Темы для подготовки к экзамену

1. Общество. Государство и право. Основные понятия в области информационного права. Термины и определения.

**Общество (в широком смысле)** — совокупность исторически сложившихся форм совместной деятельности людей, направленных на лучшее удовлетворение общих потребностей и интересов.

Основными элементами общества выступают отдельные индивидуумы и их коллективные объединения:

1) семья
2) юридическое лицо
3) государство и его органы
4) органы местного самоуправления
5) общественные объединения и политические партии

**Государство** – это публично-правовая и суверенная организация власти, которая обеспечивает общие интересы населения и является гарантом прав и свобод человека и гражданина. Одним из признаков государства является право. Без права нельзя управлять государством.

**Право** - особый регулятор общественных отношений в форме совокупности общеобязательных правил и норм поведения, устанавливаемых государством для регулирования наиболее важных общественных отношений.

**Информационное право** — система охраняемых государством социальных норм и отношений, возникающих в информационной сфере. Правовое определение основных понятий осуществляется в нормах Федерального **закона No149** «Об информации, информационных технологиях и о защите информации»

**Информация** — сведения (сообщения, данные) независимо от формы их представления;

**Обладатель информации** — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

**Доступ к информации** — возможность получения информации и ее использования;

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

**Информационные технологии** — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

**Информационная система** — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

**Информационно-телекоммуникационная сеть** — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

2. Методы правовой защиты информации. Законодательство в области информационного права.

**Правовая защита информации** – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Законодательство в области информационного права:

Конституция РФ от 12.12.1993 (с изменениями от 01.07.2020)

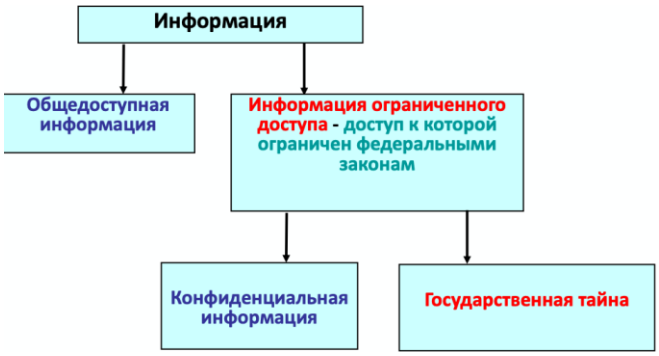
Гражданский кодекс РФ 21.10.1994
Закон «Об информации, информационных технологиях и о защите информации» 2006 г.
ФЗ «О коммерческой тайне» 29 июля 2004 г. N 98-ФЗ
ФЗ «О связи» 07.07.2003 N 126-ФЗ
ФЗ «О ЭЦП» 10.01.2002 N 1-ФЗ
ФЗ «О СМИ» 27.12.1991 N 2124-1
ФЗ «Государственной тайне» 21.07.1993 г. N 5485-I


## 3. Методы правовой защиты информации. Концепция и доктрина информационной безопасности России.

Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере. Доктрина ИБ РФ утверждена Указом Президента РФ от 05 12 2016 **No646.**

В настоящей Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, систем, сайтов в сети "Интернет", сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением ИБ, а также совокупность механизмов регулирования общественных отношений.

## 4. Правовые основы защиты государственной тайны. Законодательство в области защиты государственной тайны.




В соответствии с ФЗ от 20.02.95 г. **No 24-ФЗ** «Об информации, информатизации и защите информации» вся информация делится на открытую и с ограниченным доступом.

Закон РФ от 21.07.1993 **No 5485-1** "О государственной тайне":

**Государственная тайна** – это защищаемые государством сведения, распространение которых может нанести ущерб безопасности РФ.

Государственную тайну на основании ст. 5 Закона РФ "О государственной тайне" составляют:

- сведения в военной области;
- в экономики, науки и техники, в вопросах обороноспособности и безопасности;
- сведения в области финансовой, денежно-кредитной, внешней политики и экономики.
- сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятель

Государство в отношении сведений, составляющих государственную тайну, имеет право:

**1**. Устанавливать степень секретности информации и гриф секретности носителей этих сведений в соответствии со степенью тяжести возможного ущерба в случае их распространения:

- особой важности (ОВ) – ущерб интересам РФ;

• совершенно секретно (СС) – ущерб интересам министерства, отрасли;
• секретно (С) – ущерб интересам предприятия, учреждения или организации.
**2.** Рассекречивать сведения, составляющие государственную тайну.
**3.** Разрешать и прекращать допуск граждан, должностных лиц, предприятий, организаций
**4.** Разрешать доступ лиц, имеющих допуск к гос. тайне.
**5.** Ограничивать право собственности рос. предприятий на информацию.
**6.** Распоряжаться сведениями, составляющими гос. тайну (передавать).
**7.** Требовать соблюдения законодательства о государственной тайне.
**8.** Требовать обязательной сертификации средств защиты информации.
**9.** Требовать привлечения к ответственности лиц, виновных в нарушении законодательства о государственной тайне.

5. Содержание понятия конфиденциальная информация. Служебная, профессиональная и другие тайны. Положения «Гражданского кодекса РФ» по обеспечению защиты всех видов тайн.

**Конфиденциальная информация** - это документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ.

**Основные понятия из ФЗ «Об информации, информационных технологиях и о защите информации» (27 июля 2006 N 149-ФЗ):**

- **Информация**: сведения независимо от формы их представления.
- **Обладатель информации**: лицо, самостоятельно создавшее информацию или получившее право на ее использование.
- **Конфиденциальность информации:** обязательное требование не передавать информацию третьим лицам без согласия обладателя.

**Защита информации** включает правовые, организационные и технические меры для:

- Обеспечения защиты информации от неправомерных действий.
- Соблюдения конфиденциальности информации ограниченного доступа.
- Реализации права на доступ к информации.

**Перечень сведений конфиденциального характера**:

1. **Персональные данные**: информация о частной жизни гражданина, позволяющая его идентифицировать.
2. **Тайна следствия и судопроизводства**.
3. **Служебная тайна**: информация, доступ к которой ограничен органами государственной власти.
4. **Профессиональная тайна**: информация, доступ к которой ограничен в соответствии с законами (врачебная, нотариальная, адвокатская тайна и т.д.).
5. **Коммерческая тайна**: информация, доступ к которой ограничен для защиты коммерческих интересов.
6. **Сведения о сущности изобретения** до официальной публикации.

**Виды тайн**:

- **Профессиональная тайна**: информация, полученная при исполнении профессиональных обязанностей (врачебная, нотариальная, адвокатская тайна и т.д.).
- **Служебная тайна**: информация, ставшая известной в государственных органах и органах местного самоуправления.
- **Коммерческая тайна**: информация, позволяющая получить коммерческую выгоду.

**Положения Гражданского кодекса РФ** обеспечивают защиту всех видов тайн и устанавливают ответственность за их разглашение.

**(Статья 434.1 (часть первая), Статья 65.2 (часть первая), Статья 857 (часть вторая), Статья 946 (часть вторая), Статья 1123 Гражданского кодекса РФ (часть третья).**

6. Понятие персональных данных. Основные положения ФЗ о персональных данных. Подзаконные акты, регламентирующие выполнения Федерального закона.

ФЗ от 27.07.2006 **No152-ФЗ** «О персональных данных»

**ПЕРСОНАЛЬНЫЕ ДАННЫЕ** — любая информация, относящаяся к определенному или определяемому физическому лицу.

**1. Персональные данные 1 категории (специальные ПД).**

1.1. Сведения о состоянии здоровья и интимной жизни, о расовой и национальной принадлежности, политических взглядах, религиозных или философских убеждениях.

**2. Персональные данные 2 категории (биометрические ПД).**

Данные, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1:

2.1. Сведения о биометрических ПД, о физиологические особенности, кроме 1 категории.

**3. Персональные данные 3 категории (общие ПД).**

Персональные данные, позволяющие идентифицировать субъекта персональных данных:

3.1. ФИО, год, месяц, дата и место рождения, паспортные данные.

3.2. Номер, серия страхового свидетельства государственного пенсионного страхования.

3.3. Сведения из страховых полисов обязательного (добровольного) мед. страхования.

3.4. Сведения о воинском учете.

**4. Персональные данные 4 категории (общедоступные ПД).**

Обезличенные и общедоступные персональные данные:

4.1. Сведения о семейном положении.

4.2. Данные о трудовой деятельности.

4.3. Сведения об образовании, квалификации, о наличии специальных знани.

4.4. Сведения об имуществе.


Обработка персональных данных должна осуществляться на основе принципов:

1)законности целей и способов обработки ПД и добросовестности;

2)соответствия целей обработки ПД целям, заранее заявленным при сборе ПД.

3)соответствия объема и характера обрабатываемых ПД, способов обработки персональных данных целям обработки персональных данных;

4)достоверности персональных данных.

5)недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Подзаконные акты, регламентирующие выполнения Федерального закона.

1) **Постановление Правительства РФ № 687 от 15.09.2008** — устанавливает порядок обработки персональных данных без использования средств автоматизации.

2) **ФСТЭК России № 21 от 18.02.2013** — определяет требования к защите персональных данных при их обработке в информационных системах персональных данных.

3) **Приказ Роскомнадзора № 996 от 14.12.2015** — утверждает порядок уведомления об обработке персональных данных и ведения реестра операторов.

7. Правовые основы допуска к информации ограниченного доступа. Положения Конституции РФ о защите информации ограниченного доступа.

Основные положения ФЗ от 27.07.2006 **No 149-ФЗ** «Об информации, информационных технологиях и о защите информации»

Регулирует отношения, возникающие при:

1) осуществлении права на поиск, передачу, производство информации;
2) применении информационных технологий;
3) обеспечении защиты информации.
Основные ПРИНЦИПЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ отношений в сфере информации:
- установление ограничений доступа к информации только ФЗ;
- обеспечение безопасности РФ при создании информационных систем, их эксплуатации;
- достоверность информации и своевременность ее предоставления;
**Обязанности обладателя информации, оператора информационной системы (ст.16.4):**
- предотвращение несанкционированного доступа к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации;
- возможность незамедлительного восстановления информации;
- постоянный контроль за обеспечением уровня защищенности информации.
- Обязательность соблюдения конфиденциальности информации;
- Обязательность ввода государственной информационной системы в эксплуатацию в порядке, установленном заказчиком (ст. 14.5);
- Методы и способы защиты информации гос. систем систем должны соответствовать требованиям, установленным ФОИВ, уполномоченным в области ПДТР и ТЗИ (ст.16.5)
- Установленные ФЗ от 27.07.2006 N 149- ФЗ требования к государственным информационным системам, распространяются на муниципальные системы.

**КОНСТИТУЦИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Статья 23**

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну.
2. Каждый имеет право на тайну переписки, телефонных переговоров, сообщений.

**Статья 24**

1. Сбор, хранение, использование инф. частной жизни лица без согласия не допускаются.
2. Органы гос. власти и органы местного самоуправления обязаны обеспечить каждому ознакомление с материалами, непосредственно затрагивающими его права и свободы.

**Статья 29**

4. Каждый имеет право свободно искать, производить и распространять информацию.
5. Гарантируется свобода массовой информации. Цензура запрещается.

8. Правовые основы допуска к информации ограниченного доступа. Законы РФ. Постановления Правительства РФ об утверждение Инструкции о порядке допуска к информации, составляющей государственную тайну.

**Постановление Правительства РФ от 6 февраля 2010 г. N 63**

Инструкция, разработанная в соответствии с законодательством РФ о гос. тайне, определяет порядок допуска должностных лиц и граждан РФ к гос. тайне и формы учетной документации, необходимой для оформления такого допуска.
Устанавливаются следующие формы допуска граждан к гос. тайне:
• **первая форма** - для граждан, допускаемых к сведениям особой важности;
• **вторая форма** - к совершенно секретным сведениям;
• **третья форма** - к секретным сведениям.
Каждая последующая форма даёт доступ к сведениям более низкой степени.
Допуск граждан к государственной тайне предусматривает:
а) принятие на себя обязательств перед государством по нераспространению.
б) письменное согласие на частичные, временные ограничения их прав в соответствии.
в) письменное согласие на проведение в отношении их органами проверок;
г) определение видов, размеров и порядка предоставления социальных гарантий

д) ознакомление с нормами, предусматривающими ответственность за его нарушение;
е) принятие руководителем организации решения о допуске оформляемого гражданина к сведениям, составляющим государственную тайну.
У форма – без проверочных мероприятий. В случае руководитель организации может направить материалы в орган безопасности для проведения проверочных мероприятий.

9. Система правовой ответственности за утечку информации или утрату носителей. Основные положения Уголовного кодекса РФ.

**Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 01.04.2019)**

ОСНОВНЫЕ НАКАЗУЕМЫЕ ДЕЯНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

- **Ст. 138:** нарушение тайны переписки, телефонных переговоров, сообщений.
- **Ст. 138.1:** Незаконный оборот спец. тех. средств для негласного получения информации.
- **Ст. 183:** незаконное получение и разглашение сведений, коммерч., налог., банк. тайну

Глава 28. Преступления в сфере компьютерной информации

- **Ст. 272:** неправомерный доступ к компьютерной информации
- **Ст. 273:** создание, использование и распространение вредоносных программ
- **Ст. 274:** нарушение правил эксплуатации ЭВМ, системы или их сети
- **Ст. 274.1:** Неправомерное воздействие на критическую инф. инфраструктуру
- **Статья 276.** Шпионаж
- **Статья 283.** Разглашение гос. тайны
- **Статья 283.1**. Незаконное получение сведений, составляющих гос. тайну
- **Статья 284.** Утрата документов, содержащих гос. тайну

**Нормы о преступлениях зафиксированы в 28 главе УК РФ:**

**— ст. 272 (Неправомерный доступ к компьютерной информации),**

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло уничтожение, блокирование, модификацию, копирование информации, - наказывается штрафом в 200 000 рублей или в размере заработной платы за период до 18 месяцев, исправительными работами до года, лишением свободы на срок до 2 лет.
2. … причинившее крупный ущерб или совершенное из корыстной заинтересованности, - штраф от 100 до 300 000 или в зарплаты/дохода за период от 1 до 2 лет, исправительными работами на срок от 1 до 2 лет, либо лишением свободы до 4 лет.
3. Деяния, 1 или 2 статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения – 500 р, до 3 лет
4. Деяния, 1 или 2 статьи, 2 или 3 настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - лишение свободы на срок до 7 лет.

**— ст. 273 (Создание, использование и распространение вредоносных программ для ЭВМ)**

**— ст. 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно- телекоммуникационных сетей)**

**— ст. 274 (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации)**

10. Система правовой ответственности за утечку информации или утрату носителей. Основные положения Кодекса РФ об административных правонарушениях в области защиты информации.

**КОДЕКС Российской Федерации об административных правонарушениях от 30.12.2001 No195-ФЗ**

**Глава 13. Административные правонарушения в области связи и информации**

**Статья 13.11.** Нарушение законодательства Российской Федерации в области персональных данных

**Статья 13.12.** Нарушение правил защиты информации
п. 2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на должностных лиц – от 10 до 20 МРОТ, на юридических лиц – от 100 до 200 МРОТ.
п. 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц – от 30 до 40 МРОТ, на юридических лиц – от 200 до 300 МРОТ.
**Статья 13.13**. Незаконная деятельность в области защиты информации
**Статья 13.14.** Разглашение информации с ограниченным доступом

## 11. Правовые основы деятельности служб в области обеспечения информационной безопасности. Федеральные законы, регламентирующие действие специальных служб в области обеспечения информационной безопасности (ФСБ РФ, ФСТЭК РФ, СВР РФ и др.)

Основными нормативно-правовыми актами, регламентирующими деятельность таких специальных служб, как ФСБ, ФСТЭК и СВР, являются:

1. **ФЗ № 40-ФЗ от 3 апреля 1995 года "О федеральной службе безопасности"**:
    - Регулирует деятельность ФСБ РФ.
    - Определяет задачи ФСБ по обеспечению гос. безопасности(инф. безоп.)
    - Устанавливает полномочия ФСБ в области контрразведки, борьбы с терроризмом, защиты государственной тайны и др.
2. **Фз № 126-ФЗ от 7 июля 2003 года "О связи"**:
    - Регулирует отношения в связи и устанавливает требования к операторам
3. **ФЗ № 149-ФЗ от 27 июля 2006 года "Об информации, информационных технологиях и о защите информации"**:
    - Определяет общие принципы регулирования инф. тех. и защиты информации и устанавливает правила защиты информации.
4. **ФЗ № 187-ФЗ от 26 июля 2017 года "О безопасности критической информационной инфраструктуры Российской Федерации"**:
    - Регулирует правовые основы обеспечения безопасности критической инфраструктуры и обязанности и ответственность их операторов.
5. **ФЗ № 98-ФЗ от 29 июля 2004 года "О коммерческой тайне"**:
    - Устанавливает правовые основы защиты конфиденциальной информации,
    - Определяет обязанности организаций по защите коммерческой тайны.
6. **ФЗ № 294-ФЗ от 26 декабря 2008 года "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля"**:
    - Регулирует порядок проведения проверок и контроля в области ИБ.
7. **ФЗ № 432-ФЗ от 28 декабря 2010 года "О Службе внешней разведки Российской Федерации"**:
    - Определяет задачи и полномочия СВР РФ, включает положения о защите гос. тайны и ИБ в рамках деятельности СВР.

## 12. Законодательство в области защиты информации. Техническое регулирование в области защиты информации.

Законодательство в области защиты информации - набор нормативных актов и правовых положений, направленных на обеспечение конфиденциальности, целостности и доступности информации

Примеры законодательства в этой области могут включать:

1. **Закон о защите персональных данных:** регулирует сбор, хранение и использование ПД граждан.
2. **Закон о коммерческой тайне:** устанавливает правовой режим для информации, составляющей коммерческую тайну, и меры за её незаконное использование.
3. **Закон о государственной тайне:** регулирует обращение с информацией, составляющей государственную тайну, и меры за её неправомерное раскрытие.

Техническое регулирование в области защиты информации охватывает стандарты, методы и технологии, используемые для обеспечения безопасности информации.
Примеры технического регулирования:

1. **Стандарты защиты информации:** ISO/IEC 27001, устанавливающий требования к системам управления информационной безопасностью.
2. **Криптографические стандарты:** AES (Advanced Encryption Standard) для защиты данных путём их шифрования.
3. **Технические меры защиты данных:** меры по защите сетей, систем и приложений, (брандмауэры, антивирусы, многофакторная аутентификация)

## 13. Законодательство в области защиты информации. Решение вопросов лицензирования деятельности и сертификации средств защиты информации. Нормативная база.

Разработка и производство крипто-средств, защищенных с использованием этих же средств информационных систем регламентируется ФСБ России.
С этой целью разработан и утвержден **Административный регламент ФСБ РФ по исполнению гос. функции по лицензированию** производства криптографических средств.

**Приказ ФСБ РФ от 30 августа 2012 г. N 440** "Об утверждении Административного регламента ФСБ РФ по предоставлению гос. услуги по осуществлению лицензирования деятельности по разработке, производству, распространению криптографических средств)
**Постановление Правительства Российской Федерации от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (с изменениями от 23 апреля 1996 г., 29 марта 1999 г., 17 декабря 2004 г., 21 апреля 2010 г.)**
**Системы сертификации создаются**:
**— Федеральной службой по техническому и экспортному контролю,**
**— Федеральной службой безопасности Российской Федерации,**
**— Министерством обороны Российской Федерации**
**Сертификация средств защиты информации осуществляется на основании требований гос. стандартов, нормативных документов, утверждаемых Правительством РФ.**

**Обязательная сертификация в системе сертификации СЗИ-ГТ проводится на основании федеральных законов**
— "О государственной тайне",
— "Об органах федеральной службы безопасности в Российской Федерации"
— постановления от 26.06.95 г. N 608 "О сертификации средств защиты информации".
Во исполнение законов Российской Федерации
— "О сертификации продукции и услуг", — "О государственной тайне",
— постановления от 26 июня 1995 года N 608 "О сертификации средств защиты информации",
— Указа Президента РФ от 9 января 1996 года N 21 "О мерах по упорядочению разработки, производства, использования специальных технических средств, предназначенных для негласного получения информации"

14. Правовые проблемы, связанные с защитой прав обладателей интеллектуальной собственностью. Основные положения Гражданского кодекса РФ (Часть четвертая).

**Основные правовые нормы данных правоотношений собраны в 4 части Гражданского кодекса РФ от 18.12.2006 N 230-ФЗ (ред. от 23.05.2018)**

Раздел VII. Права на результаты интеллектуальной деятельности и средства индивидуализации. В структура главы ГК РФ делится на следующие виды права:

- авторское право (гл. 70) и смежные с ним права (гл. 71);
- патентное право (гл. 72); - право на селекционное достижение (гл. 73);
- право на топологию микросхемы (гл. 74); - права на средства индивидуализации (гл. 76).

**Право интеллектуальной собственности** - совокупность прав, предоставленных лицу (группе лиц) вследствие его (их) интеллектуальной деятельности.

**Интеллектуальные права** – это признаваемые законом субъективные права на владение продуктами интеллектуальной деятельности и способами индивидуализации.

**Виды интеллектуальных прав (статья 1226 ГК РФ)**

**1) Исключительное право** входит в группу имущественных прав. Предусматривает:

• Право пользоваться таким продуктом на своё усмотрение любым законным способом;
• Право распоряжаться этим продуктом;
• Право дозволять/возбранять посторонним лицам пользование продуктом;
• Право на юридическую защиту.

**2) Личные неимущественные права**, напрямую связанные с автором продукта, заключают в себе: право на авторство, на имя и т.п. . Все они не подлежат отчуждению от автора и передаче третьим лицам. Автор только владеет и пользуется личным неимущественным правом, в то время как распоряжаться и отказаться от него не может.

**3) Иные интеллектуальные права** (На основании статей 1292, 1293):

• **Право доступа**, включая авторское право на подражание произведениям изобразительного искусства, а также право создателя архитектуры на видео и фото;
• **Право следования** – процентные отчисления от стоимости перепродажи и др.

Виды прав на объекты интеллектуальной собственности, которые включают в себя:

**1) Авторское право**

**2) Права, смежные с авторскими:** исключительное право музыкальных исполнителей, организаций эфирного вещания и производителей фонограмм.

**3) Патентное право**

**4) Нетрадиционные объекты интеллектуальной собственности**. • селекционные достижения; • топологии интегральных микросхем; • секреты производства.

**5) Средства индивидуализации юр. лиц, предприятий, товаров и услуг**. объекты, регулируемые единым правовым институтом охраны маркетинговых обозначений.

15. Правовые проблемы, связанные с защитой прав обладателей интеллектуальной собственностью. Патентное право.

**Патентное право** – комплекс правовых норм, регламентирующих охрану изобретений, промышленных образцов и полезных моделей (промышленной собственностью) путем выдачи патентов. Патентное право распространяется также на селекционные достижения.

16. Правовые проблемы, связанные с защитой прав обладателей интеллектуальной собственностью. Авторское право.

**Авторское право**, регулирующее отношения лиц в процессе создания и использования произведений литературы, науки и искусства. Основой авторского права является понятие «произведение» как уникального результата творческой деятельности, облачённого в некую объективную форму.

Определение «авторское право» не относится к идеям и концепциям, открытиям и фактам, способам и методам, а также принципам, системам и процессам.

17. Особенности организации анализа рисков информационной безопасностью. Технологии анализа информационных рисков. Модели зрелости

Оценивание рисков может производиться с помощью:

— **экспертных оценок** (непосредственно (явно) или косвенно - с использованием автоматических программных средств, в логику работы которых заложена некоторая база знаний о зависимости меры какого- либо риска от наблюдаемых условий);

— **исторических сведений** о вероятности реализации уязвимости и ущерба от ее реализации (недостатками метода являются потребность в достаточно большом объеме исторических данных (а для некоторых угроз их может просто не существовать) и невозможность точного оценивания тренда в случае меняющейся обстановки, что мы наблюдаем практически во всех сферах ИБ);

— **аналитических подходов** (находящихся в большей степени в академических разработках), например, с построением графов взвешенных переходов

Основным фактором, определяющим отношение организации к вопросам информационной безопасности, является степень ее зрелости. Различным уровням зрелости соответствуют различные потребности в области информационной безопасности.

## Модель Cartner Group

| Уровни зрелости | Характеристика уровня зрелости |
|---|---|
| 0 | Проблема обеспечения ИБ управлением компании в должной мере не осознана и формально задачи обеспечения информационной безопасности компании не ставятся.<br>Выделенной службы информационной безопасности нет.<br>Служба автоматизации использует традиционные механизмы и средства защиты информации стека протоколов TCP/IP и сервисов Интранет, а также операционной среды и приложений (ОС, СУБД, СППР, ERP, ERP II, CRM). |
| 1 | Проблема обеспечения ИБ рассматривается управлением компании как исключительно техническая проблема.<br>Выделенной службы защиты информации нет.<br>Организационные меры обеспечения ИБ не используются. Финансирование осуществляется в рамках единого бюджета на IT-технологии.<br>Служба автоматизации дополнительно к средствам защиты информации 0 уровня может использовать средства отказоустойчивости, резервного копирования информации, источники бесперебойного питания, а также межсетевые экраны, виртуальные частные сети (VPN), антивирусные средства, средства прозрачного шифрования и e-Token. |
| 2 | Проблема обеспечения ИБ управлением компании осознана и рассматривается как взаимноувязанный комплекс организационных и технических мер.<br>Используются методики анализа информационных рисков, отвечающие минимальному, базовому уровню защищенности КИС.<br>В компании определены состав и структура штатной службы информационной безопасности.<br>Принята корпоративная Политика информационной безопасности.<br>Финансирование ИБ ведется в рамках отдельного бюджета на создание и поддержку корпоративной системы защиты информации.<br>Служба информационной безопасности дополнительно к средствам защиты информации 0 и 1 уровней использует средства защиты от НСД, системы обнаружения вторжений (IDS), инфраструктуру открытых ключей (PKI), а также соответствующие политике безопасности компании организационные меры (внешний и внутренний аудит, разработка планов защиты, непрерывного ведения бизнеса, действия в внештатных ситуациях и пр.) |
| 3 | Проблема обеспечения ИБ управлением компании осознана в полной мере.<br>Наряду с такими понятиями как бизнес культура существует понятие культуры информационной безопасности компании.<br>Активно используются методики полного количественного анализа информационных рисков, а также соответствующие инструментальные средства.<br>Назначен старший офицер по режиму информационной безопасности компании (CISO).<br>Определена состав и структура группы внутреннего аудита безопасности КИС(CISA), группы предупреждения и расследования компьютерных преступлений, группы экономической безопасности.<br>Руководством компании утверждены Концепция и Политика безопасности, План защиты и другие нормативно-методические материалы и должностные инструкции.<br>Финансирование ведется исключительно в рамках отдельного бюджета.<br>Служба информационной безопасности дополнительно к средствам защиты информации 0-2 уровней использует средства централизованного управления информационной безопасностью компании и средства интеграции с платформами управления сетевыми ресурсами. |

**Модель Carnegie Mellon University**

**Уровень 1. «Анархия»**

**Признаки:**

- сотрудники сами определяют, что хорошо, а что плохо; - затраты и качество не прогнозируются; - отсутствуют формализованные планы; - отсутствует контроль изменений; - высшее руководство плохо представляет реальное положение дел.

Политика в области ИБ не формализована, руководство не занимается этими вопросами. Обеспечением информационной безопасности сотрудники могут заниматься по своей инициативе, в соответствии со своим пониманием задач по должности.

**Уровень 2. «Фольклор»**

**Признаки:**

- выявлена определенная повторяемость организационных процессов; - опыт организации представлен в виде преданий корпоративной мифологии; - знания накапливаются в виде личного опыта сотрудников и пропадают при их увольнении.

На уровне руководства существует определенное понимание задач обеспечения информационной безопасности. Существуют стихийно сложившиеся процедуры обеспечения информационной безопасности, их полнота и эффективность не анализируются. Процедуры не документированы и полностью зависят от личностей вовлеченных в них сотрудников. Руководство не ставит задач формализации процедур защиты информации.

**Уровень 3. «Стандарты»**

**Признаки:**

- корпоративная мифология записана на бумаге; - процессы повторяемы и не зависят от личных качеств исполнителей; - информация о процессах для измерения эффективности не собирается; - наличие формализованного описания процессов не означает, что они работают; - организация начинает адаптировать свой опыт к специфике бизнеса;
- производится анализ знаний и умений сотрудников с целью определения необходимого уровня компетентности; - вырабатывается стратегия развития компетентности.

Руководство осознает задачи в области информационной безопасности. В организации имеется документация (возможно неполная), относящаяся к политике информационной безопасности. Руководство заинтересовано в использовании стандартов в области информационной безопасности.

**Уровень 4. «Измеряемый»**

**Признаки:**

- процессы измеряемы и стандартизованы.

Имеется полный комплект документов, относящихся к обеспечению режима информационной безопасности, оформленный в соответствии с каким-либо стандартом. Действующие инструкции соблюдаются, документы служат руководством к действию соответствующих должностных лиц. Регулярно проводится внутренний (и возможно внешний) аудит в области ИБ. Руководство уделяет должное внимание вопросам информационной безопасности, в частности имеет адекватное представление относительно существующих уровней угроз и уязвимостей, потенциальных потерях в случае возможных инцидентов.

**Уровень 5 «Оптимизируемый»**

**Признаки:**

- основное внимание уделяется повторяемости, измерении эффективности, оптимизации;
- вся информация о функционировании процессов фиксируется; - руководство заинтересовано в количественной оценке существующих рисков, готово нести

ответственность за выбор определенных уровней остаточных рисков, ставит оптимизационные задачи построения системы защиты информации.
Проблема обеспечения режима информационной безопасности будет ставиться (хотя бы в неявном виде) и решаться для организаций, находящихся на разных уровнях развития, по-разному. На данном уровне ставятся и решаются различные варианты оптимизационных задач в области обеспечения режима информационной безопасности.
Примеры постановок задач:
— Выбрать вариант подсистемы информационной безопасности, оптимизированной по критерию стоимость/эффективность при заданном уровне остаточных рисков.
— Выбрать вариант подсистемы информационной безопасности, при котором минимизируются остаточные риски при фиксированной стоимости подсистемы безопасности.
— Выбрать архитектуру подсистемы информационной безопасности с минимальной стоимостью владения на протяжении жизненного цикла при определенном уровне остаточных рисков.

18. Подготовка системы управления информационной безопасностью организации к сертификации в соответствии с ГОСТ Р ИСО/МЭК 27001-2006.

Целью такого проекта является подготовка и сертификация системы управления информационной безопасностью, СУИБ компании согласно требованиям гармонизированного стандарта ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности".
Подготовка системы управления информационной безопасностью к сертификации в соответствии с ГОСТ Р ИСО/МЭК 27001-2006 осуществляется по следующим этапам.

**Этап 1. Оценка текущего состояния СУИБ**

На данном этапе проводятся все необходимые мероприятия для идентификации и документирования целей и мер контроля в соответствии с ГОСТ Р ИСО/МЭК 27001-2006.
1. Должны быть определены цели и задачи (Scope) проекта, а также политика ИБ для СУИБ, выдвигаемой на сертификацию по требованиям ГОСТ Р ИСО/МЭК 27001-2006.
2. Должна быть определена область применения системы управления информационной безопасностью. Ее границы следует определить, исходя из характеристики организации, ее местоположения, информационных активов и используемых технологий.
3. Должна быть осуществлена проверка адекватности и полноты системы оценки рисков. Система оценки рисков должна выявлять угрозы для информационных активов предприятия, уязвимые места и их последствия для организации, а также определять величину риска.
4. На основе политики ИБ организации и с учетом степени необходимой гарантии определяются те области рисков, которые должны быть управляемыми.
5. Из подробного списка рекомендуемых международным стандартом ГОСТ Р ИСО/МЭК 27001-2006целей контроля следует выбрать цели контроля, необходимые для внедрения; отбор следует обосновать.
6. Должен быть подготовлен документ о применимости стандарта. В нем следует изложить выбранные цели и средства контроля, а также причины их выбора. Кроме того, в этом отчете необходимо указать средства контроля из списка стандарта ГОСТ Р ИСО/МЭК 27001-2006, которые не были приняты.

Проверяется имеющаяся в компании документация по системе управления информационной безопасностью на основе критериев, определенных стандартом ГОСТ Р ИСО/МЭК 27001-2006. Документация по системе управления ИБ должна содержать следующую информацию:

1. Свидетельства о предпринятых мерах в соответствии с принципами системы управления информационной безопасностью.
2. Общие принципы управления ИБ, включая политику в области информационной безопасности, цели и применяемые средства контроля, описанные в документе о применимости стандарта.
3. Описание процедур, принятых в целях эффективного применения средств контроля и проверенных на соответствие политике в области безопасности. При этом должны быть указаны обязанности ответственных лиц и их действия.
4. Описание процедур по управлению и использованию системы управления информационной безопасности. При этом должны быть указаны обязанности ответственных лиц и их действия.

Компания должна определять и реализовывать процедуры контроля всей требуемой документации, чтобы выполнить следующие требования в отношении последней:
— документация готова к использованию;
— производится периодическая проверка документации и внесение необходимых изменений в соответствии с политикой безопасности организации;
— производится управление обновлениями и обеспечение доступности документации везде, где осуществляется деятельность, имеющая важное значение для эффективного функционирования системы управления информационной безопасностью;
— устаревшая информация своевременно удаляется;
— устаревшая документация, требуемая тем не менее для юридических целей и/или сохранения знаний, определяется и сохраняется.
Документация должна быть удобной в обращении, содержать даты подготовки (включая даты внесения изменений) и быть легко узнаваемой, вестись в установленном порядке и храниться в течение определенного срока.
Следует определить и выполнять процедуры и обязанности по разработке и введению изменений в различные виды документов.
Документация может быть представлена в любой форме: печатной или электронной.
Проверяются все существующие процедуры ведения учетных записей в соответствии с критериями стандарта ГОСТ Р ИСО/МЭК 27001-2006.
Данные, полученные в результате функционирования системы управления информационной безопасностью, должны сохраняться в документированном виде с целью демонстрации соответствия требованиям стандарта ГОСТ Р ИСО/МЭК 27001-2006 применимо к самой системе и организации в целом (например, книга посетителей, аудиторская документация и санкционирование доступа).

Таблица Группы разрабатываемых нормативных документов организации:

| № | Группы разрабатываемых нормативных документов организации |
|---|---|
| 1 | Документы работников |
| 2 | Делопроизводство |
| 3 | Приказы |
| 4 | Протоколы и решения совещаний |
| 5 | Политики информационной безопасности |
| 6 | Положения |
| 7 | Регламенты и методологии |
| 8 | Стандарты |
| 9 | Договоры и соглашения |
| 10 | Аудит ИБ |

Компания должна самостоятельно определить и выполнять процедуры выявлению, учету, хранению и использованию данных.

По свидетельствующих о соответствии предъявляемым требованиям.

Документы должны быть удобными в обращении, узнаваемыми и указывать на конкретные действия. Их следует хранить и поддерживать в таком состоянии, чтобы можно было легко восстановить и защитить от повреждения или потери.

В результате выявляются любые недостатки СУИБ в соблюдении стандартов ГОСТ Р ИСО/МЭК 27001-2006 и подготовка плана их устранения. На данном этапе выполняются предусмотренные стандартом ГОСТ Р ИСО/МЭК 27001-2006 мероприятия, связанные с оценкой документации по внедрению общих принципов системы управления ИБ и ознакомление с текущим состоянием дел в рамках проекта.

**Этап 2. Оценка эффективности внедрения СУИБ**

На данном этапе работ, согласно требованиям стандарта ГОСТ Р ИСО/МЭК 27001-2006, проводится оценка, подтверждающая эффективность внедрения системы управления информационной безопасностью и ее соответствие установленным требованиям, а также выбранным мерам и средствам контроля стандарта ГОСТ Р ИСО/МЭК 27001-2006.

По итогам выполнения работ составляется отчет, в котором будет высказано мнение относительно сертификации, в частности в отчете будет отражена оценка деятельности по управлению информационной безопасностью на объектах организации на предмет соответствия международному стандарту ГОСТ Р ИСО/МЭК 27001-2006.

**Этап 3. Инспекции СУИБ**

В соответствии с правилами сертификации необходимо проводить регулярную оценку объекта на соответствие требованиям международного стандарта ISO 27001:2005. Критерии периодичности таких посещений основаны на действующих критериях получения аккредитации UKAS.

Как правило, проводится две инспекции в год до истечения трех лет с момента сертификации, после чего срок действия сертификации продлевается.

По истечении трех лет с момента сертификации может потребоваться дополнительный день для возобновления срока действия сертификации.

Предусматривается, что на третьем этапе инспекционные визиты будут проводиться один раз в шесть месяцев представителями, например, BSI Россия, начиная с момента

получения сертификации на протяжении первых трех лет срока действия сертификации, данные проверки будут осуществляться в соответствии с согласованным планом оценки.

19. Основные положения в области обеспечения информационной безопасности в системах межведомственного электронного взаимодействия.

Осуществляется в соответствии со следующими нормативными правовыми актами и нормативными правовыми документами:

**Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»**

**ЭЛЕКТРОННОЕ СООБЩЕНИЕ** - информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

**ЭЛЕКТРОННЫЙ ДОКУМЕНТ** - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

**ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

**Федеральный закон закрепляет:**

• положения о регулировании создания и эксплуатации информационных систем,

• общие требования к использованию информационно- телекоммуникационных сетей,

• устанавливает принципы регулирования общественных отношений, связанных с использованием информации.

Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

**Постановление Правительства РФ от 22 сентября 2009 г. N 754 "Об утверждении Положения о системе межведомственного электронного документооборота" (С изменениями и дополнениями от 1 августа 2011 г., 6 сентября 2012 г., 6 апреля 2013 г.)**

Межведомственный электронный документооборот представляет собой взаимодействие информационных систем электронного документооборота

**–федеральных органов исполнительной власти,**

**–органов исполнительной власти субъектов Российской Федерации**

**–и иных государственных органов (далее соответственно — информационные системы электронного документооборота, участники межведомственного электронного документооборота).**

Установлен порядок ведения электронной служебной переписки между федеральными органами государственной власти, Администрацией Президента Российской Федерации и Аппаратом Правительства Российской Федерации:

• направление и получение решений и поручений Президента Российской Федерации и Правительства Российской Федерации,

• получение информации о ходе их рассмотрения,

• направление докладов Президенту Российской Федерации и Правительству Российской Федерации,

• внесение в Правительство Российской Федерации проектов нормативных правовых актов,

• осуществление согласительных процедур по ним.

• Организатором межведомственного электронного документооборота является ФСО России.

1. Допускается обмен сообщениями, содержащими общедоступную информацию и ту, что отнесена к служебной тайне.
2. Определены принципы электронного документооборота, его технико- технологическая структура, меры по обеспечению информационной безопасности. Организатором межведомственного электронного документооборота является ФСО России.
3. Технические средства узла участника документооборота должны располагаться в помещениях, обеспечивающих их сохранность и конфиденциальность информации.
4. Электронные сообщения подлежат регистрации.
Организатором межведомственного электронного документооборота является ФСО России.
5. Для организации каналов связи межведомственного электронного документооборота используются:
— каналы связи организатора межведомственного электронного документооборота
— и (или) каналы связи, арендуемые организатором межведомственного электронного документооборота у операторов связи.

**Технические требования к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти (утв. распоряжением Правительства Российской Федерации от 2 октября 2009 г. N 1403-р)**

• Через указанную систему происходит обмен электронными сообщениями между федеральными органами государственной власти.
• Она обеспечивает доставку электронных сообщений адресатам с отсылкой отправителю квитанций о времени их получения; целостность электронных сообщений; поддержку справочников (коды лиц, подписывающих документы, подразделений, адресатов документов и т. д.).
• Приведены требования к ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ систем
• Должна обеспечиваться антивирусная защита системы межведомственного электронного документооборота.
• При передаче сообщений, содержащих гостайну, должны использоваться сертифицированные технические и (или) программные средства защиты информации.

**"СИСТЕМА МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА"** — федеральная информационная система, обеспечивающая в автоматизированном режиме защищенный обмен электронными сообщениями, в том числе сообщениями, содержащими информацию, отнесенную к сведениям, составляющим служебную тайну, между Администрацией Президента Российской Федерации, Аппаратом Правительства Российской Федерации и федеральными органами исполнительной власти, а также иными федеральными органами государственной власти;

**"СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА"** — система автоматизации делопроизводства и документооборота в федеральном органе исполнительной власти, обеспечивающая возможности внутреннего электронного документооборота.

**Приказ ФСБ России и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. N 416/489 "Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования**

Методы и способы защиты информации определяются оператором ИС. Он обязан поддерживать целостность и доступность информации, своевременно выявлять и предотвращать неправомерные действия в ее отношении, не допускать воздействие на технические средства ИС. Необходимо обеспечить возможность оперативного восстановления (в течение 8 часов) модифицированной или уничтоженной информации,

а также записи и хранения сетевого трафика. Запросы пользователей о предоставлении сведений и ответы на них регистрируются в электронном журнале обращений.

В зависимости от значимости информации ИС подразделяются на 2 класса. К первому относятся правительственные и иные ИС, нарушение целостности и доступности информации которых может привести к угрозе безопасности страны. Все остальные входят во II класс. В зависимости от класса установлены и требования к защите информации. Так, в первых могут применяться лишь сертифицированные ФСБ России средства криптографической защиты, обнаружения вирусов, контроля доступа, фильтрации и блокирования сетевого трафика. В ИС II класса могут использоваться средства защиты, сертифицированные ФСТЭК России.

Информационные системы общего пользования должны обеспечивать:

1.сохранность и неизменность обрабатываемой информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения (далее — ЦЕЛОСТНОСТЬ информации);

2.беспрепятственный доступ пользователей к содержащейся в информационной системе общего пользования информации (далее — ДОСТУПНОСТЬ информации);

3.защиту от действий пользователей в отношении информации, не предусмотренных правилами пользования информационной системой общего пользования, приводящих, в том числе к уничтожению, модификации и блокированию информации (далее — НЕПРАВОМЕРНЫЕ ДЕЙСТВИЯ).

**Приказ Министерства информационных технологий и связи Российской Федерации от 9 января 2008 г. N 1 "Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации"**

В целях защиты от несанкционированного доступа к сетям связи и передаваемой посредством их информации операторы связи принимают:

— организационные

— и технические меры, направленные на предотвращение доступа к линиям связи, сооружениям связи, средствам связи, находящимся как внутри, так и вне сооружений связи, и передаваемой по сетям связи информации, осуществляемого с нарушением установленного этими операторами связи порядка доступа.

• Узлы связи сетей связи подразделяются на узлы связи I, II, III категории защищенности.

• Приведено категорирование узлов связи по защищенно

• Защита от несанкционированного доступа к абонентским линиям связи при применении радиоэлектронных средств обеспечивается кодированием информации в радиоканале.

• Все случаи несанкционированного доступа к сетям связи и передаваемой посредством их информации подлежат обязательной регистрации и анализу.

**Постановление Правительства РФ от 8 сентября 2010 г. N 697 "О единой системе межведомственного электронного взаимодействия" (с изменениями и дополнениями от 8 июня, 28 ноября 2011 г., 6 ноября 2013 г.)**

Утверждено Положение о единой системе межведомственного электронного взаимодействия. Это федеральная информационная государственная система.

С помощью системы материалы, поданные через Единый портал государственных и муниципальных услуг (функций), передаются в информсистемы соответствующих органов и организаций для обратной отправки необходимых сведений. Обеспечивается обмен сообщениями между указанными лицами. Системы органов и организаций к единой системе подключает ее оператор (Минкомсвязь России).

Целью создания системы взаимодействия является технологическое обеспечение информационного взаимодействия:

а) при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме;
б) в иных случаях, предусмотренных федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации.

**ЕДИНАЯ СИСТЕМА МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ** — федеральная государственную информационную систему, включающую: информационные базы данных, в том числе содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа через систему взаимодействия к их информационным системам (далее - электронные сервисы), сведения об истории движения в системе взаимодействия электронных сообщений при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в электронной форме, а также программные и технические средства, обеспечивающие взаимодействие информационных систем органов и организаций, используемых при предоставлении в электронной форме государственных и муниципальных услуг и исполнении государственных и муниципальных функций.

**Распоряжение Правительства РФ от 2 октября 2009 г. N 1403-р «Об утверждении технических требований к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти»**

**"СИСТЕМА МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА"** — федеральная информационная система, обеспечивающая в автоматизированном режиме защищенный обмен электронными сообщениями, в том числе сообщениями, содержащими информацию, отнесенную к сведениям, составляющим СЛУЖЕБНУЮ ТАЙНУ, между Администрацией Президента Российской Федерации, Аппаратом Правительства Российской Федерации и федеральными органами исполнительной власти, а также иными федеральными органами государственной власти;
Организатор межведомственного электронного документооборота осуществляет следующие функции:
а) организационное и методическое обеспечение межведомственного электронного документооборота;
б) формирование и актуализация глобальных адресных справочников почтовых серверов;
в) обеспечение инфраструктуры документооборота;
г) обеспечение межведомственного соответствии с законодательством Российской Федерации.

Информационная безопасность при осуществлении межведомственного электронного документооборота обеспечивается комплексом технических и организационных мероприятий.

**ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ:**
а) контроль выполнения требований нормативных документов, регламентирующих обеспечение защиты информации;
б) определение должностных лиц участников межведомственного электронного документооборота и организатора межведомственного электронного документооборота, ответственных за обеспечение информационной безопасности;
в) установление порядка резервного копирования, восстановления и архивирования баз данных, находящихся на головном узле межведомственного электронного документооборота, а также порядка обновления антивирусных баз;
г) установление порядка допуска для проведения ремонтно-восстановительных работ программно-технических средств;

д) организация режимных мероприятий в отношении помещений, в которых размещены узлы участников межведомственного электронного документооборота, и технических средств этих узлов.

**Постановление Правительства РФ от 8 сентября 2010 г. N 697 «О единой системе межведомственного электронного взаимодействия» (8 июня, 28 ноября 2011 г., 6 ноября 2013 г.)**

Это федеральная информационная госсистема. В нее входят базы данных и сведения об истории движения электронных сообщений при предоставлении (исполнении) государственных и муниципальных услуг (функций) в электронной форме (далее - услуги, функции).

Также система включает в себя программные и техсредства, обеспечивающие взаимодействие информсистем органов и организаций, используемых при предоставлении услуг и исполнении функций. С помощью системы материалы, поданные через Единый портал государственных и муниципальных услуг (функций), передаются в информсистемы соответствующих органов и организаций для обратной отправки необходимых сведений. Обеспечивается обмен сообщениями между указанными лицами. Системы органов и организаций к единой системе подключает ее оператор (Минкомсвязь России). Система должна быть введена в эксплуатацию в 3-месячный срок. Субъектам Российской Федерации и муниципалитетам рекомендовано создать аналогичные региональные системы.

**Постановление Правительства РФ от 10 июля 2013 г. N 584 "Об использовании федеральной государственной информационной системы"**

«Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»

**ИДЕНТИФИКАЦИЯ** — процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. Под идентификацией понимается также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**АУТЕНТИФИКАЦИЯ** — процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта.

**Постановление Правительства РФ от 10 июля 2013 г. N 584 "Об использовании федеральной государственной информационной системы...**

Данным постановлением регламентирован порядок использования единой системы идентификации и аутентификации в инфраструктуре, обеспечивающей электронное оказание государственных и муниципальных услуг. Лица, зарегистрированные в этой системе, получают санкционированный интернет-доступ к сведениям, содержащимся в государственных (муниципальных) и иных информационных системах. Им предоставляется "личный кабинет" на Едином портале государственных и муниципальных услуг (функций). Для регистрации в единой системе используются простые электронные и усиленные квалифицированные электронные подписи. Самостоятельно пройти эту процедуру можно, зайдя на единый портал, или посредством иных госинформсистем, взаимодействующих с единой системой. Регистрация не требуется для получения бесплатной общедоступной информации. Единая система используется на безвозмездной основе.

20. Понятие шифровального средства. Нормативная база. Организационное обеспечение

криптографической защиты в РФ. Категории шифровальных средств. Основные классы СКЗИ.

**СРЕДСТВА ШИФРОВАНИЯ** — аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее передаче по каналам связи и (или) при ее обработке и хранении.

**Постановление Правительства Российской Федерации от 29 декабря 2007 г. N 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»**

**Приказ ФСБ России от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»**

**Определяют две большие категории шифровальных средств:**

• шифры, предназначенные для защиты информации, содержащей сведения, составляющие государственную тайну Российской Федерации;

• шифры, предназначенные для защиты конфиденциальной информации, не составляющую государственную тайну, доступ к которой ограничен в соответствии с законодательством России.

В зависимости от уровня обеспечиваемой защиты, средства криптографической защиты информации **(СКЗИ) подразделяются на различные классы, такие как КС1, КС2, КС3, КВ1, КВ2, КА1.**

21. Порядок классификации средств криптографической защиты информации. Нормативная база.

**Классификация СКЗИ**

В зависимости от уровня обеспечиваемой защиты, средства криптографической защиты информации (СКЗИ) подразделяются на различные классы, такие как КС1, КС2, КС3, КВ1, КВ2, КА1. Этот принцип классификации определяется следующими факторами:

- **Комплекс инструментов нарушителя.** Классификация учитывает возможность удаленного или физического доступа нарушителя, его способности в области реализации атак и наличие актуальных угроз и недокументированных возможностей.
- **Защищаемые объекты.** Класс СКЗИ зависит от того, какая информация, документация или компоненты информационной системы должны быть защищены. Это могут быть серверы, рабочие станции, базы данных и другие элементы системы.
- **Место потенциальных атак.** Классификация СКЗИ учитывает возможность атак внутри или за пределами контролируемых зон. Некоторые классы СКЗИ могут обеспечивать защиту от внутренних атак, а другие - от внешних угроз.

В соответствии с ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», СКЗИ подразделяются на следующие классы:

- СКЗИ для формирования электронной цифровой подписи (ЭЦП)
- СКЗИ для хранения ключевой информации
- СКЗИ общего назначения
- СКЗИ специального назначения.

22. Основные уровни защиты информации на предприятии. Требования к порядку разработки, производства, реализации и эксплуатации СКЗИ. Терминология.

**Можно выделить три основных уровня защиты информации:**
• защита информации на уровне рабочего места пользователя;
• защита информации на уровне подразделения предприятия;
• защита информации на уровне предприятия.

Приказ ФСБ РФ от 9 февраля 2005 г. № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
**Основные требования к порядку разработки:**
Требования к СКЗИ (цель криптографической защиты информации с описанием предполагаемой модели нарушителя, определяющей возможные угрозы, которым должно противостоять разрабатываемое (модернизируемое) СКЗИ
Требования к аппаратным, программно-аппаратным и программным средствам сети (системы) конфиденциальной связи, совместно с которыми предполагается использование создаваемого нового образца СКЗИ или модернизируемого действующего образца СКЗИ
Требования к условиям размещения СКЗИ при их эксплуатации
Требования к ключевой системе СКЗИ и т.д.)
**Основные требования к порядку производства:**
Производство СКЗИ осуществляется в соответствии с техническими условиями, согласованными с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.
СКЗИ изготавливаются в полном соответствии с конструкцией и технологией изготовления опытных образцов СКЗИ, прошедших испытания на функционирование опытного образца СКЗИ в штатных режимах и имеющих положительное заключение экспертизы тематических исследований СКЗИ.
Все изменения в конструкции СКЗИ и технологии их изготовления изготовитель СКЗИ должен согласовывать со специализированной организацией и ФСБ России.
**Основные требования к порядку реализации:**
Реализация (распространение) СКЗИ и (или) РКД на них осуществляется юридическим лицом или индивидуальным предпринимателем, имеющим право на осуществление данного вида деятельности, связанного с шифровальными (криптографическими) средствами.
Реализация (распространение) СКЗИ и (или) РКД на них осуществляется только после получения лицензии
**Терминология:**
**Средство криптографической защиты информации** — средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.
**КРИПТОСРЕДСТВО** – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну
**К криптосредствам относятся средства криптографической защиты информации (СКЗИ)** — шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.
**СКЗИ** — Сертифицированные средства криптографической защиты конфиденциальной информации.
**КЛЮЧЕВОЙ ДОКУМЕНТ** — физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости — контрольную, служебную и технологическую информацию;

**КЛЮЧЕВОЙ НОСИТЕЛЬ** — физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.);

**КЛЮЧЕВОЙ БЛОКНОТ** — набор бумажных ключевых документов одного вида (таблиц, перфолент, перфокарт и т.п.), сброшюрованных и упакованных по установленным правилам.