Лекция 2

21.09.2022

**ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ:**

1. Распространение информации - действие, направленное на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
2. Защита информации - принятие правовых, организационных и технических мер(направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, распространения, а также иных неправомерных действий в отношении такой информации), соблюдение конфиденциальности информации, информации ограниченного доступа и реализацию права на доступ к информации.
3. Защита информации от утечки - деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа и получение защищаемой информации разведками.
4. Защита информации от несанкционированного воздействия - деятельность, направленная на предотвращение, воздействие на защищаемую информацию с нарушением установленных прав на изменение информации, приводящих к ее искажению, уничтожению, блокированию доступа к информации.
5. Защита информации от непреднамеренного воздействия
6. Защита информации от несанкционированного доступа
7. Защита информации от разведки
8. Защита информации от агентурной разведки.
9. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и несанкционированного действия на информацию.

**ПОНЯТИЯ, СВЯЗАННЫЕ С ОРГАНИЗАЦИЕЙ ЗАЩИТЫ ИНФОРМАЦИИ:**

1. Организация защиты информации - содержание и порядок действий, направленных на обеспечение защиты информации.
2. Система зашиты информации - совокупность органов или исполнителей, используемой информации, также объектов защиты, организованной и работающей по правилам установленными соответствующими правовыми организационно-распорядительными и нормативными документами в области защиты информации.

**Лекция 3**

28.09.2022

**Основные принципы построения систем защиты:**

**Защищённость и обоснованность защиты**

Принцип законности и обоснованности предусматривает то, чо защищаемая информация по своему правовому статусу относится к информации, к которой требуется защита с соответствием законодательству.

**Системность**

Системный подход к защите информационной системы предполагает необходимость учёта всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов условий и факторов:

1. При всех видах информационной деятельности и информационного проявления
2. Во всех структурных элементах
3. При всех режимах функционирования
4. На всех этапах жизненного цикла
5. С учётом взаимодействия объекта защиты с внешней средой

**Комплексность**

Комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты.

**Непрерывная защита**

Защита информации непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизни информационной системы, начиная с самых ранних стадий проектирования.

**Разумная достаточность**

Подразумевается, что нужно выбрать такой уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемы.

**Гибкость**

Средства защиты должны обладать определенной гибкостью (свойством подстраиваться под изменения).

**Открытость алгоритмов и средств защиты**

Суть этого принципа состоит в том, что знания алгоритмов работы системы защиты не должны давать возможности ее преодоления даже разработчику защиты.

**Простота применения средств защиты**

Механизмы должны быть понятны и просты в использовании.

Концепция комплексной защиты информации

**Требования к комплексной защите:**

1. Разработка и доведение до уровня регулярного использования всех необходимых механизмов гарантированного обеспечения требуемого уровня защищённости информации
2. Существование механизмов практической реализации требуемого уровня защищённости
3. Наличие средств рациональной реализации всех необходимых мероприятий по защите информации на базе достигнутого уровня развития науки и техники
4. Разработка способов оптимальной организации и обеспечения проведения всех мероприятий по защите а процессе обработки информации

**Задачи защиты информации:**

1. введение избыточности элементов системы;
2. резервирование элементов системы;
3. регулирование доступа к элементам системы
4. регулирование использования элементов системы;
5. маскировка информации;
6. контроль элементов системы;
7. регистрация сведений;
8. уничтожения информации;
9. сигнализация
10. реагирование

**Средства реализации комплексной защиты информации:**

**Технические средства**

1. Аппаратные - устройства, встраиваемые в телекоммуникационную аппаратуру
2. Физические (решетки на окнах замки на дверях, сигнализация и т.д.)

**Программные средства защиты**

Представляют собой программное обеспечение, предназначенное для выполнения функции защиты информации.

**Организационные средства защиты**

Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры и телекоммуникаций для обеспечения защиты информации.

**Законодательные средства защиты**

Определяется законодательными актами, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушения этих правил.

**Морально-этические средства защиты**

Необязательные. Имеют рекомендательный характер.

Лекция 4

19.10.2022

**Уровни представления информации:**

**Уровень носителей информации**

1. признак информации (форма, размер, структура, свойство)
2. -симатическая (не зависит от вида носителей
3. Вещественные носители - все физические носители(диски, бумага и т.д.)
4. Энергетические носители - это электромагнитные акустические поля

\*Уровень средств взаимодействия с носителем

Для защиты на втором уровне нужно следить за исправностью устройств считывания информации, за отсутствием технических средств несанкционированного доступа к информации

\*Логический уровень

Уровень может быть представлен в виде логических дисков, каталогов, файлов, на удаление информации на логическом уровне не всегда удаляет информацию с нижних уровней.

\*Синтаксический уровень

Данный уровень связан с кодированием.

**В зависимости от цели различаются следующие виды кодирования**

1. с целью устранения избыточности
2. с целью устранения ошибок
3. с целью недоступности информации

\*Семантический уровень:

Данный уровень связан со смыслом е передаваемой информации.

**Основные свойства защищаемой информации:**

1. Ценность
2. Секретность (характеристиа, обеспечивается способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочия на нее)
3. Целостность
4. Доступность
5. Рассеяние (ценная часть смешивается с менее ценной, с целью ее маскировки) ;
6. Сжатие(архивирование)

\_

Служебная тайна.

Служебная тайна содержит информацию ограниченного содержания, к которой относятся не секретные сведения, касающиеся деятельности организации, ограничение на распоряжение которых вызвано служебной необходимостью.

**Разновидности служебной тайны**

1. судебно-следсвенные
2. тайна гос.банков
3. производственная тайна

**Профессиональная тайна.**

Профессиональная тайна - инструмент защиты персональных данных у граждан.

1. Тайна страхования
2. Тайна налоговых органов
3. Тайна завещания
4. Тайна голосования

Коммерческая тайна - относятся секреты предприятия.

**Лекция 5**

26.10.2022

**Угрозы информационной безопасности:**

1. Внешние
2. Внутренние

Угроза - фактор, стремящийся нарушить работу системы.

**Классификация угроз И.Б.:**

1. -нарушение конфиденциальности (лицо не располагающее полномочиями к информации получает доступ, в том случае если информация становится известной лицу, нерасполагающему полномочиями доступа к ней)
2. нарушение целостности (реализуется при несанкционированном изменении информации, хранящейся в информационной системе или передаваемой из одной системы в другую)
3. нарушение доступности (реализуется когда в результате преднамеренных действий, принимаемых злоумышленником, блокируется доступ к ресурсу вычислительной системы)

**Основные направления и методы реализации угроз:**

1. обращение к объектам доступа
2. создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты
3. модификация средств защиты, позволяющая реализовать угрозу информационной безопасности
4. Внедрение в техническое средство программных или технических механизмов, разрушающих функции системы

**Основные методы реализации угроз И.Б.:**

1. определние злоумышленником типа и параметров носителя информации
2. информация в программно-аппаратной среде
3. получение злоумышленником данных о применяемых системах защиты
4. хищение или копирование машинных носителей информации, содержащих конфиденциальные данные
5. несанкционированное копирование программного обеспечения
6. уничтожение носителя информации
7. заражение программными вирусами

**Неформальная модель нарушителя:**

- Внутренние

- Внешние

**Нарушения:**

-Безответственность

-Самоутверждение

-Корыстный интерес

**Классификация нарушителей:**

- По уровню знаний о системе

- По уровню возможностей

- По времени действий

- По месту действий

**Лекция 6**

16.11.2022

Построение систем защиты от угрозы нарушения конфиденциальности.

Определение и основные способы несанкционированного доступа.

Для предназначенного НСД используются как общедоступные, так и скрытые способы и средства.

**Такими средствами являются**

1. инициативное сотрудничество (предательство)
2. склонение к сотрудничеству (подкуп, шантаж)
3. подслушивание переговоров самыми различными путями
4. негласное ознакомление со сведениями, составляющими тайну
5. хищение, копирование, подделка, уничтожение
6. незаконное подключение к каналам и линиям связи и передача данных
7. перехват (акустический или радиоперехват, в том числе и за счёт побочных электромагнитных излучений и наводок)
8. визуальное наблюдение, фотография
9. сбор и аналитическая обработка детальной информации или производственных отходов

**К основным способам НСД информационных системах относятся**

1. непосредственное обращение к объектам доступа
2. создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты
3. модификация средств защиты, позволяющих осуществить НСД
4. внедрение в технические средства информационной системы программных или технических механизмов, нарушающих предполагаемую структуру и функции системы и позволяющих осуществить НСД

**Методы защиты от НСД**

1. организационные (меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующими информационную систему)
2. технологические (реализуются на базе аппаратных средств, как пример - охранная сигнализация)
3. правовые (за исполнением правовых актов общегосударственного значение)
4. финансовые (специальная доплата при работе защищаемой информации, доклад при работе защищаемой информации, а также вычиты и штрафы)
5. морально- этические (необязательная недействующая фигня)
6. инженерно-технические (нарушение конфиденциальности происходит в результате утечки информации, а защита информации от утечки - это деятельность, направленная на предотвращение неконтролируемого доступа к информации, в результате ее разглашения, несанкционированного доступа к информации получение защищаемой информации разведками)

**Причинами утечки могут являться**

1. несоблюдение персональных норм
2. ошибки в проектировании
3. разведки

**Каналы утечки информации**

1. акустические
2. электромагнитные
3. визуально-оптические
4. материально-вещественные
5. информационные

**Группы методов аутентификации**

1. индивидуальног объектоа заданного типа (удостоверения, пропуска и т.д.)
2. индивидуальныз биометрических характеристик(отпечатки пальцев, сетчатка глаза)
3. знаний, известных только пользователю и проверяющей стороне информации (пароль)

**Криптология**

1. криптография (занимается поиском и исследованием математических методов преобразования информации)
2. криптоанализ(обратное криптографии,исследование расшифровки информации БЕЗ знания ключа)

**Криптографические методы**

1. передача конфиденциальной информации по каналам связи
2. обеспечение достоверности и целостности информации
3. установление подлинности передаваемых сообщений
4. хранение информации (документов, бах данных) на носителях в зашифрованном виде;
5. выработка информации для идентификации и аутентификации субъектов, пользователей и устройств
6. выработка информации, используемой для защиты аутентифицирующих элементов защищаемой системы

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текста.

Зашифрованный текст и ключ ----> криптосистема ----> открытый текст

В симметричных криптосистемах для шифрования и дешифрования используется один и тот же ключ.

В асимметричных: для шифрования - открытый ключ, а для дешифрования - закрытый ключ.

**К средствам криптографической защиты информации относятся**

1. аппаратные
2. программно-аппаратные
3. программные средства

**Основные причины нарушения безопасности информации при ее обработке СКЗИ:**

1. утечка информации по техническим каналам
2. неисправности в работе СКЗИ
3. работа совместно с другими программами: непреднамеренное и преднамеренное влияние(криптовирусы)
4. воздействие человека

Правовая сторона разработки и использования СКЗИ регламентируется указом Президента РФ от 03.04.95 №334 с учётом принятых ранее законодательных и нормативных актов РФ.

Дополнительной учитываемой законодательной базой являются законы:

1. "О федеральных органах правительственной связи и информации"
2. "О государственной тайне "
3. "Об информации, информационных технологиях и о защите информации"
4. "О сертификации продукции и услуг"

**Лекция 7**

19.10.2022

Уровни представления информации

**Уровень носителей информации**

1. признак информации (форма, размер, структура, свойство)
2. симатическая (не зависит от вида носителей
3. Вещественные носители - все физические носители(диски, бумага и т.д.)
4. Энергетические носители - это электромагнитные акустические поля

**Уровень средств взаимодействия с носителем**

Для защиты на втором уровне нужно следить за исправностью устройств считывания информации, за отсутствием технических средств несанкционированного доступа к информации

**Логический уровень**

Уровень может быть представлен в виде логических дисков, каталогов, файлов, на удаление информации на логическом уровне не всегда удаляет информацию с нижних уровней.

**Синтаксический уровень**

Данный уровень связан с кодированием.

В зависимости от цели различаются следующие виды кодирования

1. с целью устранения избыточности
2. с целью устранения ошибок
3. с целью недоступности информации

**Семантический уровень**

Данный уровень связан со смыслом е передаваемой информации.

**Основные свойства защищаемой информации**

1. Ценность
2. Секретность (характеристика, обеспечивается способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочия на нее)
3. Целостность
4. Доступность
5. Рассеяние (ценная часть смешивается с менее ценной, с целью ее маскировки)
6. Сжатие(архивирование)

\_

Служебная тайна.

Служебная тайна содержит информацию ограниченного содержания, к которой относятся не секретные сведения, касающиеся деятельности организации, ограничение на распоряжение которых вызвано служебной необходимостью.

**Разновидности служебной тайны**

1. Судебно-следсвенные
2. тайна государственных банков
3. производственная тайна
4. профессиональная тайна
5. профессиональная тайна - инструмент защиты персональных данных у граждан
6. тайна страхования
7. тайна налоговых органов
8. тайна завещания
9. тайна голосования

К коммерческой тайне - относятся секреты предприятия.

**Лекция 8**

30.11.2022

Информационные войны и информационное противоборство

Развитие информационных технологий привело к таким видам борьбы, как информационная война, техническая и информационно-психологическая война

**Информационная война** - информационное воздействие друг на друга с целью получения выигрыша материальной, военной, политической сфер

**Информационные войны**

1. Персональные - связана с нарушением личной информационной неприкосновенности
2. Корпоративные - соперничество между корпорациями
3. Глобальные - ущерб наносится информационным ресурсам

**Глобальная информационную войну можно разделить на**

1. воздействие на индивидуальное, групповое, массовое сознание с использованием средств массовой информации
2. воздействие на системы принятия решений политической, экономической, военной, научно-технической и социальной сфер
3. воздействие на информационные системы с целью управления и блокирования обрабатываемой информации

**Информационная война**

1. информационно-техническая
2. информационно-психологическая

**Сферы ведения информационной войны**

1. политическая
2. финансово-экономическая
3. дипломатическая
4. военная

**Информационно-техническая война**

1. командно-управленческая
2. разведывательная
3. электронная
4. экономическая
5. кибер-война
6. хакерские войны

**Радиоэлектронная война** - вид информационной борьбы, который нарушает или затрудняет средств функционирования электронных средств противника путем излучения, отражения электромагнитных сигналов, акустических и инфракрасных сигналов

**Информационно-психологическая война** - информационное воздействие на психику человека, сознание людей.