МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

Институт искусственного интеллекта

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

специализация № **1** **"**Анализ безопасности компьютерных систем**"**

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОРАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЛЕКЦИЯ № **1-2022.**
Организационное обеспечение защищенности искусственного интеллекта

ЛЕКЦИЯ № **2-2022.**
Организация
цифровой экономики Российской Федерации

ЛЕКЦИЯ № **3-2022.**
Безопасность информации, содержащейся в системе координации информатизации

Лекция № **4-2022.**
Обеспечение информационной безопасности межведомственного взаимодействия

ЛЕКЦИЯ № 5-2022 .
Методология защиты конфиденциальной информации коммерческого характера

ЛЕКЦИЯ № **6-2022.**
Организационное обеспечение информационной безопасности при осуществлении рекламной и публикаторской деятельности

ЛЕКЦИЯ № **7-2022.**
Основные направления и методы работы с персоналом, обладающим конфиденциальной информации

ЛЕКЦИЯ № **8-2022.**
Ответственность за нарушение правил защиты информации

ЛЕКЦИЯ № 9-2022.
Организация внутриобъектового режима на объекте информатизации

ЛЕКЦИЯ № 10-2022.
Аналитическая работа - основа управления организационным обеспечением информационной безопасности

ЛЕКЦИЯ № **11-2022.**
Лицензионные требования при обращении со СТС негласного получения информации

Лекция № 12-2022.
Лицензионные требования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации

ЛЕКЦИЯ № **13-2022.**
Обеспечение лицензионных требований при распространении СКЗИ

ЛЕКЦИЯ № 14-2022.
Сертификация СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

ЛЕКЦИЯ № 15-2022.
Требования по контролю за организацией и обеспечением безопасности информации с использованием сертифицированных СКЗИ

Лекция № 16-2022.
Организационное обеспечение информационной безопасности использования средств электронной подписи

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция № 16-2022.

Организационное обеспечение информационной безопасности использования средств электронной подписи

Лекция № 16-2022.
Организационное обеспечение информационной безопасности использования средств электронной подписи

ВОПРОС 1. Правовые основания разработки Руководства по обеспечению безопасности использования электронной подписи и средств ЭП

ВОПРОС 2. Требования по размещению средств квалифицированной электронной подписи

ВОПРОС 3. Требования по инсталяции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

ВОПРОС 4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации

ВОПРОС 1.

Правовые основания разработки Руководства по обеспечению безопасности использования электронной подписи и средств ЭП

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

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 Федеральным законом.

Информирование заявителей:

— об условиях и порядке использования электронных подписей и средств электронной подписи,

— о рисках, связанных с использованием электронных подписей,

— о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки,

осуществляется путем выдачи Удостоверяющим центром каждому заявителю Руководства по обеспечению безопасности использования ЭП и средств электронной подписи.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Для разработки Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи будут использованы нормативные правовые акты Российской Федерации.

Во-первых, Руководство составляется в соответствии с требованиями Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

Федеральный закон «Об электронной подписи» фиксирует переход от письменного бюрократического общества к информационному обществу, а также создает необходимые правовые условия данного перехода. Закон способствует формированию электронного государства, электронного гражданина, электронного сознания.

Один из главных принципов, который он закрепляет - прозрачность действий владельца электронной подписи. Теоретически исключается подписание электронной подписью электронного документа за другое лицо.

Принцип действия электронной подписи

Подготовка ключей

Закрытый ключ — ***Программно-технический комплекс*** — ***Открытый ключ***

Остаётся у владельца подписи

Передаётся адресату

Хеш-функция *(Идентификатор документа, математически рассчитываемый на основании текста самого документа, позволяющий сравнивать документ на соответствие)*

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Другой аспект прозрачности - невозможность отказаться от совершенной подписи.

Даже без графологической экспертизы электронная подпись позволяет с точностью до секунды установить время совершения подписи и ее владельца.

На современном этапе развития общества в России в процессы повседневной деятельности всех отраслей общественной сферы активно внедряются новые высокопроизводительные информационно-телекоммуникационные технологии.

В этих условиях использование корпоративных, региональных и глобальных телекоммуникационных систем для обеспечения нормальной деятельности системы государственного управления и деловой жизни общества приобретает первостепенное значение.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Действующий Федеральный закон «Об электронной подписи» содержит 23 статьи:

Статья 1. Сфера действия настоящего Федерального закона.
Статья 2. Основные понятия, используемые в настоящем Федеральном законе.
Статья 3. Правовое регулирование отношений в области использования электронных подписей.
Статья 4. Принципы использования электронной подписи.
Статья 5. Виды электронных подписей.
Статья 6. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью.
Статья 7. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами.
Статья 8. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи.
Статья 9. Использование простой электронной подписи.
Статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей.
Статья 11. Признание квалифицированной электронной подписи.
Статья 12. Средства электронной подписи.
Статья 13. Удостоверяющий центр.
Статья 14. Сертификат ключа проверки электронной подписи.
Статья 15. Аккредитованный удостоверяющий центр.
Статья 16. Аккредитация удостоверяющего центра.
Статья 16.1. Федеральный государственный контроль (надзор) в сфере электронной подписи (с 11 июля 2021 г. 170-ФЗ)
Статья 17. Квалифицированный сертификат.
Статья 18. Выдача квалифицированного сертификата.
Статья 18.1. Доверенная третья сторона (с 8 июня 2020 г. N 166-ФЗ)
Статья 18.2. Аккредитация доверенной третьей стороны (с 8 июня 2020 г. N 166-ФЗ)
Статья 19. Заключительные положения.
Статья 20. Вступление в силу настоящего Федерального закона.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Федеральный закон расширяет сферу использования и допустимые виды ЭП.

Прежний закон разрешал применять только сертифицированные средства ЭЦП, а область ее использования ограничивалась гражданско-правовыми отношениями.

Правовое поле действия Федерального закона направлено, во-первых, на обеспечение **совершения гражданско-правовых сделок.**

Основы правового регулирования гражданско-правовых сделок регламентированы законодательством Российской Федерации, согласно которому сделками признаются действия граждан и юридических лиц, направленные на установление, изменение или прекращение гражданских прав и обязанностей.

Правовое поле Федерального закона «Об электронной подписи»

- Совершение гражданско-правовых сделок
- Оказание государственных и муниципальных услуг
- Исполнение государственных и муниципальных функций
- Совершение иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Предусмотрено, что использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронной подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, определенным законом, иными правовыми актами или соглашением сторон.

Так, например, в целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Сегодня ЭП широко применяется при совершении сделок и в таких сферах, как сдача отчетности в электронном виде, банковская сфера, электронные государственные закупки, электронный документооборот государственных (муниципальных) органов управления и др..

Во-вторых, положения Федерального закона «Об электронной подписи» применяются в случае оказания государственных и муниципальных услуг.

Такое использование ЭП регламентировано положениями федеральных законов, постановлений Правительства Российской Федерации и некоторыми др. актами.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Также положения Федерального закона «Об электронной подписи» применяются при исполнении государственных и муниципальных функций.

Эти функции исполняются с целью реализации полномочий федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, правовые основы которых регламентированы федеральными законами, а также в положениях (указах и т.п.) о конкретном федеральном органе государственной власти.

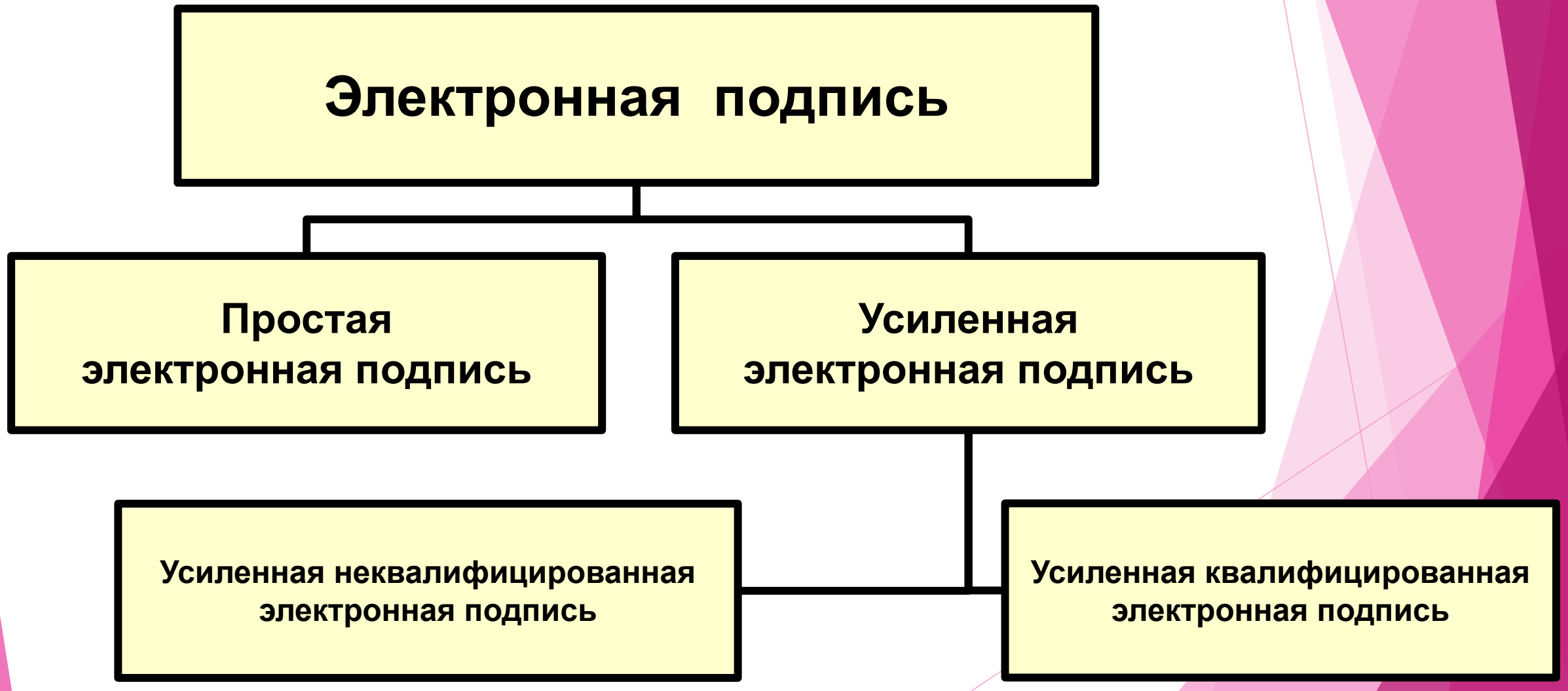
Исполнение государственных функций осуществляется в рамках соответствующих административных регламентов, при разработке которых органы власти предусматривают оптимизацию (повышение качества) исполнения государственных функций, в том числе посредством осуществления отдельных административных процедур (действий) в электронной форме.

В частности, при определении особенностей предоставления государственной услуги в электронной форме указывается перечень классов средств ЭП, которые допускаются к использованию при обращении за получением государственной услуги, оказываемой с применением усиленной квалифицированной ЭП.

Средства ЭП выбираются на основании утверждаемой конкретным ФОИВ по согласованию с ФСБ России МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ в информационной системе, используемой в целях приема обращений за получением государственной услуги и (или) предоставления такой услуги.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

В настоящее время Федеральный закон выделяет 2 вида ЭП: простая и усиленная (рис.2).



ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Суть электронной подписи:

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Применение электронной подписи

TAX COM

- Квалифицированная электронная подпись
- Выдана аккредитованным удостоверяющим центром
- Соответствие 63-ФЗ «Об электронной подписи»
- На любом носителе: Токен, Флеш-карта, реестр Windows
- Должна быть на руководителя организации
- Требуется ПО криптографической защиты (Крипто-Про)

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Кроме того, положения Федерального закона «Об электронной подписи» применяются при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Законодатель установил расширенный характер сферы применения норм комментируемого Закона, то есть, в любой деятельности, которая затрагивает права и интересы субъектов правоотношений, может применяться ЭП в соответствии с нормами данного Закона.

При этом соответствующими нормативными правовыми актами конкретизируется соответствующая область использования ЭП.

Так, например, электронный документ, подготовленный с использованием ГАС «Выборы», приобретает юридическую силу после его подписания электронными подписями соответствующих должностных лиц.

Трудовым законодательством установлено, что если предусмотрено взаимодействие дистанционного работника или лица, поступающего на дистанционную работу, и работодателя путем обмена электронными документами, то используются усиленные квалифицированные электронные подписи дистанционного работника или лица, поступающего на дистанционную работу, и работодателя в порядке, установленном федеральными законами и иными нормативными правовыми актами Российской Федерации.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Каждая из сторон указанного обмена обязана направлять в форме электронного документа подтверждение получения электронного документа от другой стороны в срок, определенный трудовым договором о дистанционной работе.

В таких правовых условиях Руководство является средством официального информирования лиц, владеющих квалифицированной ЭП:

— об условиях,

— рисках,

— порядке использования квалифицированной ЭП и средств ЭП,

— о мерах, необходимых для обеспечения безопасности при использовании квалифицированной ЭП.

Кроме того, при использовании квалифицированной ЭП в ИС владельцу сертификата необходимо выполнять требования следующих документов уполномоченных ФОИВ:

1. **Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, (утверждена приказом ФАПСИ от 13 июня 2001 г. N 152).**

   В Инструкции определяется единый порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством РФ обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

2. **Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) (утверждено приказом ФСБ России от 9 февраля 2005 г. N 66).**

   Использование СКЗИ и ЭЦП обеспечивает:

   — сохранение конфиденциальности переписки;
   — однозначность идентификации компании, приславшей отчетность;
   — защиту файлов от несанкционированных исправлений.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

- I. Общие положения
- II. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации
- III. Порядок обращения с СКЗИ и криптоключами к ним. Мероприятия при компрометации криптоключей
- IV. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним
- V. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Инструкция
об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

Данным порядком рекомендуется руководствоваться также при организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ (в настоящее время — ФСБ России) средств криптографической защиты не подлежащей обязательной защите конфиденциальной информации, доступ к которой ограничивается в соответствии с законодательством Российской Федерации или по решению обладателя конфиденциальной информации (за исключением информации, содержащей сведения, к которым в соответствии с законодательством Российской Федерации не может быть ограничен доступ).

Обладателями конфиденциальной информации могут быть государственные органы, государственные организации и другие организации независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Сертифицированные средства криптографической защиты конфиденциальной информации:

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении;

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи";

- аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в **сетях конфиденциальной связи** организуют и обеспечивают **операторы конфиденциальной связи**.

Сети конфиденциальной связи - сети связи, предназначенные для передачи конфиденциальной информации.

Операторы конфиденциальной связи - операторы связи, предоставляющие на основании **лицензии ФСБ России** услуги конфиденциальной связи с использованием СКЗИ.

Безопасность хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи, организуют и обеспечивают лица, имеющие **лицензию ФСБ России**.

Операторы конфиденциальной связи и лица, имеющие **лицензию ФСБ России** и не являющиеся операторами конфиденциальной связи, в настоящей Инструкции именуются **лицензиаты ФСБ России**.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Лица, оказывающие возмездные услуги по организации и обеспечению безопасности хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи, должны иметь лицензию ФСБ России на деятельность по предоставлению услуг в области шифрования информации.

Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, обладатели которой не имеют лицензий ФСБ России, лицензиаты ФСБ России организуют и обеспечивают:

— либо по указанию вышестоящей организации,

— либо на основании договоров на оказание услуг по криптографической защите конфиденциальной информации.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Лицензиаты ФСБ России несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

— лицензионным требованиям и условиям,

— эксплуатационной и технической документации к СКЗИ,

— а также положениям данной Инструкции.

При этом лицензиаты ФСБ России должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации лицензиат ФСБ России создает один или несколько органов криптографической защиты, о чем письменно уведомляет ФСБ России.

Органом криптографической защиты может быть организация, структурное подразделение организации - лицензиата ФСБ России, обладателя конфиденциальной информации.

Функции органа криптографической защиты могут быть возложены на физическое лицо.

Допускается возложение функций органа криптографической защиты на специальное структурное подразделение по защите государственной тайны, использующее для этого шифровальные средства.

Количество органов криптографической защиты и их численность устанавливает лицензиат ФСБ России.

ОРГАН КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ОСУЩЕСТВЛЯЕТ:

1) проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием:

— типа и номеров используемых СКЗИ,

— номеров аппаратных, программных и аппаратно-программных средств,

— где установлены или к которым подключены СКЗИ,

— с указанием также номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ,

— результатов проверки функционирования СКЗИ);

ОРГАН КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ОСУЩЕСТВЛЯЕТ:

2) разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

3) обучение лиц, использующих СКЗИ, правилам работы с ними;

4) поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

5) учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ (т.е. пользователи СКЗИ);

ОРГАН КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ОСУЩЕСТВЛЯЕТ:

6) подачу заявок в ФАПСИ или лицензиату, имеющему лицензию ФСБ России на деятельность по изготовлению ключевых документов для СКЗИ, на изготовление ключевых документов или исходной ключевой информации;

- КЛЮЧЕВОЙ ДОКУМЕНТ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию;

- ИСХОДНАЯ КЛЮЧЕВАЯ ИНФОРМАЦИЯ - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

7) Изготовление из исходной ключевой информации ключевых документов, их распределение, рассылку и учет;

ОРГАН КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ОСУЩЕСТВЛЯЕТ:

8) контроль за соблюдением условий использования СКЗИ, установленных:

— эксплуатационной и технической документацией к СКЗИ,

— сертификатом ФСБ России,

— Инструкцией ФСБ России;

9) расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации;

10) разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

ОРГАН КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ОСУЩЕСТВЛЯЕТ:

11) разработку схемы организации криптографической защиты конфиденциальной информации (с указанием:

— наименования и размещения нижестоящих органов криптографической защиты, если таковые имеются,

— обладателей конфиденциальной информации,

— реквизитов договоров на оказание услуг по криптографической защите конфиденциальной информации,

а также с указанием:

— типов применяемых СКЗИ и ключевых документов к ним,

— видов защищаемой информации,

— используемых совместно с СКЗИ технических средств связи,

— прикладного и общесистемного программного обеспечения,

— средств вычислительной техники).

Указанную схему утверждает лицензиат ФСБ России.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

К выполнению обязанностей сотрудников органов криптографической защиты лицензиатами ФСБ России допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ.

Лиц, оформляемых на работу в органы криптографической защиты, следует ознакомить с Инструкцией № 152-2001 под расписку.

Обязанности, возлагаемые на сотрудников органа криптографической защиты, могут выполняться штатными сотрудниками или сотрудниками других структурных подразделений, привлекаемыми к такой работе по совместительству.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

При определении обязанностей сотрудников органов криптографической защиты лицензиаты ФСБ России должны учитывать, что безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации обеспечивается:

1) соблюдением сотрудниками органов криптографической защиты режима конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;

2) точным выполнением сотрудниками органов криптографической защиты требований к обеспечению безопасности конфиденциальной информации;

3) надежным хранением сотрудниками органов криптографической защиты СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации;

При определении обязанностей сотрудников органов криптографической защиты лицензиаты ФСБ России должны учитывать, что безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации обеспечивается:

4) своевременным выявлением сотрудниками органов криптографической защиты попыток посторонних лиц получить сведения

— о защищаемой конфиденциальной информации,

— об используемых СКЗИ

— или ключевых документах к ним;

При определении обязанностей сотрудников органов криптографической защиты лицензиаты ФСБ России должны учитывать, что безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации обеспечивается:

5) немедленным принятием сотрудниками органов криптографической защиты мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Обучение и повышение квалификации сотрудников органов криптографической защиты осуществляют организации, имеющие лицензию на ведение образовательной деятельности по соответствующим программам.

Сотрудники органа криптографической защиты должны иметь разработанные в соответствии с настоящей Инструкцией и утвержденные лицензиатом ФСБ России функциональные обязанности.

Объем и порядок ознакомления сотрудников органов криптографической защиты с конфиденциальной информацией определяется обладателем конфиденциальной информации.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Обязанности между сотрудниками органа криптографической защиты должны быть распределены с учетом персональной ответственности за сохранность:

— СКЗИ,

— ключевой документации и документов,

— за порученные участки работы.

Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации.

До такого утверждения техническая возможность использования СКЗИ лицами, включенными в данный перечень, должна быть согласована с лицензиатом ФСБ России.

Лицензиаты ФСБ России в рамках согласованных с обладателями конфиденциальной информации полномочий по доступу к конфиденциальной информации имеют право утверждать такой перечень в отношении подчиненных им должностных лиц.

Пользователи СКЗИ обязаны:

1) **не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;**

2) **соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;**

3) **сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;**

4) **сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным Инструкцией № 152-2001, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;**

5) **немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.**

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты.

Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

Обладатели конфиденциальной информации,

— если они приняли решение о необходимости криптографической защиты такой информации или

— если решение о необходимости ее криптографической защиты в соответствии с Положением ПКЗ-2005 принято государственными органами или государственными организациями,

ОБЯЗАНЫ выполнять указания соответствующих органов криптографической защиты **по всем вопросам** организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Для организации взаимодействия обладателей конфиденциальной информации,

безопасность хранения, обработки и передачи по каналам связи которой с использованием СКЗИ организуют и обеспечивают различные лицензиаты ФСБ России,

из созданных этими лицензиатами ФСБ России органов криптографической защиты выделяется КООРДИНИРУЮЩИЙ орган криптографической защиты.

Все органы криптографической защиты, образованные этими лицензиатами ФСБ России, обязаны выполнять указания КООРДИНИРУЮЩЕГО органа криптографической защиты по обеспечению такого взаимодействия.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Инструкции, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи защищаемой с использованием СКЗИ конфиденциальной информации, **должны согласовываться с лицензиатом ФСБ России** .

Такие **Инструкции** подготавливаются согласно эксплуатационной и технической документации на соответствующие сети связи, автоматизированные и информационные системы, в которых передается, обрабатывается или хранится конфиденциальная информация, с учетом используемых СКЗИ и положений Инструкции ФАПСИ (№ 152-2001).

Лицензиаты ФСБ России с учетом особенностей своей деятельности могут разрабатывать **методические рекомендации** по применению Инструкции № 152-2001, не противоречащие ее требованиям.

Кроме того, при использовании квалифицированной ЭП в ИС владельцу сертификата необходимо выполнять требования следующих документов уполномоченных ФОИВ:

1. ***Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну*, *(утверждена приказом ФАПСИ от 13 июня 2001 г. N 152).***

   В Инструкции определяется единый порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

2. **Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) (утверждено приказом ФСБ России от 9 февраля 2005 г. N 66).**

Использование СКЗИ и ЭЦП обеспечивает:

— сохранение конфиденциальности переписки;

— однозначность идентификации компании, приславшей отчетность;

— защиту файлов от несанкционированных исправлений.

2. Положение ПКЗ-2005.

Разработано в целях определения порядка разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений составляющих государственную тайну.

Государственная тайна - защищаемые государством сведения в области его

— военной,
— внешнеполитической,
— экономической,
— разведывательной,
— контрразведывательной
— оперативно-розыскной

деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

К шифровальным (криптографическим) средствам (**средствам криптографической защиты информации**), включая документацию на эти средства, относятся средства указанные на рисунке.

ПКЗ-2005 не регулирует отношения, связанные с экспортом и импортом СКЗИ, и не распространяется на использование шифровальных (криптографических) средств иностранного производства.

Режим защиты информации путем использования СКЗИ устанавливается

— обладателем информации конфиденциального характера,

— собственником (владельцем) информационных ресурсов (информационных систем)

— или уполномоченными ими лицами на основании законодательства Российской Федерации.

При организации обмена информацией конфиденциального характера, участниками которого являются государственные органы и организации, выполняющие государственные заказы, необходимость криптографической защиты информации и выбор применяемых СКЗИ определяются государственными органами или организациями, выполняющими государственные заказы.

При организации обмена информацией, доступ к которой ограничивается по решению:

— обладателя,

— пользователя (потребителя) данной информации,

— собственника (владельца) информационных ресурсов (информационных систем),

не являющихся организациями, выполняющими государственные заказы,

или уполномоченными ими лицами (за исключением информации, содержащей сведения, к которым в соответствии с законодательством Российской Федерации не может быть ограничен доступ),

необходимость ее криптографической защиты и выбор применяемых СКЗИ определяются соглашениями между участниками обмена.

Необходимость криптографической защиты информации конфиденциального характера при ее обработке и хранении без передачи по каналам связи, а также **выбор** применяемых **СКЗИ** определяются

— обладателем

— или пользователем (потребителем) данной информации.

СКЗИ должны удовлетворять требованиям технических регламентов, оценка выполнения которых осуществляется в порядке, определяемом Федеральным законом от 27 декабря 2002 года N 184-ФЗ "О техническом регулировании".

Качество криптографической защиты информации конфиденциального характера, осуществляемой СКЗИ, **обеспечивается реализацией требований** по безопасности информации, предъявляемых к:

— СКЗИ,

— ключевой системе СКЗИ,

— а также к сетям связи (системам), используемым СКЗИ с целью защиты информации при ее передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении (далее - сети (системы) конфиденциальной связи)

— и условиям размещения СКЗИ при их использовании (далее - **требования по безопасности информации**).

Для криптографической защиты информации конфиденциального характера должны использоваться СКЗИ, удовлетворяющие требованиям по безопасности информации, устанавливаемым в соответствии с законодательством Российской Федерации.

Реализация в конкретных образцах СКЗИ и сетях (системах) конфиденциальной связи требований по безопасности информации возлагается на разработчика СКЗИ.

ВОПРОС 1.
Правовые основания разработки Руководства по обеспечению безопасности использования ЭП и средств ЭП

Также к правовым основаниям разработки Руководства по обеспечению безопасности использования электронной подписи и средств ЭП следует отнести эксплуатационная документация для средств электронной подписи.

На основании выше перечисленных документов можно разработать комплект организационно-технических и административных мер по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Лекция № 16-2022.
Организационное обеспечение информационной безопасности использования средств электронной подписи

ВОПРОС 1. Правовые основания разработки Руководства по обеспечению безопасности использования электронной подписи и средств ЭП

ВОПРОС 2. Требования по размещению средств квалифицированной электронной подписи

ВОПРОС 3. Требования по инсталяции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

ВОПРОС 4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации

ВОПРОС 2.

Требования по размещению средств квалифицированной электронной подписи

ВОПРОС 2. Требования по размещению средств квалифицированной электронной подписи

Технические средства квалифицированной электронной подписи должны быть установлены в изолированном помещении.

При размещении средств вычислительной техники с установленными на них средствами квалифицированной электронной подписи должны быть выполнены следующие условия:

А) Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать уполномоченным исполнителям работ сохранность доверенных им конфиденциальных документов и сведений;

Б) Должен быть исключен доступ посторонних лиц к носителям ключевой информации и СКЗИ;

В) Приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в этих помещениях.

ВОПРОС 2. Требования по размещению средств квалифицированной электронной подписи

В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен КОНТРОЛЬ за их действиями во избежание несанкционированных воздействий с их стороны на:

— ключевую информацию,

— средства криптографической защиты,

— средства электронной подписи,

— передаваемую информацию.

Лекция № 16-2022.
Организационное обеспечение информационной безопасности использования средств электронной подписи

ВОПРОС 1. Правовые основания разработки Руководства по обеспечению безопасности использования электронной подписи и средств ЭП

ВОПРОС 2. Требования по размещению средств квалифицированной электронной подписи

ВОПРОС 3. Требования по инсталляции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

ВОПРОС 4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации

ВОПРОС 3.

Требования по инсталляции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

ВОПРОС 3. Требования по инсталляции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

А) Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей.

Правила назначения и смены паролей должны удовлетворять следующим требованиям:

- длина пароля должна быть не менее 6 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права никому сообщать;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

ВОПРОС 3. Требования по инсталляции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

Б) При использовании ключей ЭП средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- на средствах вычислительной техники с установленными средствами квалифицированной ЭП должна быть установлена только одна операционная система;
- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;
- не использовать нестандартные, измененные или отладочные версии операционных систем;
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;
- необходимо предусмотреть меры, максимально ограничивающие доступ к:
    - системному реестру;
    - файлам и каталогам;
    - временным файлам;
    - журналам системы;
    - файлам подкачки;
    - кэшируемой информации (пароли и т.п.);
    - отладочной информации.

Б) При использовании ключей ЭП средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

Кроме того, на средствах вычислительной техники необходимо:

- **организовать удаление (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;**
- **исключить попадание в систему программ, позволяющих использовать ошибки ОС, для повышения предоставленных привилегий;**
- **регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.);**
- **регулярно обновлять антивирусные базы.**

ВОПРОС 3. Требования по инсталляции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

В) В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

Г) Необходимо организовать и использовать:

- **систему аудита;**
- **обеспечить регулярный анализ результатов аудита;**
- **реализовать комплекс мероприятий по антивирусной защите.**

ВОПРОС 3. Требования по инсталляции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

ЗАПРЕЩАЕТСЯ:

- осуществлять копирование ключевых носителей;
- записывать на ключевые носители постороннюю информацию;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;
- вносить какие-либо изменения в программное обеспечение средств квалифицированной ЭП;
- оставлять средства вычислительной техники с установленными средствами квалифицированной ЭП без контроля после ввода ключевой информации;
- использовать ключ ЭП и соответствующий сертификат ключа проверки ЭП, Заявление на изменение статуса которого подано в вышестоящий территориальный орган, в течение времени, исчисляемого с момента подачи Заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса;
- использовать ключ ЭП, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;
- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки ЭП.

Лекция № 16-2022.
Организационное обеспечение информационной безопасности использования средств электронной подписи

ВОПРОС 1. Правовые основания разработки Руководства по обеспечению безопасности использования электронной подписи и средств ЭП

ВОПРОС 2. Требования по размещению средств квалифицированной электронной подписи

ВОПРОС 3. Требования по инсталляции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

ВОПРОС 4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации

ВОПРОС 4.

Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации

ВОПРОС 4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации

1. Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной ЭП при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной ЭП согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером, присвоенным Заявителем.

Ключи квалифицированной ЭП на ключевом носителе могут быть защищены паролем (ПИН-кодом).

Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной ЭП.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети «Интернет» или по внутренней электронной почте (кроме открытых ключей).

Не допускается размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, так как это способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

2. Обращение с ключевой информацией и ключевыми носителями.

…

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций

— формирования и проверки квалифицированной электронной подписи,

— шифрования,

— дешифрования.

Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами квалифицированной ЭП должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования.

Технические средства, используемые для работы в информационных системах, должны удовлетворять следующим требованиям:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие ранее рассмотренным требованиям;
- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;

3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи

…

Технические средства, используемые для работы в информационных системах, должны удовлетворять следующим требованиям:

…

- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

- должны регулярно устанавливаться обновления операционной системы;

3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи

Технические средства, используемые для работы в информационных системах, должны удовлетворять следующим требованиям:

…

- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;

- должна быть активирована регистрация событий информационной безопасности;

- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В случае передачи (списания, сдачи в ремонт) посторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств).

Использование такой информации третьими лицами может потенциально нанести вред организации.

Лекция № 16-2022.
Организационное обеспечение информационной безопасности использования средств электронной подписи

ВОПРОС 1. Правовые основания разработки Руководства по обеспечению безопасности использования электронной подписи и средств ЭП

ВОПРОС 2. Требования по размещению средств квалифицированной электронной подписи

ВОПРОС 3. Требования по инсталляции средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

ВОПРОС 4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации

14.12.2022 г. **Лекция № 16-2022.**

Организационное обеспечение информационной безопасности использования средств электронной подписи

СПАСИБО ЗА ВНИМАНИЕ