Основы ИБ

Тема №1 Занятие №1

1. Периоды развития средств и методов защиты информации.

Первый период (с древнейших времён до 20-х годов XIX века) определяется началом создания осмысленных и самостоятельных средств и методов защиты информации и связан с появлением возможности фиксации информационных сообщений на твердых носителях, то есть с изобретением письменности.

Этот период характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

Вместе с неоспоримым преимуществом сохранения и перемещения данных возникла проблема сохранения в тайне,

существующей уже отдельно от источника конфиденциальной информации, поэтому практически одновременно с рождением письменности возникли такие методы защиты информации, как шифрование и скрытие.

Второй период (с двадцатых годов XIX века до тридцатых годов XX века) характеризуется появлением технических средств обработки информации и передачи сообщений с помощью электрических сигналов и электромагнитных полей (например, телефон, телеграф, радио). В связи с этим возникли проблемы защиты от так называемых радиоэлектронных технических каналов утечки (побочных излучений, наводок и др.).

Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

Также в этот период активно развиваются технические средства разведки, многократно увеличивающие возможности промышленного и государственного шпионажа.

Огромные, все возрастающие убытки предприятий и фирм способствовали научно-техническому прогрессу в создании новых и совершенствовании старых средств и методов защиты информации.

Третий период (с тридцатых годов XX века по настоящее время) связан с внедрением автоматизированных систем обработки информации. При этом, продолжают активно развиваться способы и методы защиты от утечки по техническим каналам.

2. Этапы развития средств и методов защиты информации в рамках 3 периода.

I этап – начиная с 1935 года по 1945 год – связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства помех.

II этап – начиная с 1946 года по 1965 год – связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

III этап – начиная с 1965 года по 1973 год – обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

IV этап – начиная с 1973 года по 1985 год – связан с использованием мобильных средств связи с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Образовались сообщества людей – хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей и организаций. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности – важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право – новая отрасль международной правовой системы.

V этап – начиная с 1985 года по настоящее время – связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

3. В чем состоит актуальность информационной безопасности?

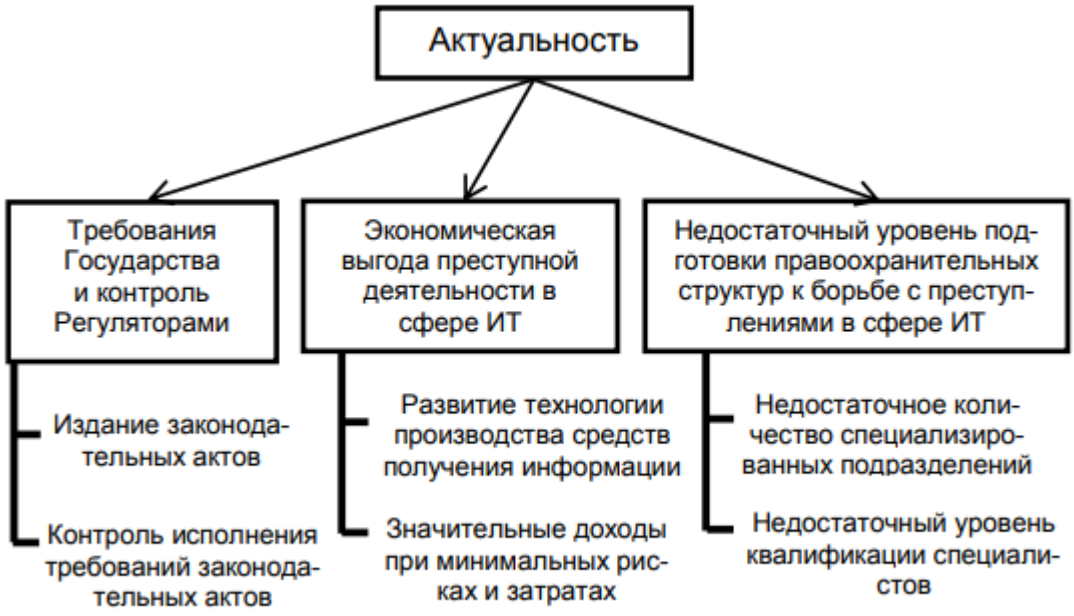

Рис. 1.1. Актуальность информационной безопасности

4. Причины, побуждающие заниматься защитой информации.

5. Что такое информация?
Информация - это любые сведения (данные) независимо от формы их представления

6. Определение конфиденциальной информации.
Конфи - это подвид информации ограниченного доступа, представляющий собой: персональные данные, служебные сведения, тайны следствия + судопроизводства, коммерческая тайна, проф. тайна, сущность изобретения

7. Дать классификацию информации.
Общедоступная и ограниченного доступа

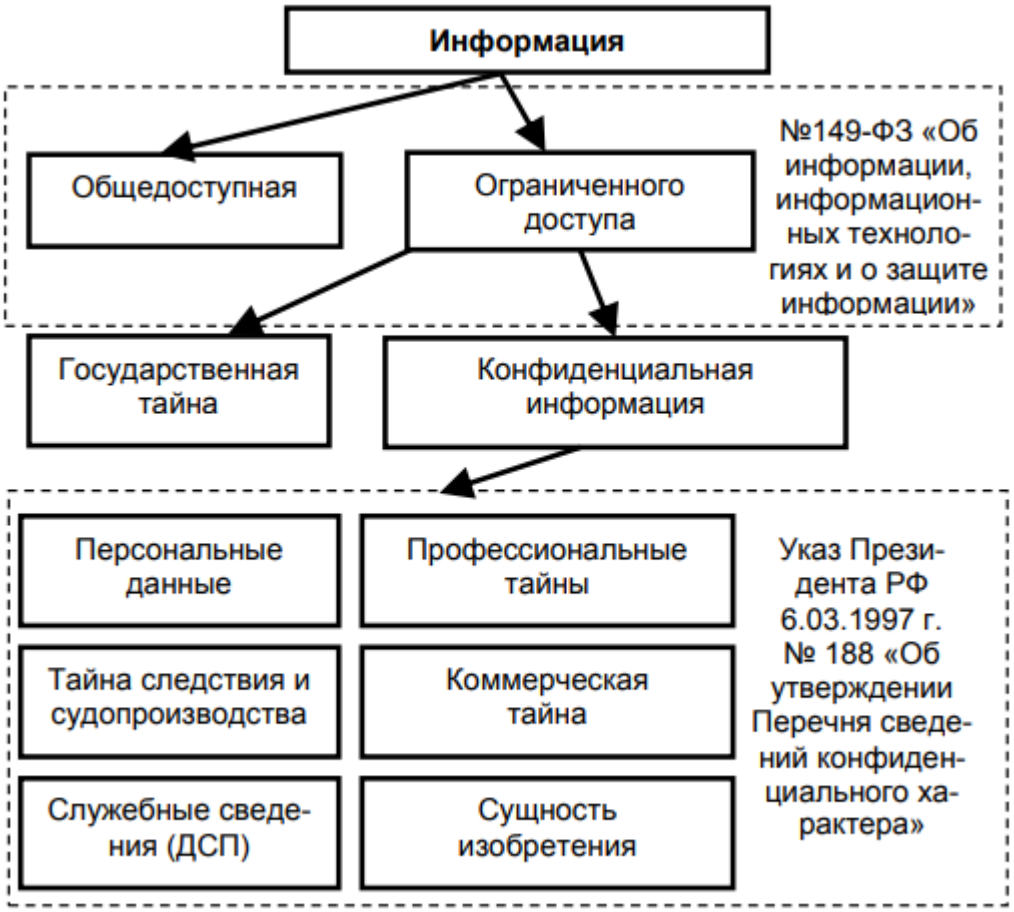

Рис. 2. Классификация информации

8. Перечислить основные аспекты ИБ.

Конфиденциальный аспект. Означает, что нужно тщательно контролировать работу с данными, чтобы устранить возможность их утечки, а также предотвратить несанкционированный доступ к ним со стороны неизвестных людей. Конфиденциальность должна присутствовать на всех этапах: при разработке ресурса, при работе с данными, при их сохранении, внесении в базу и транзите.

Целостностный аспект. Это комплексная работа при защите данных, которая обеспечит защиту от сбоев в работе и уничтожения самих данных. Целостность больше связана с системой управления ресурсом, а не с его технической частью.

Аспект доступности. Включает в себя обеспечение надежного и эффективного доступа к защищаемой информации только проверенных лиц. Если защищаемая система была «взломана», то данный аспект гарантирует ее качественное восстановление и обеспечение работоспособности.

9. Дать определение конфиденциальности информации.

конфиденциальность информации – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право

10. Дать определение целостности информации.
целостность информации – состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

11. Дать определение доступности информации.
доступность информации – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

12. Что такое информационная система?
Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств

13. Что является объектом защиты информации?
Объектом защиты информации является **информационная система** (предприятия, коммерческой организации) или автоматизированная система обработки данных. В состав объектов защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.
Предметом же защиты – информация.

14. Дать определение ИБ РФ.
информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

15. Дать определение ИБ в узком смысле.
В более узком смысле будем считать: **информационная безопасность** – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

16. Что такое защита информации?
Защита информации - это действия, направленные на предотвращение утечки информации, а также несанкционированного доступа к ней

17. Как классифицируют меры защиты информации?
1. **Правовые** (законодательные);
2. **Морально-этические**;
3. **Организационные**;
4**. Инженерно-технические:**
– физические;
– технические (программно-аппаратные);
– криптографические.

Правовая защита информации или 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.
К **морально-этическим** мерам относятся устоявшиеся в обществе нормы поведения. В отдельных случаях они могут быть оформлены в письменном виде, например, уставом или кодексом чести организации. Соблюдение морально-этических норм не является обязательным и носит скорее профилактический характер.
Организационные (административные) меры защиты – меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой. Среди базовых организационных мер по защите информации можно выделить следующее: – формирование политики безопасности; – регламентация доступа в помещения; – регламентация допуска сотрудников к использованию ресурсов информационной системы. – определение ответственности в случае несоблюдения требований информационной безопасности и др.
Инженерно-техническая защита (ИТЗ) – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации. Она решает следующие задачи: – предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или искажения; – защита носителей информации от уничтожения в результате воздействия стихийных сил; – предотвращение утечки информации по различным техническим каналам.

18. Дать понятие правовой защите информации.

Правовая защита информации или **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

19. Дать понятие организационным мерам ЗИ.
Организационные (административные) меры защиты – меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой. Среди базовых организационных мер по защите информации можно выделить следующее: – формирование политики безопасности; – регламентация доступа в помещения; – регламентация допуска сотрудников к использованию ресурсов информационной системы.

20. Дать определение физической ЗИ.
Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

21. Дать определение ТЗИ.
Техническая защита информации (ТЗИ) – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

22. Дать определение криптографической ЗИ.
Криптографическая защита информации – защита информации с помощью ее криптографического преобразования

23. Дать понятие ЗИ от утечки.
ЗИ от утечки - деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате её разглашения, несанкционированного доступа и получения защищаемой информации службами разведки

24. Дать понятие ЗИ от разглашения.
ЗИ от разглашения - деятельность, направленная на предотвращение несанкционированного доступа к информации неопределенным кругом лиц или передачи защищаемой информации неопределенному кругу лиц.

25. Дать определение ЗИ от НСД

ЗИ от несанкционированного доступа -деятельность, направленная на предотвращения получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав и/или правил доступа к защищаемой информации.

26. Дать определение ЗИ от НСВ

ЗИ от несанкционированного воздействия - деятельность, направленная на предотвращения воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате уничтожению или сбою функционирования носителей информации.

Тема №1 Занятие №2

27. Понятие комплексности при защите информации.

Комплексность при ЗИ – совокупность организационно-правовых и инженерно-технических мероприятий, направленных на обеспечение ЗИ от разглашения, утечки, НСД и НСВ.

28.Уровни (рубежи) защиты информации.

Уровни ЗИ:

1)Охрана по периметру территории
2)Охрана по периметру здания
3)Охрана помещения
4)Защита аппаратных средств
5)Защита программных средств
6)Защита информации

29.Определение комплексной системы защиты информации (КСЗИ).

КСЗИ – использование в оптимальном сочетании различных методов и средств ЗИ: правовых, организационных, физических, технических, криптографических.

Комплексная система защиты информации (КСЗИ) - это совокупность организационно-правовых и инженерно-технических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки, несанкционированного доступа и воздействия.

- 30. Основные задачи, решаемые КСЗИ.данных, передаваемых по каналам связи

1) Управление доступом пользователей автоматизированной системы с целью её защиты от случайного или умышленного вмешательства и НСД.
2) Защита данных, передаваемых по каналам связи
3) Регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношений к её безопасности
4) Контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора по безопасности о попытках НСД к ресурсам системы
5) Контроль и поддержание целостности критических ресурсов системы защиты и среды использования прикладных программ
6) Управление средствами системы защиты
7) Обеспечение замкнутой среды проверенного ПО с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ и средств

преодоления системы защиты, а также от внедрения вредоносных компьютерных программ.
8) Управление средствами системы защиты

Тема №2 Занятие №1

1. Как классифицируют меры защиты информации?
   1) правовая (законодательная) защита информации
   2) организационная защита информации
   3) инженерно-техническая защита
   -физическая защита информации
   -техническая защита информации
   -криптографическая защита информации

2. Дать понятие правовой защите информации

правовая (законодательная) 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

3. Дать понятие организационным мерам ЗИ.
   организационная защита информации – реализующая меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой

4. Дать определение физической ЗИ.
   физическая защита информации — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

5. Дать определение ТЗИ
   техническая защита информации — защита информации, заключающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

6. Дать определение криптографической ЗИ.
   криптографическая защита информации — защита информации с помощью ее криптографического преобразования.

7. Что включает Государственная система защиты информации?
   Государственная система защиты информации включает:
   – органы законодательной, исполнительной и судебной властей;
   – законодательство, регулирующее отношения в области защиты информации и информационных ресурсов;
   – нормативную правовую базу по защите информации;
   – службы (органы) защиты информации предприятий, организаций, учреждений.

8. Функции органов законодательной власти.
   Органы законодательной власти (Государственная дума) издают законы, регулирующие отношения в области защиты информации.

9. Функции органов исполнительной власти.
   Органы исполнительной власти (правительство) контролируют исполнение этих законов. Правительство принимает соответствующие постановления в области защиты информации и издает распоряжения, являющиеся подзаконными нормативными правовыми актами.

10. Функции Министерств и ведомств.
    Министерства и ведомства разрабатывают и принимают постановления и решения, являющиеся нормативными правовыми актами. Кроме того, они разрабатывают и утверждают такие нормативные акты, как положения, руководства, инструкции, правила, методические рекомендации. К нормативным актам этого уровня относятся также приказы и письма руководителей ведомств и министерств.

11. Основное содержание Доктрины информационной безопасности Российской Федерации

    Доктрина информационной безопасности Российской Федерации, Указ Президента РФ от 5 декабря 2016 года, содержит систему взглядов на обеспечение национальной безопасности в информационной сфере. Она определяет национальные интересы страны, такие как защита прав и свобод граждан, бесперебойное функционирование критической информационной инфраструктуры, развитие ИТ-отрасли, достоверная информация о госполитике и международная информационная безопасность. В Доктрине перечислены информационные угрозы, стоящие перед страной и обществом, включая вмешательство других стран и спецслужб, рост компьютерной преступности, нарушение конституционных прав и свобод, зависимость от зарубежных ИТ-технологий и использование технологического превосходства для доминирования в информационном

пространстве. Основная стратегическая цель обеспечения информационной безопасности в обороне страны - это защита интересов личности, общества и государства от внутренних и внешних угроз, связанных с использованием информационных технологий в военно-политических целях.

12. Основное содержание Стратегии национальной безопасности Российской Федерации.
    Стратегия национальной безопасности Российской Федерации, утвержденная в июле 2021 года, дает анализ угроз в области информационной безопасности, которые включают увеличение вероятности возникновения угроз безопасности граждан, расширение использования информационно-коммуникационных технологий для вмешательства во внутренние дела государств, увеличение компьютерных атак на российские информационные ресурсы, активизация деятельности специальных служб иностранных государств, распространение недостоверной информации, стремление транснациональных корпораций закрепить свое монопольное положение в сети "Интернет" и расширение масштабов преступлений в информационно-коммуникационной сфере. Целью обеспечения информационной безопасности является укрепление суверенитета России в информационном пространстве, а для ее достижения необходимо решить задачи, такие как создание инфраструктуры для обеспечения защиты информации, развитие национальных информационных технологий и защиты детей от негативной информации в интернете.

13. Основное содержание №149-ФЗ «Об информации, информационных технологиях и о защите информации».

    В статье рассматриваются **основные аспекты Федерального закона № 149-ФЗ**, который является основным законом об информации в России. Закон определяет такие понятия, как информация, веб-сайт, электронная коммуникация и поисковая система, а также излагает требования к защите информации. Закон содержит указания о том, какая информация считается конфиденциальной, когда и как доступ к информации может быть ограничен, а также как происходит обмен данными между организациями. Ключевые положения закона включают запрет на сбор и распространение личной информации без согласия, равный статус всех информационных технологий, защиту определенной информации и ответственность тех, кто хранит и защищает информацию. Государство ведет реестр запрещенных веб-сайтов, и владелец заблокированного веб-сайта может добиться его разблокировки, удалив незаконную информацию и уведомив Роскомнадзор.

14. Основное содержание **№ 152-ФЗ «О персональных данных».**

Этот закон регулирует работу с персональными данными – личными данными конкретных людей. Его обязаны соблюдать те, кто собирает и хранит эти данные. Например, компании, которые ведут базу клиентов или сотрудников.
Ключевые моменты закона:

1) Перед сбором и обработкой персональных данных нужно спрашивать согласие их владельца.
2) Для защиты информации закон обязывает собирать персональные данные только с конкретной целью.
3) Если вы собираете персональные данные, то обязаны держать их в секрете и защищать от посторонних.
4) Если владелец персональных данных потребует их удалить, вы обязаны сразу же это сделать.
5) Если вы работаете с персональными данными, то обязаны хранить и обрабатывать их в базах на территории Российской Федерации. При этом данные можно передавать за границу при соблюдении определенных условий, прописанных в законе – жесткого запрета на трансграничную передачу данных нет.

15. Основное содержание **№ 5485-1-ФЗ «О государственной тайне».**

Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ. Положения Закона обязательны для исполнения на территории РФ и за ее пределами органами представительной, исполнительной и судебной властей, МСУ, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами РФ, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства РФ о государственной тайне.
Под **государственной тайной** понимаются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.
Определены полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.
Самостоятельный раздел Закона закрепляет перечень сведений, которые могут быть отнесены к государственной тайне.
Засекречивание сведений и их носителей – это введение для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.
Определены сведения, не подлежащие засекречиванию (о чрезвычайных происшествиях и катастрофах, о состоянии экологии, здравоохранения,

санитарии, демографии, образования, культуры, сельского хозяйства, преступности и др.). Устанавливаются три степени секретности и соответствующие этим степеням грифы секретности для носителей сведений: «особой важности», «совершенно секретно» и «секретно». Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом РФ. Законом регламентирован и порядок рассекречивания сведений и их носителей – снятия ранее введенных ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям. Основаниями для рассекречивания сведений являются: взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну; изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Закреплены положения о распоряжения сведениями, составляющими государственную тайну.

Определены органы защиты государственной тайны. Допуск должностных лиц и граждан РФ к государственной тайне осуществляется в добровольном порядке. Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством РФ.

Устанавливается три формы допуска к государственной тайне: **к сведениям особой важности, совершенно секретным или секретным**. Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности. Определены основания для отказа в допуске к государственной тайне, условия прекращения допуска. Рассмотрены вопросы ограничения прав лиц, допущенных или ранее допускавшихся к государственной тайне, организации доступа к таким сведениям и ответственности за нарушение законодательства о государственной тайне. Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Координация работ по организации сертификации средств защиты информации возлагается на межведомственную комиссию по защите государственной тайны. За обеспечением защиты государственной тайны предусмотрены парламентский, межведомственный и ведомственный контроль, а также прокурорский надзор.

16. Основное содержание **№ 98-ФЗ «О коммерческой тайне».**

Федеральным законом регулируются отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее

конфиденциальности и предупреждением недобросовестной конкуренции. Действие Закона распространяется на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

Коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Устанавливается законодательное ограничение на отнесение информации к коммерческой тайне в интересах общества, государства и граждан. Так, режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении сведений **о численности, составе работников, системе оплаты труда, об условиях труда, показателях производственного травматизма и профессиональной заболеваемости, наличии свободных рабочих мест, а также задолженности работодателей по выплате заработной платы и по иным социальным выплатам.** Также устанавливается обязательность предоставления на безвозмездной

17. Основное содержание **№ 63-ФЗ «Об электронной подписи»**.
    Он расширяет сферу использования и допустимые виды электронных подписей (ЭП). **Выделяются 2 вида ЭП: простая и усиленная.** Последняя может быть квалифицированной либо неквалифицированной.
    Простая ЭП подтверждает, что данное электронное сообщение отправлено конкретным лицом.
    Усиленная неквалифицированная ЭП позволяет не только однозначно идентифицировать отправителя, но и подтвердить, что с момента подписания документа его никто не изменял.
    Сообщение с простой или неквалифицированной ЭП может быть приравнено к бумажному документу, подписанному собственноручно, если стороны заранее об этом договорились, а также в специально предусмотренных законом случаях.
    Усиленная квалифицированная ЭП дополнительно подтверждается сертификатом, выданным аккредитованным удостоверяющим центром. Сообщение с такой ЭП во всех случаях приравнивается к бумажному документу с собственноручной подписью.
    Уполномоченный в сфере ЭП орган определяет Правительство РФ. Он проводит аккредитацию удостоверяющих центров. Закреплены требования к удостоверяющему центру. Так, стоимость его чистых активов должна составлять не менее 1 млн руб. Еще одно условие – наличие в штате квалифицированных сотрудников. Максимальный срок аккредитации – 5 лет. Предусмотрены механизмы признания иностранных ЭП.

18. Основное содержание **№ 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».**

Он регулирует отношения в области **обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.** Определены основные принципы обеспечения безопасности, полномочия госорганов, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов. Закреплены понятия компьютерной атаки, компьютерного инцидента и др. Определен порядок функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы. Предусмотрены категорирование объектов; ведение реестра значимых объектов; оценка состояния защищенности; госконтроль; создание специальных систем безопасности

Основные понятия

1. **Информация** -

любые сведения (данные) независимо от формы их представления.

2. **Конфиденциальность информации** –*

состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право

3. **Целостность информации** -

состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

4. **Доступность информации** -

состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

5. **Информационная система** -

совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

6. **Защита информации** -

называется деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

7. **Информационная безопасность** -

это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

8. **Безопасность информации** -

это состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность

9. **Техническая защита информации** -

защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [5].

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, которые самостоятельно или в комплексе с другими средствами, реализуют следующие способы защиты:
- идентификацию (распознавание) и аутентификацию (проверку подлинности) субъектов (пользователей, процессов);
- разграничение доступа к ресурсам;
- регистрацию и анализ событий;
- криптографическое закрытие информации;
- резервирование ресурсов и компонентов систем обработки информации и др.

10. **Криптографическая защита информации** -
защита информации с помощью ее криптографического преобразования

11. **Комплексная система защиты информации (КСЗИ)** - это совокупность организационно-правовых и инженерно-технических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки, несанкционированного доступа и воздействия.