществляется в форме электронных документов».*

Электронные документы формируются в дела в соответствии с номенклатурой дел и индексируются в порядке, установленном в отношении дел составленных из документов на бумажном носителе. При составлении номенклатуры дел указывается, что дело ведется в электронном виде. Сроки хранения документов, установленные перечнем и указанные в номенклатуре дел, едины для документов на бумажных и электронных носителях. В настоящий момент утвержден четкий порядок ведения работы с электронными документами, что позволяет внедрить в деятельность всех подразделений системы МВД России ЕАИС «ЭДиД».

СЭД должен как минимум предусмотреть механизм защиты от основных угроз:

- обеспечение сохранности документов;
- обеспечение безопасного доступа;
- обеспечение подлинности документов;
- протоколирование действия пользователей.

СЭД должен обеспечить сохранность документов от потери и порчи и иметь возможность их быстрого восстановления. В 45% случаев потеря важной информации приходится на физические причины (отказ аппаратуры, стихийные бедствия и т.п.), 35% обусловлены ошибками пользователей и менее 20% действием вредоносных программ и злоумышленников.

Целью создания СЭД является повышение эффективности организационно-управленческой (административной) деятельности ОВД, связанных с документационным обеспечением и представлением юридически значимого документооборота.

***Поставленная цель достигается путем выполнения следующих задач:***

- повышение полноты и уровня оперативности информационной поддержки принятия управленческих решений в системе МВД России;
- повышение уровня информационной поддержки и эффективности организационно-управленческой(административной) деятельности подразделений делопроизводства и режима территориальных подразделений ОВД РФ;
- повышение уровня информационного взаимодействия в части обмена юридически значимыми электронными документами;
- создание единого информационного пространства документационного обеспечения в ОВД РФ;
- обеспечение единообразия работы с электронными документами в ОВД РФ с сохранением защищенности, управляемости и доступности документов;
- обеспечение сквозного контроля прохождения документов и повышение уровня исполнительской дисциплины сотрудников;
- обеспечение безопасного обмена документами в рамках Сервиса;
- обеспечение безопасности хранения и разграничения доступа к информации, включая журналирование действий пользователей и электронную подпись.

*СЭД обеспечивает выполнение следующих возможностей:*

Регистрация следующих типов документов:

- входящие документы;
- обращения граждан в том числе карточки приема граждан
- НПА;
- приказы;
- исходящие документы;
- входящие секретные документы;
- секретные НПА;
- секретные приказы;
- секретные исходящие документы;

Импорт информации о документах из смежных систем:

- МЭДО;
- обращения граждан;
- НПА;
- входящие документы;

*СЭД разделен на следующие группы сервисов:*

1. Интеграционные сервисы – набор сервисов, обеспечивающие интеграцию между документационными подразделениями и единое пространство документооборота в рамках МВД России.

2. Документационные сервисы – набор сервисов позволяющие автоматизировать работу документационных подразделений МВД России и исполнителей в части электронного документооборота.

3. Мобильный сервис СЭД – приложение для планшетного компьютера позволяющее автоматизировать деятельность руководителей подразделения МВД России по вынесению резолюций (выдаче поручений) с обеспечением юридической значимости выполняемого действия.

**ВЫВОД:** таким образом, электронный документ должен быть оформлен по общим правилам делопроизводства и иметь реквизиты, установленные для аналогичного документа на бумажном носителе, за исключением оттиска печати и изображения государственного герба РФ. Электронные документы создаются, обрабатываются, и хранятся в системах электронного документооборота.

## **Вопросы для самоконтроля:**

1. Понятие Сервиса электронного документооборота ИСОД МВД России.
2. Порядок подготовки документов к отправке.
3. Построение маршрута согласования документа в СЭД МВД России.
4. Порядок исполнения документов и подготовки ответов на служебные письма и обращения граждан и организаций.

## **Задания на самоподготовку:**

1. Изучить требования приказа МВД России от 31 мая 2011 года №600 «Об утверждении Перечня документов, образующихся в деятельности ОВД РФ, с указанием сроков хранения, создания, хранение и использование которых осуществляется в форме электронных документов».
2. Изучить требования приказа МВД России от 20 июня 2012 года №615 «Об утверждении инструкции по делопроизводству в ОВД РФ» в части порядка работы с электронными документами.

**Спасибо за  
внимание!**