ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.1.28 Техническая защита информации

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Форма обучения очная

СОДЕРЖАНИЕ

Лабораторная работа № 6-7 Оценка защищенности выделенного помещения от утечки информации по акустическому и виброакустическому каналам.

Лабораторная работа № 8-9 Изучение средств обеспечения конфиденциальности данных.

3. Методические указания по проведению практических занятий

Практическое занятие № ПЗ-1 Наводки электромагнитных излучений ТСПИ. Параметрический канал утечки информации.

Практическое занятие № ПЗ-2 Технические каналы утечки информации при передаче ее по каналам связи.

Практическое занятие № ПЗ-3 Электрические линии связи. Средства передачи электрических сигналов.

Практическое занятие № ПЗ-4 Средства передачи электрических сигналов. Каналы утечки информации за счет паразитных связей.

Практическое занятие № ПЗ-5 Опасные сигналы и их источники. Электрические каналы утечки информации.

Практическое занятие № ПЗ-6 Электрические каналы утечки информации. Контроль и прослушивание телефонных каналов связи.

Практическое занятие № ПЗ-7 Контроль и прослушивание телефонных каналов связи. Электромагнитные каналы утечки информации.

Практическое занятие № ПЗ-8 Индукционный канал утечки информации. Технические каналы утечки речевой информации.

Практическое занятие № ПЗ-9 Краткие сведения по акустике. Звуковое поле.

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1 (2 часа).
Тема: «Термины и определения в области технической защиты информации.»
1.1.1 Вопросы лекции:
1. Объект информатизации, выделенное помещение, основные технические средства и системы
2. Вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации
3. Средство разведки, специальное техническое средство негласного получения информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

1.1.2 Краткое содержание вопросов:

1. Объект информатизации, выделенное помещение, основные технические средства и системы

Объект информатизации - совокупность средств информатизации вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи защищаемой информации, а также выделенные помещения.

Выделенное помещение (ВП) - специальное помещение, предназначенное для проведения собраний, совещаний, бесед и других мероприятий речевого характера по секретным или конфиденциальным вопросам.
Мероприятия речевого характера могут проводиться в выделенных помещениях с использованием технических средств обработки речевой информации (ТСОИ) и без них.

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной (секретной) информации
К ОТСС могут относиться средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных), технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической видео-, смысловой и буквенно-цифровой информации) используемые для обработки конфиденциальной (секретной) информации.

2. Вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в выделенных помещениях.

3. Средство разведки, специальное техническое средство негласного получения информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации

Средство контроля эффективности защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для контроля эффективности защиты информации

Доступность информации - состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия

Доступ к информации (доступ) - ознакомление с информацией, её обработка, в частности копирование, модификация или уничтожение информации.

Целостность информации - состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения

1. 2 Лекция № 2 (2 часа).
Тема: «Классификация технических каналов утечки информации.»
1.2.1 Вопросы лекции:
1.Место технической защиты информации в государственной системе защиты информации в Российской Федерации.
2.Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации). Виды технических каналов утечки информации.

1.2.2 Краткое содержание вопросов:

1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации.

Государственная система защиты информации представляет собой совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации. Так же является составной частью системы обеспечения национальной безопасности Российской Федерации и призвана защищать безопасность государства от внешних и внутренних угроз в информационной сфере.

Организацию деятельности государственной системы технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной Государственной системой осуществляет ФСТЭК России.

Государственная система защиты информации как система более сложная, включает в себя подсистемы лицензирования деятельности предприятий в области защиты информации, сертификации средств защиты информации и аттестации объектов информатизацип требованиям безопасности информации.

Выше перечисленные подсистемы представляют в совокупности деятельность следующих органов:

- Федеральная служба технического и экспортного контроля (ФСТЭК России) и ее территориальные органы (региональные управления в субъектах Российской Федерации)
- Федеральные органы исполнительной власти, другие органы и организации Российской Федерации, руководящие работники которых входят в состав коллегии

ФСТЭК России по должности (Минюст, Минобороны, МЧС, МВД, МИД, Минпромэнерго, Минэкономразвития, Минприроды, ФСО, ФСБ, СВР, ГУСП, РАН, ЦБР)

- Структурные подразделения по защите информации федеральных органов исполнительной власти, других органов государственной власти и организаций Российской Федерации
- Предприятия, проводящие работы с использованием сведений, отнесенных к информации ограниченного доступа, и их подразделения по защите информации
- Научно-исследовательские организации по проблемам защиты информации
- Организации-разработчики средств защиты информации, защищенных технических средств и средств контроля эффективности защиты информации
- Предприятия, оказывающие услуги в области защиты информации
- Организации Федерального агентства по техническому регулированию и метрологии (бывшего Госстандарта России), выполняющие работы по стандартизации в области защиты информации
- Органы системы лицензирования деятельности в области защиты информации
- Органы системы сертификации средств защиты информации
- Органы системы аттестации объектов защиты по требованиям безопасности информации

2.Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации). Виды технических каналов утечки информации.

Проблема угрозы безопасности этой информации, под которой понимается явление, действие или процесс, результатом которого могут быть утечка, уничтожение, модифицирование информации или блокирование доступа к ней. Утечка информации приводит к разглашению информации; - утечке по техническим каналам; - несанкционированному доступу к информации. Техническая защиты информации – это деятельность, направленная на обеспечение некриптографическими методами безопасности информации подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Цели технической защиты информации – предотвращение утечки информации по техническим каналам, предотвращение несанкционированного доступа и воздействия на информацию в информационных системах. Объектами технической защиты информации являются: - защищаемые автоматизированные информационные системы; - защищаемые информационные ресурсы; - защищаемые информационные технологии.

Объект защиты – это информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту.

Основные задачи ТЗИ: - защита информации от утечки; - защита информации от несанкционированного воздействия; - защита информации от непреднамеренного воздействия; - оценка соответствия объекта защиты требованиям нормативно методических документов по защите информации.

Нормативные правовые акты по технической защите информации – это федеральные законы, указы и распоряжения Президента РФ, Постановления правительства РФ. Нормативно-правовые акты являются основным источником права в Государстве. Юридическая сила нормативно-правовых актов является наиболее существенным признаком их классификации. Она определяет их место и значимость в общей системе государственного нормативного регулирования. Закон – это главный нормативно-правовой акт.

1. 3 Лекция № 3-4 (4 часа).
Тема: «Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.»
1.3.1 Вопросы лекции:
1. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений.
2. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений.
3. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ.
4. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.

1.3.2 Краткое содержание вопросов:

1. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений.

В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения, а именно: вследствие протекания переменного электрического тока;

-на частотах работы высокочастотных генераторов;

- возникающие вследствие паразитной генерации в элементах.

Источниками ПЭМИ могут являться:

-задающие генераторы,

-генераторы тактовой частоты

- генераторы стирания и подмагничивания магнитофонов

- гетеродины радиоприемных и телевизионных устройств

- генераторы измерительных приборов.

Наиболее опасным является вывод информации на экран монитора.

ПЭМИ возникают при следующих режимах обработки информации СВТ: вывод информации на экран монитора, ввод данных с клавиатуры, запись информации на накопители, чтение информации с накопителей, передача данных в каналы связи, вывод данных на периферийные печатные устройства – принтеры, плоттеры.

2. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений.

Причинами возникновения электрических каналов утечки информации являются наводки информационных сигналов, и могут возникать:

- в линиях электропитания ТСПИ;

- в линиях электропитания и соединительных линиях ВТСС;

- в цепях заземления ТСПИ и ВТСС

- в посторонних проводниках.

Перехват наведенных сигналов с линий электропитания и заземления ТСПИ возможен в случае, если трансформаторная подстанция или заземлитель находятся за пределами контролируемой зоны объекта.

3. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ.

Одним из активных способов перехвата информации, обрабатываемой ТСПИ, является способ «высокочастотного облучения», при котором ТСПИ облучается мощным высокочастотным гармоническим сигналом.

Суть возникновения канала утечки информации заключается в следующем. ТСПИ облучается непрерывным высокочастотным электромагнитным излучением или высокочастотными радиоимпульсами. При взаимодействии облучающего электромагнитного поля с элементами ТСПИ в их цепях наводится высокочастотное колебание, выступающее в роли вторичного несущего сигнала. Наведенное высокочастотное колебание, протекая по цепям ТСПИ, являющимися в данном случае случайными антеннами, переизлучается по законам электромагнитной индукции в окружающее пространство. В том случае, когда вторичное несущее колебание модулируется информационным сигналом, например компьютерными данными, циркулирующими в СВТ, или низкочастотными сигналами в системах передачи информации, возникает опасный сигнал и, следовательно, канал утечки информации.

При переизлучении параметры сигналов изменяются, поэтому данный канал утечки информации часто называют параметрическим.

4. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.

Для перехвата информации, обрабатываемой ТСПИ, также возможно использование негласных электронных устройств перехвата информации (аппаратных закладных устройств), скрытно внедряемых в технические средства и системы.

Аппаратные закладные устройства представляют собой миниатюрные передатчики, излучение задающих генераторов которых модулируется информационным сигналом.

По виду перехватываемой информации аппаратные закладки можно разделить на:

- аппаратные закладки для перехвата изображений, выводимых на экран

- аппаратные закладки для перехвата информации, вводимой с клави

ту-

- аппаратные закладки для перехвата информации, выводимой на периферийные устройства (например, принтер).

- аппаратные закладки для перехвата информации, записываемой на жесткий диск ПЭВМ (HDD);

- аппаратные закладки для перехвата информации, записываемой на

внешние накопители (flash память, CD, DVD, USB-накопители и т.п.).

Аппаратная закладка, как правило, состоит из блока перехвата, блока передачи информации, блока дистанционного управления и блока питания.

1. 4 Лекция № 5 (2 часа).
Тема: «Акустические (речевые) каналы утечки информации.»
1.4.1 Вопросы лекции:
1. Структура акустического канала утечки информации.

2. Общая характеристика и классификация технических каналов утечки акустической информации.
3. Акустовибрационные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики.

1.4.2 Краткое содержание вопросов:

1. Структура акустического канала утечки информации.

Структура ТКУИ: Источник источник сигнала среда передачи приемник злоумышленник.

В качестве источника сигнала могут быть: - объект наблюдения, отражающий электромагнитные и акустические волны; - объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах; - передатчик функционального канала связи; - закладное устройство; - источник опасного сигнала; - источник акустических волн, модулированных информацией.

Передатчик выполняет следующие функции: - создает поля или электрический ток, которые переносят информацию;- производит запись информации на носитель; - усиливает мощность сигнала (носителя с информацией); - обеспечивает передачу сигнала в среду распространения в заданном секторе пространства.

Среда распространения носителя – часть пространства, в которой перемещается носитель.

Основными параметрами, среды распространения, являются: - физические препятствия для субъектов и материальных тел; - мера ослабления сигнала на единицу длины; - частотная характеристика;- вид и мощность п

мех для сигнала. **Классификация ТКУИ**:

По физичекой природе носителя: оптические, радиоэлектронные, акустические, материально - вещественные.

По информативности: информативные, малоинформативные, неинформативные

По времени функционирования: постоянные, эпизодические, случайные.

По структуре: одноканальные, составные

2. Общая характеристика и классификация технических каналов утечки акустической информации.

Радиоэлектронный канал – это канал передачи, носителем информации в котором является электрический ток или электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.
Структура радиоэлектронного канала утечки информации в общем случае включает источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала.
Источники сигналов могут быть четырех видов:

Передатчики функциональных каналов связи, Источники опасных сигналов, Объекты, отражающие электромагнитные волны в радиодиапазоне,

В зависимости от способа перехвата информации различают два вида радиэлектронных каналов утечки информации:

- Каналы утечки, способствующие перехвату информации, передаваемой функциональным источником сигнала.

- Каналы утечки, имеющие собственный набор элементов: передатчик сигналов, среду распространения и приемник сигналов.

3. Акустовибрационные каналы утечки речевой информации.

Средства акустической разведки и их технические характеристики.В акустовибрационных каналах утечки речевой информации информативным сигналом

являются вибрационные колебания, возбуждаемые в строительных констукциях служебных помещений и в инженерных коммуникациях акустическим сигналом. Для перехвата речевой информации по акустовибрационным каналам используются электронные стетоскопы и электронные устройства перехвата речевой информации с датчиками контактного типа.

1. 5 Лекция № 6 (2 часа).
Тема: «Оптические каналы утечки информации»
1.5.1 Вопросы лекции:
1. Особенности радиоэлектронных каналов утечки информации.
2. Виды и структура радиоэлектронных каналов утечки информации.
3. Направляющие линии связи, их характеристики.
1.5.2 Краткое содержание вопросов:

1.Особенности радиоэлектронных каналов утечки информации.

Незащищенные средства передачи, приема и обработки информации, работающие от электрического тока образуют радиоэлектронный канал утечки информации. В радиоэлектронном канале передачи носителем информации является электрический ток и электрическое поле с частотами колебаний от звукового диапазона до десятков ГГц.

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

-независимость функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;

-высокая достоверность добывания информации, особенно при перехвате ее

В функциональных каналах связи (за исключением случаев дезинформации);

-большой объем добываемой информации;

-оперативность получения информации вплоть до реального масштаба

времени;

-скрытность перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронном канале производится перехват радио и электрических сигналов, радиолокационное и радиотепловое наблюдение. Следовательно, в рамках этого канала утечки добывается семантическая информация, видовые и сигнальные демаскирующие признаки. Радиоэлектронные каналы утечки информации используют радио, радиотехническая, радиолокационная и радиотепловая разведка.

Структура радиоэлектронного канала утечки информации в общем случае включает источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала.

2.Виды и структура радиоэлектронных каналов утечки информации.

В радиоэлектронных каналах утечки информации источники сигналов могут быть четырех видов:

-передатчики функциональных каналов связи;

-источники опасных сигналов;

-объекты, отражающие электромагнитные волны в радиодиапазоне;

-объекты, излучающие собственные (тепловые) радиоволны в радиодиапазоне. Средой распространения радиоэлектронного канала утечки информации являются атмосфера безвоздушное пространство и направляющие – электрические провода различных типов и волноводы. Носитель в виде электрического тока распространяется по проводам, а электромагнитное поле – в атмосфере, в безвоздушном пространстве или по

направляющим – волноводам. В приемнике производится выделение (селекция) носителя с интересующей получателя информацией по частоте, усиление выделенного слабого сигнала и съем с него информации – демодуляции.

При перехвате сигналов функциональных каналов связи передатчики этих каналов являются одновременно источниками радиоэлектронных каналов утечки информации. В общем случае направление распространения электромагнитной волны от передатчика к санкционированному получателю и злоумышленнику отличаются. В функциональных каналах связи максимум излучения энергии электромагнитной волны ориентируют в направлении расположения приемника санкционированного получателя. Поэтому мощность источника сигналов радиоэлектронного канала утечки информации, как правило, существенно меньше мощности излучения в функциональном канале связи. В зависимости от способа перехвата информации различают два вида радиоэлектронного канала утечки информации.

В канале утечки первого вида производится перехват информации, передаваемой по функциональному каналу связи. С этой целью приемник сигнала канала утечки информации настраивается на параметры сигнала функционального радиоканала или подключается (контактно или дистанционно) к проводам соответствующего функционального канала. Такой канал утечки имеет общий с функциональным каналом источник сигналов – передатчик. Так как места расположения приемников функционального канала и канала утечки информации в общем случае не совпадают, то среды распространения сигналов в них от общего передатчика различные или совпадают, например, до места подключения приемника к проводам телефонной сети.

Радиоэлектронный канала утечки второго вида имеет собственный набор элементов: передатчик сигналов, среду распространения и приемник сигналов. Передатчик этого канала утечки информации образуется случайно (без участия источника или получателя информации) или специально устанавливается в помещении злоумышленником. В качестве такого передатчика применяются источники опасных сигналов и закладные устройства. Опасные сигналы, как отмечалось раннее, возникают на базе акустоэлектрических преобразователей, побочных низкочастотных и высокочастотных полей, паразитных связей и наводок в проводах и элементах радиосредств. Предпосылки для них создаются в результате конструктивных недоработок при разработке радиоэлектронного средства, объективных физических процессов в их элементах, изменениях параметров в них из – за старения или нарушений правил эксплуатации, не учете полей вокруг средств или токонесущих проводов при их прокладке в здании и т. д.

3.Направляющие линии связи, их характеристики.

Наиболее широко применяются сигналы, ширина спектра которых соответствует ширине спектра стандартного телефонного канала. Такие сигналы передают речевую информацию с помощью телефонных аппаратов и распространяются по **направляющим линиям связи**, связывающих абонентов как внутри организации, так внутри населенного пункта, города, страны, земного шара в целом.

Более широко применяются кабельные линии связи. Кабельные линии связи получили доминирующее развитие при организации объектовой, городской и междугородной телефонной связи. Они составляют 65% телефонных линий России. Кабели бывают симметричными и коаксиальными.

Если обе жилы цепи, образованного кабелем, выполнены из провода одинакового диаметра, имеют одинаковую изоляцию и расположены так, что между ними можно провести плоскость симметрии, то кабель называется симметричным. Если же оба

проводника цепи выполнены в форме соосных цилиндров, в поперечном сечении имеют форму концентрических окружностей, то такой кабель – коаксиальный.

1. 6 Лекция № 7 (2 часа).
Тема: «Радиоэлектронные каналы утечки информации.»
1.6.1 Вопросы лекции:
1. Структура материально-вещественного канала утечки информации и характеристики ее элементов.
2. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде.
3. Особенности утечки информации о радиоактивных веществах.

1.6.2 Краткое содержание вопросов:

1.Структура материально-вещественного канала утечки информации и характеристики ее элементов.

Основным и наиболее мощным внешним источником света, освещающим объекты наблюдения в дневное время, является Солнце. При температуре поверхности около 6000^{o} С Солнце излучает огромное количество энергии в достаточно широкой полосе – от ультрафиолетового до инфракрасного (0,17 – 4 мкм). Максимум солнечного излучения приходиться на 0,47 мкм, в ультрафиолетовой части оно резко убывает, в инфракрасной области зависимость уровня излучения от длины волны регистрируется в виде широкой и пологой кривой. Освещенность в дневное время земной поверхности Солнцем составляет в зависимости от его высоты, облачности атмосферы 10^{1}-10^{5}лк. С движением Солнца к горизонту Земли, когда зенитное расстояние между ними достигает максимума, освещенность Солнцем уменьшается до 10лк. При этом изменяется спектр солнечного света. Так как при прохождении толщи атмосферы синие и фиолетовые лучи ослабляются сильнее, чем оранжевые и красные, максимум излучения Солнца смещается в красную область цвета. С заходом Солнца за горизонт и наступлением сумерек освещенность убывает вплоть до наступления астрономических сумерек , за которым следует наиболее темное время суток – ночь. Освещенность в лунную ночь при безоблачном небе, когда так называемую естественную ночную освещенность (ЕНО) создает отраженный от Луны солнечный свет, составляет около 0,3 лк. Величина ЕНО света Луны в течение месяца меняется приблизительно в 100 раз в зависимости от взаимного расположения Луны, Солнца и Земли. Лунный месяц разделяется по уровню освещенности на четыре части, каждая длительностью около недели.

2.Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде.

Способы защиты демаскирующих веществ предусматривают применение мер, обеспечивающих уменьшение их концентрации до значений, исключающих определение злоумышленниками структуры и свойств демаскирующих веществ путем физического и химического анализа. Основные направления снижения концентрации демаскирующих веществ - внедрение безотходных или малоотходных технологий, а также глубокая очистка отходов и выбросов. Наиболее экономичным направлением защиты демаскирующих веществ в отходах - использование отходов в качестве вторичного сырья для создания иной продукции на этом же предприятии. Острота проблемы защиты возрастает, если промежуточные продукты с демаскирующими веществами не находят применение на одном предприятии. Для продажи их в качестве вторичного сырья, а также выброса на свалку, в водоемы или атмосферу отходы в интересах защиты информации надо очистить от демаскирующих веществ, т. е. уменьшить концентрацию демаскирующих веществ до допустимых значений. Выбор метода и способа очистки

отходов от демаскирующих веществ зависит, прежде всего, от видов (твердое, жидкое, газообразное) демаскирующих веществ и других веществ (примесей) в отходах. В качестве основных методов очистки отходов от демаскирующих веществ применяются методы механической очистки (фильтрация), нагрев, охлаждение и химические реакции. Фильтрация демаскирующих веществ осуществляется в аппаратах объемного улавливания (в циклонах, электрических фильтрах и др.), в результате абсорбции и адсорбции (поглощения всем объемом и поверхностью вещества соответственно), центрифугирования, промывки, разделения по удельной плотности, магнитным свойствам и т. д.При нагревании очистка отходов от демаскирующих веществ происходит путем пиролиза (расщепления органических веществ на более простые), крекинга (разложения нефтепродуктов), испарения, дегазификации, выпарки, сушки, прокалки, отгонки, сжигания и др. процессов, в результате которых удается отделить демаскирующее вещество от иных примесей или превратить его в вещество, информация о которых не подлежит защите.

При охлаждении отходов для выделения демаскирующих веществ используются процессы конденсации газообразных веществ, вымораживания жидкостей и др.Выделение демаскирующих веществ или превращение их в нейтральные, информация о которых не защищается, возможно также путем воздействия на отходы веществами, которые вступают с отходами в химические реакции. Отходы, очистка от демаскирующих признаков которых указанными методами невозможна или экономически нецелесообразна, подлежат захоронению. Выделенные демаскирующие вещества собираются в соответствующие емкости и подвергаются последующей обработке для нейтрализации или захоронению. Неиспользуемые радиоактивные вещества не могут быть нейтрализованы и подлежат захоронению в специальных могильниках.

3.Особенности утечки информации о радиоактивных веществах.

Задача защиты признаковой информации решается, прежде всего, путем предотвращения обнаружения и распознавания объектов, содержащих эти признаки. Среди множества признаков, присущих конкретному объекту, существуют признаки, которые позволяют обнаруживать его среди других похожих объектов и распознать его принадлежность, назначение, функции, свойства, особенности и характеристики. Признаки, позволяющие отличить один объект от другого, называются демаскирующими. Демаскирующие признаки объекта составляют часть его признаков, а значения их отличаются от значений соответствующих признаков других объектов. Совпадающие значения признаков не относятся к демаскирующим. Например, признак “рост человека” без указания его значения не является демаскирующим, так как он относится ко всем людям.

1. 7 Лекция № 8-9 (4 часа).
Тема: «Материально-вещественные каналы утечки информации.»
1.7.1 Вопросы лекции:

1. Классификация способов и средств защиты объектов информатизации.
2. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств.
3. Требования к системам электропитания и заземления основных технических средств и систем.

1.7.2 Краткое содержание вопросов:

1. 8 Лекция № 10-11 (4 часа).
Тема: «Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.»
1.8.1 Вопросы лекции:

1. Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.
2. Способы и средства защиты вспомогательных технических средств и систем.
3. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

1.8.2 Краткое содержание вопросов:

1.Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.

Защита информации от утечки по техническим каналам достигается проектно-архитектурными решениями, проведением организационных и технических мероприятий, а также выявлением портативных электронных устройств перехвата информации (закладных устройств).

Организационное мероприятие – это мероприятие по защите информации, проведение которого не требует применения специально разработанных технических средств.

К основным организационным и режимным мероприятиям относятся:

- привлечение к проведению работ по защите информации организаций, имеющих лицензию на деятельность в области защиты информации, выданную соответствующими органами;
- категорирование и аттестация объектов ТСПИ и выделенных для проведения закрытых мероприятий помещений (далее выделенных помещений) по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;
- использование на объекте сертифицированных ТСПИ и ВТСС;
- установление контролируемой зоны вокруг объекта;
- привлечение к работам по строительству, реконструкции объектов ТСПИ, монтажу аппаратуры организаций, имеющих лицензию на деятельность в области защиты информации по соответствующим пунктам;
- организация контроля и ограничение доступа на объекты ТСПИ и в выделенные помещения;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- отключение на период закрытых мероприятий технических средств, имеющих элементы, выполняющие роль электроакустических преобразователей, от линий связи и т.д.

Техническое мероприятие – это мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений.

Технические мероприятия направлены на закрытие каналов утечки информации путем ослабления уровня информационных сигналов или уменьшением отношения сигнал/шум в местах возможного размещения портативных средств разведки или их датчиков до величин, обеспечивающих невозможность выделения информационного

сигнала средством разведки, и проводятся с использованием активных и пассивных средств.

2.Способы и средства защиты вспомогательных технических средств и систем.

К наиболее широко применяемым пассивным способам защиты телефонных аппаратов и линий относятся:

- ограничение опасных сигналов;
- фильтрация опасных сигналов;
- применение буферных устройств;
- отключение преобразователей (источников) опасных сигналов.

Согласно закону Ома диоды имеют большое сопротивление (сотни кОм) для токов малой амплитуды и малое сопротивление (единицы Ом и менее) – для токов большой амплитуды (полезных сигналов), что исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияние на прохождение через диоды полезных сигналов.

3.Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

Мероприятия технической защиты проводятся с применением защитных способов и средств.

К пассивным техническим способам защиты относят [8]:

- установку систем ограничения и контроля доступа на объектах размещения ТСПИ и выделенных помещениях;
- экранирование ТСПИ и соединительных линий средств;
- заземление ТСПИ и экранов соединительных линий приборов;
- звукоизоляция выделенных помещений;
- встраивание в вспомогательные технические средства и системы (ВТСС), обладающие «микрофонным» эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров;
- ввод автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ;
- монтаж в цепях электропитания ТСПИ, а также в электросетях выделенных помещений помехоподавляющих фильтров;

К техническим мероприятиям с использованием активных способов защиты относят [8]:

- пространственное зашумление, создаваемое генераторами электромагнитного шума;
- постановку прицельных помех, генерируемых на рабочих частотах радиоканалов подслушивающих устройств специальными передатчиками;
- постановку акустических и вибрационных помех, генерируемых приборами виброакустической защиты;
- подавление диктофонов устройствами направленного высокочастотного радиоизлучения;
- зашумления электросетей, посторонних проводников и соединительных линий ВТСС, имеющих выход за пределы контролируемой зоны;
- создание режимов теплового разрушения электронных устройств.

Состав средств защиты технических каналов утечки информации, как пассивных, так и активных представлен на рис.9.

Экранирование технических средств является эффективным методом снижения их ПассЭМИ. Различают электростаическое, магнитостатическое и электромагнитное

экранирование, причем на высоких частотах (свыше 100 кГц) применяется исключительно электромагнитное экранирование.

Наряду с источниками ПассЭМИ экранируются монтажные провода и соединительные линии. Высокую степень защиты обеспечивают витая пара в экранированной оболочке и высокочастотные коаксильные кабели. Наилучшую защиту, как от электрического, так и от магнитного полей, обеспечивают линии связи типа бифиляра, трифиляра (трех скрученных вместе проводов, один из которых используется в качестве экрана), триаксильного кабеля (изолированного коаксильного кабеля в электрическом экране), металлизированного плоского многопроводного кабеля.

Экранирование помещений применяется в том случае, если контролируемая зона от ОТСС превышает размеры контролируемой зоны объекта. Самым приемлемым материалом изготовления экрана всего объема помещения является сталь листовая. При этом в помещении экранируются стены, двери и окна. Двери для обеспечения надежного электрического контакта со стенами помещения оборудуются пружинной гребенкой. Окна, для обеспечения надежного электрического контакта съемной рамки со стенами помещения, затягиваются медной сеткой с ячейкой 2х2 мм. Характеристика степени ослабления высокочастотных электромагнитных полей различными зданиями приведена в табл. 1 приложения 12.

Экранирование аппаратуры ТСПИ и соединительных линий эффективно только при правильном их заземлении. Система заземления должна состоять из следующих основных элементов:

- общего заземления;
- заземляющего кабеля;
- шин и проводов, соединяющих заземлитель с объектами;

Для создания контуров заземления наиболее часто используют следующие схемы:

- одноточечного последовательного и параллельного соединения устройств;
- многоточечного соединения устройств;
- гибридного соединения устройств.

1. 9 Лекция № 12 (2 часа).

Тема: «Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.»

1.9.1 Вопросы лекции:

1. Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
2. Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений; порядок проведения измерений.

1.9.2 Краткое содержание вопросов:

1.Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.

В настоящее время характерными и типичными становятся следующие особенности использования вычислительной техники: возрастающий удельный вес автоматизированных процедур в общем объеме процессов обработки данных;

— нарастающая важность и ответственность решений, принима-
— емых в автоматизированном режиме и на основе автоматизирован-
— ной обработки информации;
— увеличивающаяся концентрация в АСОД информационно-вычис-
— лительных ресурсов;
— большая территориальная распределенность_компонентов

— АСОД;усложнение_режимов_функционирования технических средств
— АСОД;
— накопление на технических носителях огромных объемов ин-
— формации, причем для многих видов информации становится все
— более трудным (и даже невозможным) изготовление немашинных
— аналогов (дубликатов).
— интеграция в единых базах данных информации различного
— назначения и различной принадлежности;
— долговременное хранение больших массивов информации на
— машинных носителях.
— непосредственный и одновременный доступ к ресурсам (в
— том числе и к информации) АСОД большого числа пользователей
— различных категорий и различных учреждений;
— интенсивная циркуляция информации между компонентами
— АСОД, в том числе и расположенных на больших расстояниях друг
— от друга;
— возрастающая стоимость ресурсов АСОД.

2.Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений; порядок проведения измерений.

Согласно действующим нормативно-методическим документам (НМД), при проведении специсследований требуется измерять информативные ПЭМИН, то есть такие излучения и наводки, создаваемые исследуемым техническим средством, которые содержат обрабатываемую данным техническим средством информацию. Такие излучения составляют лишь малую долю от всего спектра излучений технического средства. Все прочие излучения не должны фиксироваться. Для того чтобы выделить информационные ПЭМИН, на исследуемом техническом средстве предусматривают специальные тестовые режимы работы. Требования к тестам определяются в соответствующих ГОСТах и методиках. Информационные ПЭМИН от технического средства в тестовом режиме должны иметь максимально возможный уровень и легко опознаваться на слух. При поиске ПЭМИН исследователь прослушивает через головные телефоны сигналы на выходе демодулятора измерительного прибора, одновременно наблюдая осциллограммы этих сигналов. Если обнаружен сигнал, похожий на искомый тестовый сигнал, исследователь путём выключения и включения тестового режима исследуемого технического средства убеждается в том, что сигнал действительно генерируется именно этим средством и является информационным побочным излучением (наводкой). Таким образом, первым критерием для исследователя является информационная окраска искомого сигнала. Второй, не менее важный критерий, - изменение уровня на частоте обнаруженного сигнала при включении и выключении теста на исследуемом техническом средстве. Инженер может столкнуться с трудностями при регистрации изменений уровня, если уровень ПЭМИН в тестовом режиме незначительно отличается от уровня в штатном режиме, и в этом случае, зачастую, приходится принимать решение об отнесении данного сигнала к спектру ПЭМИН, основываясь только на наличии информационной окраски.

1. 10 Лекция № 13-14 (4 часа).
Тема: «Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.»
1.10.1 Вопросы лекции:

1. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звука и виброизоляции
2. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

1.10.2 Краткое содержание вопросов:

1.Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звука и виброизоляции

Акустика. Построение и параметрическое описание линий пространственного распределения звука в рабочих помещениях для оценки их акустических характеристик.

Настоящий стандарт устанавливает метод построения линий пространственного распределения звука в рабочем помещении и определения двух акустических характеристик рабочего помещения, используемых для управления шумом в нем: эксцесса уровня звукового давления и снижения уровня звукового давления при удвоении расстояния.Настоящий стандарт не применяют для оценки акустических качеств помещения с точки зрения речевого общения или других физиологических факторов.

В соответствии с пространственное распределение звука в рабочем помещении описывают линией, характеризующей спад уровня звукового давления, создаваемого точечным ненаправленным источником постоянного шума с известным уровнем звуковой мощности, с увеличением расстояния от источника. Настоящий стандарт устанавливает метод построения линии пространственного распределения звука, определения пространственного снижения уровня звукового давления при удвоении расстояния от источника шума и эксцесса уровня звукового давления в исследуемом помещении.

Данные, получаемые по настоящему стандарту, используют для:

- акустической характеристики помещения с точки зрения управления шумом в нем;
- определения подходящих мест установки машин и расположения рабочих мест в помещении;
- оценки необходимости увеличить звукопоглощение в помещении;
- качественной оценки возможных характеристик акустических экранов, предполагаемых к установке в помещении;
- расчета ожидаемых уровней излучения, когда машины с известным излучением работают в заданных местах в помещении;

Если источник шума применяют довольно часто, то рекомендуется контролировать его уровень звуковой мощности каждые три месяца или чаще до тех пор пока не будет получено по меньшей мере шесть положительных результатов контроля, свидетельствующих о стабильности характеристик источника шума. В дальнейшем межконтрольный интервал может быть увеличен.

Положение источника шума

При определении линии пространственного распределения звука акустический центр источника шума должен быть расположен:

- возможно ближе к полу или
- на высоте более 0.5 м над полом.

2.Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Несмотря на то, что некоторые системы постановки виброакустических помех обладают достаточно мощными генераторами и эффективными электроакустическими

преобразователями, обеспечивающими значительные радиусы действия, критерием выбора количества преобразователей и мест их установки должны быть не максимальные параметры систем, а конкретные условия их эксплуатации.

Так, например, если здание, в котором находится выделенное помещение, выполнено из сборного железобетона, электроакустические преобразователи системы зашумления должны располагаться на каждом элементе строительной конструкции, несмотря на то, что в процессе оборудования помещения измерения могут показать, что одного преобразователя достаточно для зашумления нескольких элементов (нескольких плит перекрытия или нескольких стеновых панелей). Необходимость такой методики установки преобразователей продиктована отсутствием временной стабильности акустической проводимости в стыках строительных конструкций. В пределах каждого элемента строительной конструкции предпочтительно выбирать места установки преобразователей в области геометрического центра этого элемента.

Следует отметить особую важность технологии крепления преобразователя к строительной конструкции. В акустическом плане крепежные приспособления являются согласующими элементами между источниками излучения - преобразователями и средой, в которой это излучение распространяется, т.е. строительной конструкцией. Поэтому крепежное устройство (помимо того, что оно должно быть точно рассчитано) должно не только прочно держаться в стене, но и обеспечивать полный акустический контакт своей поверхности с материалом строительной конструкции. Это достигается исключением щелей и зазоров в узле крепления с помощью клеев и вяжущих материалов с минимальными коэффициентами усадки.

Важным параметром, характеризующим работу системы постановки виброакустических помех, является уровень паразитных акустических шумов, излучаемых в объем выделенного помещения. Эти шумы генерируются двумя источниками. Во-первых, это вибрация защищаемых строительных конструкций. В общем случае, если создана оптимальная вибрационная помеха, эти шумы не зависят от системы зашумления и могут быть минимизированы только путем увеличения равномерности плотности энергии помехи в плоскости защищаемой конструкции за счет увеличения количества преобразователей. Вторым источником акустических шумов является собственно работающий преобразователь. Акустическое излучение вибропреобразователей можно существенно снизить, размещая их в заранее подготовленных в строительных конструкциях нишах, закрытых, например, штукатуркой после установки преобразователя

1. 11 Лекция № 15 (2 часа).
Тема: «Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам.»
1.11.1 Вопросы лекции:

1. Порядок проведения измерений.
2. Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств вычислительной техники.

1.11.2 Краткое содержание вопросов:

1.Порядок проведения измерений.

Порядок проведения измерений мегомметрами типа М-4100 и ЭСО202/2Г. Перед началом проведения измерений необходимо:

1. Перед началом проведения измерения мегомметр должен быть подвергнут контрольной проверке, которая заключается в проверке показаний прибора при разомкнутых проводах (стрелка прибора должна находиться у отметки бесконечность - ?) и замкнутых проводах (стрелка прибора должна находиться на отметке 0).

2. Убедиться, что на испытуемом кабеле нет напряжения (проверять отсутствие напряжения необходимо испытанным указателем напряжения, исправность которого должна быть проверена на заведомо находящихся под напряжением частях электроустановки - п. 3.3.1 «Межотраслевых правил по охране труда» ПОТ Р М-016-2001).

3. Заземлить токоведущие жилы испытываемого кабеля (заземление с токоведущих частей можно снимать только после подключения мегомметра).

Подключаемые провода мегомметров должны иметь зажимы с изолированными ручками, в электроустановках выше 1000 В, кроме того, следует пользоваться диэлектрическими перчатками.

При работе с мегомметром прикасаться к токоведущим частям, к которым он присоединен, не разрешается.

Как правило, измеряют сопротивление изоляции каждой фазы кабеля относительно остальных заземленных фаз. Если измерения по этому сокращенному варианту дадут неудовлетворительный результат, то необходимо измерить сопротивление изоляции между каждыми двумя фазами и каждой фазой относительно земли.

При измерениях на кабелях выше 1000 В (когда результаты измерений могут быть искажены точками утечек по поверхности изоляции) на изоляцию объекта измерения (концевую воронку и т.д.) накладывают электрод (экранные кольца), присоединенный к зажиму «Э» (экран).

При измерениях сопротивления изоляции кабелей на напряжение до 1000 В с нулевыми жилами необходимо помнить следующее:

- нулевые рабочие и защитные проводники должны иметь изоляцию, равную изоляции фазных проводников;
- как со стороны источника питания, так и со стороны приемника нулевые проводники должны быть отсоединены от заземленных частей.

2.Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств вычислительной техники.

К техническим средствам обработки информации ограниченного доступа (ТСОИ) относятся технические средства автоматизированных систем управления, электронно-вычислительные машины и их отдельные элементы, в дальнейшем именуемые средствами вычислительной техники (СВТ); средства изготовления и размножения документов; аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода; системы внутреннего телевидения; системы видеозаписи и видеовоспроизведения; системы оперативно-командной связи; системы внутренн автоматической телефонной связи, включая и соединительные линии перечисленного выше оборудования и т.д. Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами (ОТСС).

Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, в помещениях, где они установлены, как правило, находятся и другие технические средства и системы, которые в обработке информации ограниченного доступа непосредственно не участвуют. К ним относятся: системы и средства городской автоматической телефонной связи; системы и средства передачи данных в системе радиосвязи; системы и средства охранной и пожарной сигнализации; системы и средства

оповещения и сигнализации; контрольно-измерительная аппаратура; системы и средства кондиционирования; системы и средства проводной радиотрансляционной сети и приёма программ радиовещания и телевидения (абонентские громкоговорители, средства радиовещания; телевизоры и радиоприёмники и т.д.); средства электронной оргтехники; системы и средства электрочасофикации и иные технические средства и системы. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС) .

Через помещения, в которых установлены технические средства обработки информации ограниченного доступа, могут проходить провода и кабели, не относящиеся к ТСОИ и ВТСС, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции, которые называются посторонними проводниками (ПП) [7, 9].

Электропитание ТСОИ и ВТСС осуществляется от распределительных устройств и силовых щитов, которые специальными кабелями соединяются с трансформаторной подстанцией городской электросети.

Все технические средства и системы, питающиеся от электросети, должны быть заземлены. Типовая система заземления включает общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с техническими средствами.

1. 12 Лекция № 16 (2 часа).
Тема: «Методы и средства выявления электронных устройств негласного получения информации»
1.12.1 Вопросы лекции:

1. Комплекс выявления электронных устройств негласного получения информации в каналах цифровой связи "Клен"

1.12.2 Краткое содержание вопросов:

1. Комплекс выявления электронных устройств негласного получения информации в каналах цифровой связи «Клен» обеспечивает:

- выявление и идентификацию электронных устройств негласного получения информации (ЭУНПИ), использующих в своем составе узлы и блоки средств связи стандарта GSM 900/1800 с возможностью принудительного перевода передающих модулей устройств негласного получения информации в активный режим радиообмена;
- выявление и идентификацию ЭУНПИ, использующих в своем составе узлы и блоки средств связи стандарта Wi-Fi и Bluetooth с возможностью фиксирования факта радиообмена и MAC-адресов;
- локализацию источников излучений цифровых сигналов с помощью компонентного индикатора поля-частотомера.

Возможности специального программного обеспечения комплекса:

- автоматизированная оценка параметров сигналов (центральная частота/канал, ширина спектра, уровень);
- сохранение реализаций принимаемых сигналов в базе данных;
- различные варианты отображения спектра (панорама - текущая, средняя, максимум; водопад);

- контроль параметров базовых станций GSM (CELL ID, LAC, RSSI, имя оператора);
- цифровой анализ беспроводных интерфейсов WiFi (IEEE 802.11 a/b/g/n), Bluetooth (IEEE 802.15.1), ZigBee Pro (802.15.4); DECT (EU\USA);
- графическое представление местоположения устройств WiFi;
- поддержка поэтажных схем объекта в формате bmp;
- калибровка удаленных приемных модулей WiFi;
- добавление устройств на схему методом drug&drop;
- контроль параметров беспроводных устройств (MAC-адрес (EUI), SSID (EPID), тип устройства, RSSI);
- активное обнаружение мобильных терминалов GSM;
- установка многофункциональных фильтров для оптимизации отображения результатов контроля;
- установка определяемых пользователем реакций на возникающие события;
- формирование общего отчета по результатам работы;

Состав:

- блок для обнаружения средств стандарта GSM\DCS; UMTS; DECT, WiFi 2.4\5ГГц, ZigBee Pro 2.4 ГГц;
- блок нетмонитора;
- комплект удаленных приемных модулей стандартов WiFi;
- управляющая ПЭВМ;
- компонентный индикатор поля-частотомер
- комплект специального программного обеспечения.

Технические характеристики

Диапазон рабочих частот при автоматическом анализе радиочастотного спектра:	
• от 890 до 915 МГц	GSM 900 uplink
• от 935 до 960 МГц	GSM 900 downlink
• от 1710 до 1785 МГц	DCS uplink
• от 1805 до 1880 МГц	DCS downlink
• от 1880 до 1930 МГц	DECT (EU\USA)
• от 1900 до 1920 МГц	UMTS TDD
• от 2110 до 2170 МГц	UMTS TDD
• от 1920 до 1980 МГц	UMTS FDD uplink
• от 2110 до 2025 МГц	UMTS FDD downlink
• от 2400 до 2525 МГц	ISM 2,4ГГц
• от 5150 до 5250 МГц	ISM 5ГГц

• от 5250 до 5350 МГц	ISM 5ГГц
• от 5725 до 5850 МГц	ISM 5ГГц
Стандарты подавителя беспроводной и сотовой связи	GSM 900, GSM 1800 (DCS), UMTS (3G), WiFi, Bluetooth
Выходная мощность подавителя беспроводной и сотовой связи	не менее 2 Вт, регулируемая
Стандарты логического анализатора:	
• Wi-Fi	стандарт IEEE 802.11 abgn
• Bluetooth	стандарт IEEE 802.15.1
• ZigBee Pro	стандарт IEEE 802.15.4
• DECT	стандарт ETSI\UPCS
• GSM	канал BCCH
Определение типа обнаруженных устройств по базе спектральных портретов:	
• стандарты нетмонитора	GSM 900, GSM 1800 (DCS)
• контролируемые нетмонитором параметры базовых станций GSM	CELL ID, LAC, RSSI, имя оператора
• контролируемые удаленным приемным модулем стандарты	WiFi n\b\g
• сетевой интерфейс удаленного приемного модуля	WiFi, Ethernet 10\100BaseT

1. 13 Лекция № 17-18 (4 часа).
Тема: «Организация технической защиты информации.»
1.13.1 Вопросы лекции:

1. Основные этапы проектирования системы защиты информации техническими средствами.
2. Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты.

1.13.2 Краткое содержание вопросов:

1.Основные этапы проектирования системы защиты информации техническими средствами.

Задача проектирования (разработки, совершенствования) системы защиты информации и ее элементов возникает тогда, когда создается новая организация с закрытой (секретной, конфиденциальной) информацией или существующая система не обеспечивает требуемый уровень безопасности информации.

Проектирование системы защиты, обеспечивающей достижение поставленных перед инженерно-технической защитой информации целей и решение задач, проводится путем системного анализа существующей и разработки вариантов требуемой. Построение новой системы или ее модернизация предполагает:

- определение источников защищаемой информации и описание факторов, влияющих на ее безопасность;
- выявление и моделирование угроз безопасности информации;
- определение слабых мест существующей системы защиты информации;
- выбор рациональных мер предотвращения угроз;
- сравнение вариантов по частным показателям и глобальному критерию, выбор одного или нескольких рациональных вариантов;
- обоснование выбранных вариантов в докладной записке или в проекте для руководства организации;
- доработка вариантов или проекта с учетом замечаний руководства.

Так как отсутствуют формальные способы синтеза системы защиты, то ее оптимизация при проектировании возможна путем постепенного приближения к рациональному варианту в результате итераций.

Последовательность проектирования (модернизации) системы защиты включает три основных этапа:

- моделирование объектов защиты;
- моделирование угроз информации;
- выбор мер защиты.

Основным методом исследования систем защиты является моделирование. Моделирование предусматривает создание модели и ее исследование (анализ). Описание или физический аналог любого объекта, в том числе системы защиты информации и ее элементов, создаваемые для определения и исследования свойств объекта, представляют собой его модель. В модели учитываются существенные для решаемой задачи элементы, связи и свойства изучаемого объекта.

2.Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты.

Мероприятия по защите информации отражаются в отдельном разделе технического проекта. Для его разработки должны привлекаться организации, имеющие лицензию Гостехкомиссии РФ. При разработке технического проекта необходимо учитывать:

- в выделенных помещениях необходимо устанавливать сертифицированные технические средства обработки информации и вспомогательные технические средства;

- для размещения ТСОИ целесообразно выбирать подвальные и полуподвальные помещения;

- кабинеты руководителей учреждения, а также особо важные помещения рекомендуется располагать на верхних этажах со стороны здания, менее опасной с точки зрения ведения разведки;

- необходимо предусмотреть подвод всех коммуникаций к зданию в одном месте;

- для электропитания защищаемых технических средств рекомендуется в здании учреждения оборудовать свой разделительный трансформатор;

- электросиловые кабели рекомендуется прокладывать от общего силового щита;

- число вводов коммуникаций в зону выделенного помещения должно быть минимальным, соответствовать числу коммуникаций;

- для заземления технических средств в выделенном помещении необходимо предусмотреть отдельный собственный силовой контур заземления;

- исключить выходы посторонних проводников за пределы контролируемой зоны;

- прокладка вертикальных стояков коммуникаций вне пределов зоны выделенного помещения;

- ограждающие конструкции особо важных помещений, смежные с другими помещениями учреждения, не должны иметь проемы, ниши, а также сквозные каналы для прокладки коммуникаций;

- систему приточно-вытяжной вентиляции и воздухообмена зоны выделенных помещений целесообразно сделать отдельной, она должна иметь отдельный забор и выброс воздуха;

- короба системы вентиляции рекомендуется выполнять из неметаллических материалов;

- в помещениях с системой звукоусиления целесообразно применять облицовку внутренних поверхностей ограждающих конструкций звукопоглощающими материалами;

- дверные проемы необходимо оборудовать тамбурами;

- декоративные панели должны сниматься для осмотра;

- в выделенных помещениях не должны использоваться подвесные потолки;

- для остекления должны применяться солнцезащитные и теплозащитные стеклопакеты;

- конструкции полов целесообразно предусмотреть без плинтусов;

- в выделенных помещениях не рекомендуется применять светильники люминесцентного освещения.

Раздел технического проекта по защите информации согласуется с руководством органа по защите информации учреждения.

На втором этапе силами монтажных и строительных организаций осуществляется выполнение мероприятий по защите информации, предусмотренных техническим проектом. К работам на втором этапе привлекаются организации имеющие лицензию Гостехкомиссии РФ. Органами по защите информации организуется контроль всех этапов реконструкции объекта, а также мероприятий по защите информации.

1. 14 Лекция № 19 (2 часа).

Тема: «Лицензирование деятельности по технической защите информации.»

1.14.1 Вопросы лекции:

1. Сертификация технических средств защиты информации.
2. Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации.

1.14.2 Краткое содержание вопросов:

1.Сертификация технических средств защиты информации.

Порядок проведения сертификации средств защиты информации основан на следующих принципах.

1. Обязательность сертификации изделий, обеспечивающих защиту государственной тайны или подлежащих сертификации в соответствии с нормативными актами Российской Федерации. В настоящее время такое требование установлено для средств защиты информации в системах электронного документооборота, используемых для обмена с Центральным Банком России, а также для средств и систем государственных предприятий или предприятий, на которых размещен государственный заказ.

2. На сертификацию принимаются изделия только от заявителей, имеющих лицензию на соответствующие виды деятельности. Оформление установленным порядком

права на осуществление деятельности в области защиты информации является первичным. Разрабатывать алгоритмы и средства защиты на их базе как продукцию, товар, предлагаемый на рынок, могут только предприятия, имеющие лицензию. В различных публикациях специалисты неоднократно указывали, что сами по себе даже высоконадежные средства защиты, в том числе криптографические алгоритмы или отдельные блоки и модули (аппаратные, аппаратно-программные и программные), реализующие часть процесса защиты, не могут обеспечить требуемый уровень защиты информации в комплексе. Например, без реализации специальных мер эти средства могут быть просто обойдены или необходимая информация может быть получена за счет побочных электромагнитных излучений и наводок. Для систем и комплексов, включающих совокупность явно различимых как самостоятельные изделия функционально и конструктивно законченных элементов, возможно оформление сертификата на каждый из них.

3. Процедура сертификации осуществляется в отношении только технических средств или технической части системы защиты с учетом условий их эксплуатации.

4. Двухступенчатость процесса сертификации при независимости организаций, проводящих экспертизу и сертификационные испытания: сертификация средств защиты информации осуществляется Центральным органом по сертификации, а испытания проводятся в аккредитованных испытательных центрах (лабораториях).

5. Дифференцированность подхода к уровню защиты различных видов информации.

6. Обязательность использования криптографических алгоритмов, являющихся стандартами или ранее рекомендованных либо разработанных ФАПСИ.

Специально подчеркнем, что факт одобрения ФАПСИ алгоритма до его технической реализации является одним из основных требований к представляемым на сертификацию изделиям криптозащиты. Это одобрение может быть осуществлено путем утверждения алгоритма: в качестве государственного стандарта; Правительством Российской Федерации; ФАПСИ. Следовательно, изделия, созданные на базе собственных оригинальных алгоритмов, ранее не представлявшихся в ФАПСИ, а также изделия, реализующие алгоритмы иностранной разработки или импортные шифровальные средства, на сертификацию не принимаются.

2.Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» – подтверждается, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации

Порядок проведения аттестации объектов информатизации на соответствие требованиям безопасности информации включает следующие действия

- подачу заявки на рассмотрение и проведение аттестации;
- анализ исходных данных по аттестуемому объекту информатизации;
- проведение предварительного специального обследования аттестуемого объекта информатизации;
- разработку программы и методики аттестационных испытаний;
- заключение договоров на аттестацию;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации;
- проведение аттестационных испытаний объекта информатизации;

- оформление, регистрацию и выдачу «Аттестата соответствия»;
- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
- рассмотрение апелляций.

Рассмотрим порядок проведения аттестации объектов информатизации на соответствие требованиям безопасности информации от утечки по техническим каналам.

Заявитель для получения «Аттестата соответствия» заблаговременно направляет в орган по аттестации заявку на проведение аттестации с исходными данными по аттестуемому объекту информатизации, которые включают:

- перечень подлежащих аттестации объектов информатизации и выделенных помещений с указанием для каждого объекта назначения, категории и местоположения;
- перечень установленных технических средств обработки информации ограниченного доступа (ТСОИ) с указанием наличия сертификата соответствия (предписания на эксплуатацию), заключением по результатам специальной проверки на наличие возможно внедренных электронных устройств перехвата информации, категорий и мест (помещений) их установки;
- перечень установленных вспомогательных технических средств и систем (ВТСС) с указанием наличия сертификата соответствия, заключения по результатам специальной проверки на наличие возможно внедренных электронных устройств перехвата информации и мест их установки;
- перечень установленных технических средств защиты информации с указанием наличия сертификата соответствия и мест их установки.

Орган по аттестации в месячный срок рассматривает заявку и на основании исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

2.1 Лабораторная работа №1 (2 часа).

Тема: «Побочные электромагнитные излучения средств вычислительной техники**»**

2.1.1 Цель работы:

Освоить особенности утечки информации

2.1.2 Задачи работы:

1. Особенности утечки информации.

2. Меры защиты от побочных электромагнитных излучений.

2.1.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. персональный компьютер

2.1.4 Описание (ход) работы:

1. Составить самостоятельно (или получить у преподавателя) докумен- тацию на

контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

2. Изобразить план-схему исследуемого помещения.

3. На основании нижеприведенной методики, составить план проведе- ния визуального осмотра помещения и выявить объекты, требующие при об- следовании использования имеющихся средств видеонаблюдения (Гастроль- П) и металодетектора.

4. Сделать выводы по результатам проделанной работы и подготовить отчет.

2.2 Лабораторная работа №2 (2 часа).

Тема: «Побочные электромагнитные излучения средств вычислительной техники.»

2.2.1 Цель работы:

Научиться выявлять уязвимости вычислительной техники.

2.2.2 Задачи работы:

1. Примеры снимаемой информации.

2. Выявление уязвимостей вычислительной техники.

2.2.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. персональный компьютер

2.2.4 Описание (ход) работы:

1. По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации де- тектора электромагнитного поля ST107 и меры безопасности при работе с ним.

2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.

3. Обеспечить удаление из зоны действия прибора мощных помеховых объектов.

4. Провести обследование помещения лаборатории. Выявить и тща- тельно зафиксировать все источники ЭМС, и определить их характеристики, пользуясь всеми возможностями детектора электромагнитного поля ST107.

5. Провести обследование контрольных образцов имитаторов ЗУ и про- вести их идентификацию с использованием и без использования частотомера.

6. Составить отчет о проделанной работе, который должен включать:

- описание индикатора, принципа его действия, характеристик и основ- ных приемы работы;
- данные, полученные при исследовании ЭМО в лаборатории;
- результаты идентификации контрольных образцов с подробным обос- нованием принято решения.

7. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя.

2.3 Лабораторная работа №3 (2 часа).

Тема: «Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях»

2.3.1 Цель работы:

Разобрать особенности утечки информации и примеры снимаемой информации.

2.3.2 Задачи работы:

1. Особенности утечки информации.

2. Примеры снимаемой информации.

2.3.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. персональный компьютер

2.3.4 Описание (ход) работы:

1. По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации при- бора ST031 «Пиранья» и меры безопасности при работе с ним.

2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.

3. Обеспечить удаление из помещения, где проводятся занятия, мощ- ных помеховых объектов, отключить сотовые телефоны.

4. С помощью контрольного устройства «Тест» провести проверку ра- ботоспособности прибора ST031 во всех основных режимах работу, или только в режимах указанных преподавателем. Зафиксировать характеристики тестовых сигналов, излучаемых КУ.

5. Провести обследование помещения в одном из режимов, указанном преподавателем, при обнаружении посторонних сигналов провести их иден- тификацию и определить характеристики. По возможности установить ис- точник этих излучений и его примерное местоположение.

6. Составить отчет о проделанной работе, который должен включать:

- краткое описание прибора «Пиранья», принципа его действия, характе- ристик и основных приемов работы;
- данные, полученные при исследовании эталонных сигналов КУ «Тест»;
- результаты идентификации тестовых сигналов с подробным обоснова- нием принято решения.

7. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя, проводящего занятие.

2.4 Лабораторная работа №4-5 (4 часа).

Тема: «Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях**»**

2.4.1 Цель работы:

Ознакомиться с пассивными методами защиты от наводки средств вычислительной техники в линейных коммуникациях. Разобрать активные методы защиты от наводки средств вычислительной техники в линейных коммуникациях.

2.4.2 Задачи работы:

1. Пассивные методы защиты от наводки средств вычислительной техники в линейных коммуникациях.

2. Активные методы защиты от наводки средств вычислительной техники в линейных коммуникациях.

2.4.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. персональный компьютер

2.4.4 Описание (ход) работы:

1. По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации нели- нейного локатора «Катран» и меры безопасности при работе с ним.
2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
3. Обеспечить удаление из зоны действия локатора мощных помеховых объектов.
4. Провести обследование эталонных объектов: интегральной микро- схемы, металлического предмета, МОМ структуры и элемента, содержащего одновременно полупроводник и МОМ структуру. Выявить и тщательно за- фиксировать их отличительные признаки, пользуясь всеми возможностями нелинейного локатора.
5. Провести обследование контрольных образцов, скрытых в специаль- ных коробочках и провести их идентификацию.
6. Составить отчет о проделанной работе, который должен включать: описание нелинейного локатора, принципа его действия, характеристик и ос- новных приемов работы; данные, полученные при исследовании эталонных образцов; результаты идентификации контрольных образцов с подробным обоснованием принятого решения.
7. Отчет составляется персонально каждым студентом, и полученные в нем результаты подлежат защите у преподавателя.

2.5 Лабораторная работа №6-7 (4 часа).

Тема: «Оценка защищенности выделенного помещения от утечки информации по акустическому и виброакустическому каналам»

2.5.1 Цель работы:

Изучить методы выявления электронных устройств негласного получения информации.

2.5.2 Задачи работы:

1. Методы выявления электронных устройств негласного получения информации.

2. Средства выявления электронных устройств негласного получения информации.

2.5.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. персональный компьютер

2.5.4 Описание (ход) работы:

1. По техническому описанию прибора и настоящему пособию изучить устройство,

технические характеристики, инструкцию по эксплуатации при- емника и меры безопасности при работе с ним.

2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.

3. Обеспечить удаление из зоны действия прибора мощных помеховых объектов.

4. Провести обследование помещения лаборатории. Выявить и тща- тельно зафиксировать все источники ЭМС, и определить их характеристики, пользуясь всеми возможностями приѐмника.

5. Провести обследование контрольных образцов имитаторов ЗУ и про- вести их идентификацию с использованием и без использования частотомера.

6. Составить отчет о проделанной работе, который должен включать:

- описание индикатора, принципа его действия, характеристик и основ- ных приемы работы;
- данные, полученные при исследовании ЭМО в лаборатории;
- результаты идентификации контрольных образцов с подробным обосно- ванием принято решения.

7. Отчет составляется персонально каждым студентом, и полученные в нем результаты подлежат защите у преподавателя.

2.6 Лабораторная работа № 8-9 (4 часа).

Тема: «Изучение средств обеспечения конфиденциальности данных**»**

2.6.1 Цель работы:

Изучить меры защиты конфиденциальных данных. Ознакомиться с видами средств обеспечения конфиденциальности данных.

2.6.2 Задачи работы:

1. Виды средств обеспечения конфиденциальности данных.

2. Меры защиты конфиденциальных данных.

2.6.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. персональный компьютер

2.6.4 Описание (ход) работы:

1. Установите регулятором положение max чувствительности. Для этого, находясь на относительном удалении от предполагаемых мест установки РС (например, в свободном от мебели центре комнаты), поворачивайте ручку регулятора вправо до начала загорания второго сегмента шкалы индикатора (выключатель при этом должен находиться в положении «OFF»).

2. В случае, если при максимальном загрубении чувствительности детектора (регулятор повернут против часовой стрелки до упора) на индикаторе горит более двух сегментов, что говорит о высоком уровне электромагнитных полей на объекте, включите аттенюатор (выключатель в положении «АТТ»). Это позволит Вам работать в данных условиях при соответствующем уменьшении максимальной дальности обнаружения примерно в 2–3 раза.

3. В процессе работы с прибором могут создавать помехи побочные излучения бытовых электроприборов, телевизоры, компьютеры, различные наводки от проводов сети 220В´50Гц. Предварительно изучите характер их действия и особенности распространения.

4. При осмотре объекта проводите антенной прибора вдоль предполагаемых мест установки РС. Увеличение количества одновременно горящих светодиодов индикатора и усиление тона звукового сигнала позволят Вам точно установить их месторасположение.

5. Для уменьшения чувствительности и соответственно повышения точности локализации РС плавно поворачивайте регулятор против часовой стрелки.

Для однозначной идентификации включите акустическую завязку (систему акустической обратной связи) (выключатель в положении «AUD»). На нахождение РС в зоне обнаружения детектора однозначно укажет характерный звуковой тон. В противном случае будет прослушиваться хаотичный шум.

6. Для более точного определения меняйте ориентацию антенны.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие №1 (2 часа).

Тема: «Наводки электромагнитных излучений ТСПИ. Параметрический канал утечки информации**»**

3.1.1 Задание для работы:

1. Федеральный закон Российской Федерации от 27.07.2006 (ред. от 21.07.2014) г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

2. Основные понятия.

3.1.2 Краткое описание проводимого занятия:

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) 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;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) 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;

11.1) 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;

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

13) сайт в сети "Интернет" - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет";

14) страница сайта в сети "Интернет" (далее также - интернет-страница) - часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет";

15) доменное имя - обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет";

17) владелец сайта в сети "Интернет" - лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте;

18) провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет";

19) единая система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах;

20) поисковая система - информационная система, осуществляющая по запросу пользователя поиск в сети "Интернет" информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети "Интернет" для доступа к запрашиваемой информации, расположенной на сайтах в сети "Интернет", принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

3.1.3 Результаты и выводы:

Студенты ознакомились с Федеральным законом «Об информации, информационных технологиях и о защите информации».

3.2 Практическое занятие №2 (2 часа).

Тема: «Технические каналы утечки информации при передаче ее по каналам связи»

3.2.1 Задание для работы:

1. Федеральный Закон Российской Федерации от 27.12.2002 г. (действующая редакция от 23.06.2014) № 184-ФЗ "О техническом регулировании".

2. Основные понятия.

3.2.2 Краткое описание проводимого занятия:

Статья 1. Сфера применения настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

Разработке, принятии, применении и исполнении обязательных требований к продукции, в том числе зданиям и сооружениям (далее - продукция), или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации;

Разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг; оценке соответствия.

Настоящий Федеральный закон также определяет права и обязанности участников регулируемых настоящим Федеральным законом отношений.

2. Требования к функционированию единой сети связи Российской Федерации, связанные с обеспечением целостности, устойчивости функционирования указанной сети связи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи.

3. Действие настоящего Федерального закона не распространяется на социально-экономические, организационные, санитарно-гигиенические, лечебно-профилактические, реабилитационные меры в области охраны труда, федеральные государственные образовательные стандарты, положения (стандарты) о бухгалтерском учете и правила (стандарты) аудиторской деятельности, стандарты эмиссии ценных бумаг и проспектов эмиссии ценных бумаг, стандарты оценочной деятельности, стандарты распространения, предоставления или раскрытия информации, минимальные социальные стандарты, стандарты предоставления государственных и муниципальных услуг, профессиональные стандарты, стандарты социальных услуг в сфере социального обслуживания.

4. Настоящий Федеральный закон не регулирует отношения, связанные с разработкой, принятием, применением и исполнением санитарно-эпидемиологических

требований, требований в области охраны окружающей среды, требований в области охраны труда, требований к безопасному использованию атомной энергии, в том числе требований безопасности объектов использования атомной энергии, требований безопасности деятельности в области использования атомной энергии, требований к осуществлению деятельности в области промышленной безопасности, безопасности технологических процессов на опасных производственных объектах, требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики, требований к обеспечению безопасности космической деятельности, за исключением случаев разработки, принятия, применения и исполнения таких требований к продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации.

Статья 2. Основные понятия

Для целей настоящего Федерального закона используются следующие основные понятия:

абзац 2 статьи 2 утратил силу согласно Федеральному закону от 23.06.2014 г. № 160-ФЗ;

безопасность продукции и связанных с ней процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации (далее - безопасность) - состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений;

ветеринарно-санитарные и фитосанитарные меры - обязательные для исполнения требования и процедуры, устанавливаемые в целях защиты от рисков, возникающих в связи с проникновением, закреплением или распространением вредных организмов, заболеваний, переносчиков болезней или болезнетворных организмов, в том числе в случае переноса или распространения их животными и (или) растениями, с продукцией, грузами, материалами, транспортными средствами, с наличием добавок, загрязняющих веществ, токсинов, вредителей, сорных растений, болезнетворных организмов, в том числе с пищевыми продуктами или кормами, а также обязательные для исполнения требования и процедуры, устанавливаемые в целях предотвращения иного связанного с распространением вредных организмов ущерба;

декларирование соответствия - форма подтверждения соответствия продукции требованиям технических регламентов;

декларация о соответствии - документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов;

заявитель - физическое или юридическое лицо, которое для подтверждения соответствия принимает декларацию о соответствии или обращается за получением сертификата соответствия, получает сертификат соответствия;

знак обращения на рынке - обозначение, служащее для информирования приобретателей, в том числе потребителей, о соответствии выпускаемой в обращение продукции требованиям технических регламентов;

знак соответствия - обозначение, служащее для информирования приобретателей, в том числе потребителей, о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту;

идентификация продукции - установление тождественности характеристик продукции ее существенным признакам;

контроль (надзор) за соблюдением требований технических регламентов - проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки;

международный стандарт - стандарт, принятый международной организацией;

национальный стандарт - стандарт, утвержденный национальным органом Российской Федерации по стандартизации;

орган по сертификации - юридическое лицо или индивидуальный предприниматель, аккредитованные в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации для выполнения работ по сертификации;

оценка соответствия - прямое или косвенное определение соблюдения требований, предъявляемых к объекту;

подтверждение соответствия - документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

продукция - результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях;

риск - вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда;

сертификация - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

сертификат соответствия - документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

система сертификации - совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом;

стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;

стандартизация - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг;

техническое регулирование - правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия;

технический регламент - документ, который принят международным договором Российской Федерации, подлежащим ратификации в порядке, установленном законодательством Российской Федерации, или в соответствии с международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации);

форма подтверждения соответствия - определенный порядок документального удостоверения соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

схема подтверждения соответствия - перечень действий участников подтверждения соответствия, результаты которых рассматриваются ими в качестве доказательств соответствия продукции и иных объектов установленным требованиям;

свод правил - документ в области стандартизации, в котором содержатся технические правила и (или) описание процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации продукции и который применяется на добровольной основе в целях соблюдения требований технических регламентов;

региональная организация по стандартизации - организация, членами (участниками) которой являются национальные органы (организации) по стандартизации государств, входящих в один географический регион мира и (или) группу стран, находящихся в соответствии с международными договорами в процессе экономической интеграции;

стандарт иностранного государства - стандарт, принятый национальным (компетентным) органом (организацией) по стандартизации иностранного государства;

региональный стандарт - стандарт, принятый региональной организацией по стандартизации;

свод правил иностранного государства - свод правил, принятый компетентным органом иностранного государства;

региональный свод правил - свод правил, принятый региональной организацией по стандартизации;

предварительный национальный стандарт - документ в области стандартизации, который утвержден национальным органом Российской Федерации по стандартизации и срок действия которого ограничен;

абзац 35 статьи 2 утратил силу согласно Федеральному закону от 23.06.2014 г. № 160-ФЗ;

абзац 36 статьи 2 утратил силу согласно Федеральному закону от 23.06.2014 г. № 160-ФЗ;

впервые выпускаемая в обращение продукция - продукция, которая ранее не находилась в обращении на территории Российской Федерации либо которая ранее выпускалась в обращение и свойства или характеристики которой были впоследствии изменены.

3.2.3 Результаты и выводы:

Студенты ознакомились с Федеральным законом "О техническом регулировании".

3.3 Практическое занятие №3 (2 часа).

Тема: «Электрические линии связи. Средства передачи электрических сигналов»

3.3.1 Задание для работы:

1. Указ Президента Российской Федерации от 6.03.1997 г. №188 Об утверждении Перечня сведений конфиденциального характера.

2. Основные понятия.

3.3.2 Краткое описание проводимого занятия:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

ГАРАНТ:

Согласно Федеральному закону от 15 ноября 1997 г. N 143-ФЗ сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20 апреля 1995 г. N 45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" и от 20 августа 2004 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства", другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 г. N 229-ФЗ "Об исполнительном производстве".

3.3.3 Результаты и выводы:

Студенты ознакомились с Указом Президента Российской Федерации «Об утверждении Перечня сведений конфиденциального характера».

3.4 Практическое занятие №4 (2 часа).

Тема: «Средства передачи электрических сигналов. Каналы утечки информации за счет паразитных связей»

3.4.1 Задание для работы:

1. ГОСТ 28147-89. Защита информации от утечки за счет побочных электромагнитных излучений и наводок.

2. Общие технические требования.

3.4.2 Краткое описание проводимого занятия:

В электромагнитных каналах утечки информации носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами. Основными причинами возникновения электромагнитных каналов утечки информации в ТСОИ являются:

- побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ;
- модуляция информативным сигналом побочных электромагнитных излучений высокочастотных генераторов ТСОИ (на частотах работы высокочастотных генераторов);
- модуляция информативным сигналом паразитного электромагнитного излучения ТСОИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты).

Побочным электромагнитным излучением (ПЭМИ) ТСОИ называется нежелательное радиоизлучение, возникающее в результате нелинейных процессов в блоках ТСОИ.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;
- запись информации на накопители;
- чтение информации с накопителей;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства - принтеры, плоттеры; запись данных от сканера на магнитный носитель и т.д.

При каждом режиме работы СВТ возникают ПЭМИ, имеющие свои характерные особенности. Диапазон возможных частот побочных электромагнитных излучений СВТ может составлять от 10 кГц до 2 ГГц.

Паразитным электромагнитным излучением ТСОИ называется побочное радиоизлучение, возникающее в результате самовозбуждения генераторных или усилительных блоков ТСОИ из-за паразитных связей. Наиболее часто такие связи возникают за счёт случайных

преобразований отрицательных обратных связей (индуктивных или ёмкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота автогенерации (самовозбуждения) лежит в пределах рабочих частот нелинейных элементов усилителей (например, полупроводниковых приборов). В ряде случаев паразитное электромагнитное излучение модулируется информативным сигналом(модуляцией называется процесс изменения одного или нескольких параметров электромагнитного излучения (например, амплитуды, частоты или фазы) в соответствии с изменениями параметров информативного сигнала, воздействующих на него).

Для перехвата побочных электромагнитных излучений СВТ используются специальные стационарные, перевозимые и переносимые приёмные устройства, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН).

Типовой комплекс разведки ПЭМИ включает: специальное приёмное устройство, ПЭВМ (или монитор), специальное программное обеспечение и широкодиапазонную направленную антенну.

Средства разведки ПЭМИ могут устанавливаться в близлежащих зданиях или машинах, расположенных за пределами контролируемой зоны объекта .

Наиболее опасным (с точки зрения утечки информации) режимом работы СВТ является вывод информации на экран монитора. Учитывая широкий спектр ПЭМИ видеосистемы СВТ ($DF_c > 100$ МГц) и их незначительный уровень, перехват изображений, выводимых на экран монитора ПЭВМ, является довольно трудной задачей.

Дальность перехвата ПЭМИ современных СВТ, как правило, не превышает 30-50 м.

Качество перехваченного изображения значительно хуже качества изображения, выводимого на экран монитора ПЭВМ.

Особенно трудная задача - перехват текста, выводимого на экран монитора и написанного мелким шрифтом.

3.4.3 Результаты и выводы:

Студенты ознакомились с ГОСТ 28147-89. Защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

3.5 Практическое занятие №5 (2 часа).

Тема: «Опасные сигналы и их источники. Электрические каналы утечки информации**»**

3.5.1 Задание для работы:

1. РД 50-715-92. Методические указания. Информационная технология.

2. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники.

3. Порядок организации работ при разработке и изготовлении.

3.5.2 Краткое описание проводимого занятия:

В зависимости от среды распространения информативных сигналов рассматривают два возможных канала утечки: собственно за счет ПЭМИН и коммуникационный.

По способу образования классифицируют четыре типа каналов утечки:

- канал электромагнитного излучения (ЭМИ), образуемый полями, возникающими при прохождении информации по цепям СОИ;

- канал случайных антенн (СА), возникающий за счет наведенных ЭДС в токопроводящих коммуникациях, гальванически не связанных с СОИ и имеющих выход за пределы контролируемой зоны (КЗ);

- канал отходящих коммуникаций, гальванически связанных с СОИ;

- канал неравномерного потребления тока (НПТ), образующийся за счет амплитудной модуляции тока срабатыванием элементов СОИ при обработке информации.

Канал ЭМИ характеризуется размером зоны ЭМИ – расстоянием между СОИ и антенной аппаратуры перехвата, за пределами которой невозможен эффективный прием вследствие естественного снижения уровня излучаемого сигнала.

Канал случайных антенн характеризуется размерами их зоны для сосредоточенных случайных антенн (ССА) и распределенных случайных антенн (РСА). К сосредоточенным случайным антеннам относятся любые технические средства, имеющие выход за пределы контролируемой зоны. К распределенным случайным антеннам относят провода, кабели, элементы конструкций здания и т.п. Расстояние между СОИ и СА, на котором невозможен эффективный перехват, определяет размер зоны СА.

Канал отходящих коммуникаций характеризуется предельно допустимым значением отношения мощностей информативного сигнала и нормированной помехи, при котором невозможен эффективный прием.

Канал НПТ характеризуется предельно допустимым значением отношения величины изменения тока, поступающего от источника при обработке информации, к средней величине тока потребления. Если указанное отношение не превышает предельного значения, эффективный прием по каналу НПТ невозможен. В настоящее время, с учетом практического отсутствия в составе СВТ низкоскоростных устройств (диапазон частот этого канала принимается от 0 до 30 Гц), этот канал малоактуален.

С учетом изложенного можно сформулировать критерий защищенности СОИ от утечки через ПЭМИ и наводки: СОИ считается защищенным, если:

- радиус зоны электромагнитных излучений не превышает минимально допустимого

расстояния от СОИ до границы КЗ;

- отношение мощностей информативного сигнала нормированной помехи во всех СА не превышает на границе КЗ предельно допустимую величину;

- отношение мощностей информативного сигнала нормированной помехи во всех отходящих коммуникациях на границе КЗ не превышает предельно допустимую величину;

- отношение величины изменения тока «обработки» к средней величине тока потребления от электросети на границе КЗ не превышает предельно допустимое значение.

3.5.3 Результаты и выводы:

Студенты освоили защиту информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники.

3.6 Практическое занятие №6 (2 часа).

Тема: «Электрические каналы утечки информации. Контроль и прослушивание телефонных каналов связи**»**

3.6.1 Задание для работы:

1. СТР-К Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.

2. Основные понятия.

3.6.2 Краткое описание проводимого занятия:

В настоящем документе приняты следующие основные термины, определения и сокращения:

1.1. Абонент Сети (см. также п. 1.14) - лицо, являющееся сотрудником учреждения (предприятия), имеющее соответствующим образом оформленное разрешение и технические возможности на подключение и взаимодействие с Сетями.

1.2. Абонентский пункт (АП) - средства вычислительной техники учреждения (предприятия), подключаемые к Сетям с помощью коммуникационного оборудования.

АП могут быть в виде автономных персональных электронно-вычислительных машин (ПЭВМ) с модемом и не иметь физических каналов связи с другими средствами вычислительной техники (СВТ) предприятия, а также в виде одной или нескольких объединенных локальных вычислительных сетей (ЛВС) с рабочими станциями и серверами, соединенных с Сетями через коммуникационное оборудование (модемы, мосты, шлюзы, маршрутизаторы-роутеры, мультиплексоры, коммуникационные серверы и т.п.).

1.3. Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.4. Администратор АС - лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

1.5. Администратор защиты (безопасности) информации - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

1.6. Безопасность информации - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

1.7. Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

К ним относятся:

<!--[if !supportLists]-->· <!--[endif]-->различного рода телефонные средства и системы;

<!--[if !supportLists]-->· <!--[endif]-->средства и системы передачи данных в системе радиосвязи;

<!--[if !supportLists]-->· <!--[endif]-->средства и системы охранной и пожарной сигнализации;

<!--[if !supportLists]-->· <!--[endif]-->средства и системы оповещения и сигнализации;

<!--[if !supportLists]-->· <!--[endif]-->контрольно-измерительная аппаратура;

<!--[if !supportLists]-->· <!--[endif]-->средства и системы кондиционирования;

<!--[if !supportLists]-->· <!--[endif]-->средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.д.);

<!--[if !supportLists]-->· <!--[endif]-->средства электронной оргтехники;

<!--[if !supportLists]-->· <!--[endif]-->средства и системы электрочасофикации;

<!--[if !supportLists]-->· <!--[endif]-->иные технические средства и системы.

1.8. Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

1.9. Доступность (санкционированная доступность) информации - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

1.10. Защита информации от несанкционированного доступа (защита от НСД) или воздействия - деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

1.11. Специальный защитный знак (СЗЗ) - сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты путем определения подлинности и целостности СЗЗ, путем сравнения самого знака или композиции "СЗЗ - подложка" по критериям соответствия характерным признакам визуальными, инструментальными и другими методами.

1.12. Защищаемые помещения (ЗП) - помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

1.13. Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах и обсуждаемая в ЗП.

1.14. Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

1.15. Информационные сети общего пользования (далее-Сети) - вычислительные (информационно-телекоммуникационные сети) открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

1.16. Контролируемая зона (КЗ) - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Границей КЗ могут являться:

<!--[if !supportLists]-->· <!--[endif]-->периметр охраняемой территории учреждения (предприятия);

<!--[if !supportLists]-->· <!--[endif]-->ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

В отдельных случаях на период обработки техническими средствами конфиденциальной информации КЗ временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

1.17. Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

1.18. Локальная вычислительная сеть - вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования.

1.19. Межсетевой экран (МЭ) - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС.

1.20. Несанкционированный доступ (несанкционированные действия) (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.21. Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. В контексте настоящего документа к ним относятся технические средства и системы автоматизированных систем различного уровня и назначения на базе средств вычислительной техники, средства и системы связи и передачи данных, используемые для обработки конфиденциальной информации.

1.22. Провайдер Сети - уполномоченная организация, выполняющая функции поставщика услуг Сети для абонентского пункта и непосредственно для абонентов Сети.

1.23. Система защиты информации от НСД (СЗИ НСД) - комплекс организационных мер и программно-технических (при необходимости криптографических) средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней) в автоматизированной системе.

1.24. Служебная информация СЗИ НСД - информационная база АС, необходимая для функционирования СЗИ НСД (уровень полномочий эксплуатационного персонала АС, матрица доступа, ключи, пароли и т.д.).

1.25. Технический канал утечки информации - совокупность объекта технической разведки, физической среды и средства технической разведки, которыми добываются разведывательные данные.

1.26. Услуги Сети - комплекс функциональных возможностей, предоставляемых абонентам сети с помощью прикладных протоколов (протоколы электронной почты, FTP - File Transfer Protocol - прием/передача файлов, HTTP - Hiper Text Transfer Protocol - доступ к Web-серверам, IRC - Internet Relay Chat -диалог в реальном времени, Telnet - терминальный доступ в сети, WAIS - Wide Area Information Servers - система хранения и поиска документов в сети и т.д.).

1.27. Целостность информации - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

1.28. Web-сервер - общедоступный в Сети информационный сервер, использующий гипертекстовую технологию.

3.6.3 Результаты и выводы:

Студенты освоили специальные требования и рекомендации по защите информации.

3.7 Практическое занятие №7 (2 часа).

Тема: «Контроль и прослушивание телефонных каналов связи. Электромагнитные каналы утечки информации**»**

3.7.1 Задание для работы:

1. Выявление уязвимостей от побочных электромагнитных излучений.

2. Меры защиты от побочных электромагнитных излучений.

3.7.2 Краткое описание проводимого занятия:

Активный метод предполагает применение специальных широкополосных передатчиков помех. Метод хорош тем, что устраняется не только угроза утечки информации по каналам побочного излучения компьютера, но и многие другие угрозы. Как правило, становится невозможным также и применение закладных подслушивающих устройств. Становится невозможной разведка с использованием излучения всех других устройств, расположенных в защищаемом помещении. Но этот метод имеет и недостатки. Во-первых, достаточно мощный источник излучения никогда не считался полезным для здоровья. Во-вторых, наличие маскирующего излучения свидетельствует, что в данном помещении есть серьезные секреты. Это само по себе будет привлекать к этому помещению повышенный интерес ваших недоброжелателей. В-третьих, при определенных условиях метод не обеспечивает гарантированную защиту компьютерной информации.

Обоих этих недостатков лишен пассивный метод. Заключается он в экранировании источника излучения (доработка компьютера), размещении источника излучения (компьютера) в экранированном шкафу или в экранировании помещения целиком. В целом, конечно, для защиты информации пригодны оба метода. Но при одном условии: если у вас есть подтверждение того, что принятые меры действительно обеспечивают требуемую эффективность защиты.

Применяя активный метод, то имейте в виду, что уровень создаваемого источником шума излучения никак не может быть рассчитан. В одной точке пространства уровень излучения источника помех превышает уровень излучения компьютера, а в другой точке пространства или на другой частоте это может и не обеспечиваться. Поэтому после установки источников шума необходимо проведение сложных измерений по всему периметру охраняемой зоны и для всех частот. Процедуру проверки необходимо повторять всякий раз, когда вы просто изменили расположение компьютеров, не говоря

уж об установке новых. Это может быть настолько дорого, что, наверное, стоит подумать и о других способах.

Если такие измерения не проводились, то это называется применить меры защиты «на всякий случай». Как правило, такое решение даже хуже, чем решение не предпринимать никаких мер. Ведь будут затрачены средства, все будут считать, что информация защищена, а реальная защита может вовсе и не обеспечиваться.

Каким бы путем вы ни шли, обязательным условием защиты является получение документального подтверждения эффективности принятых мер.

Если это специальное оборудование помещения (экранирование, установка генераторов шума), то детальному обследованию подлежит очень большая территория, что, конечно, недешево. В настоящее время на рынке средств защиты предлагают законченные изделия - экранированные комнаты и боксы. Они, безусловно, очень хорошо выполняют свои функции, но и стоят тоже очень хорошо.

Поэтому в наших условиях реальным остается только экранирование самого источника излучения - компьютера. Причем экранировать необходимо все. У некоторых сначала даже вызывает улыбку то, что мы экранируем, например, мышь вместе с ее хвостиком. Никто не верит, что из движения мыши можно выудить полезную информацию. А я тоже в это не верю. Мышь экранируется по той причине, что хотя она сама, может, и не является источником информации, но она своим хвостиком подключена к системному блоку. Этот хвостик является великолепной антенной, которая излучает все, что генерируется в системном блоке. Если хорошо заэкранировать монитор, то гармоники видеосигнала монитора будут излучаться системным блоком, в том числе и через хвостик мыши, поскольку видеосигналы вырабатываются видеокартой в системном блоке.

Десять лет назад экранированный компьютер выглядел настолько уродливо, что ни один современный руководитель не стал бы его покупать, даже если этот компьютер вообще ничего не излучает.

Современные же технологии основаны на нанесении (например, напылении) различных специальных материалов на внутреннюю поверхность существующего корпуса, поэтому внешний вид компьютера практически не изменяется.

Экранирование компьютера даже с применением современных технологий - сложный процесс. В излучении одного элемента преобладает электрическая составляющая, а в излучении другого – магнитная, следовательно необходимо применять разные материалы. У одного монитора экран плоский, у другого - цилиндрический, а у третьего с двумя радиусами кривизны. Поэтому реально доработка компьютера осуществляется в несколько этапов. Вначале осуществляется специсследование собранного компьютера. Определяются частоты и уровни излучения. После этого идут этапы анализа конструктивного исполнения компьютера, разработки технических требований, выбора методов защиты, разработки технологических решений и разработки конструкторской документации для данного конкретного изделия (или партии однотипных изделий). После этого изделие поступает собственно в производство, где и выполняются работы по защите всех элементов компьютера. После этого в обязательном порядке проводятся специспытания, позволяющие подтвердить эффективность принятых решений. Если специспытания прошли успешно, заказчику выдается документ, дающий уверенность, что компьютер защищен от утечки информации по каналам побочного радиоизлучения.

Комплектующие для сборки ПК поставляются из-за рубежа. С периодичностью 3-6 месяцев происходит изменение их конструкторских решений, технических характеристик, форм, габаритов и конфигураций. Следовательно, технология, ориентированная на защиту каждой новой модели ПК, требует высочайшей маневренности производства. При этом возможен вариант изготовления из металла набора универсальных корпусных изделий и размещения в них комплектующих ПК, а также периферийных устройств зарубежного производства. Недостатком этого подхода является то, что он приемлем только для полигонного или катастрофоустойчивого исполнения. Другой вариант - это выбор комплектующих для ПК из большого количества однотипных изделий по признаку минимальной излучательной способности. Этот вариант необходимо рассматривать как непрофессиональный подход к проблеме, так как он противоречит нормативной документации.

3.7.3 Результаты и выводы:

Студенты ознакомились с меры защиты от побочных электромагнитных излучений.

3.8 Практическое занятие №8 (2 часа).

Тема: «Индукционный канал утечки информации**.** Технические каналы утечки речевой информации**»**

3.8.1 Задание для работы:

1. Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров. Решение Гостехкомиссии России от 23.05.1997 т. №55

2. Основные понятия.

3.8.2 Краткое описание проводимого занятия:

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации определяется следующими документами:

- «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам», утверждены решением Гостехкомиссии России от 23 мая 1997 года № 55;
- «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено Председателем Гостехкомиссии России 25 ноября 1994 года;
- «Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации, приказ Директора ФСТЭК России от 21 апреля 2006 года № 126.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает:

1. Подача заявки на аттестацию объекта информатизации.
Заявитель для получения аттестата соответствия направляет в управление ФСТЭК России по федеральному округу (далее - Управление) заявку на проведение аттестации объекта информатизации с необходимыми исходными данными по установленной форме (приложение № 1).
2. Рассмотрение заявки на аттестацию, принятие решения на ее проведение, доведение решения до заявителя и органа по аттестации объектов информатизации.
2.1. По результатам рассмотрения заявки Управлением, организации-заявителю в 3-дневный срок направляется перечень органов по аттестации объектов информатизации, аккредитованных ФСТЭК России в Системе сертификации средств защиты информации № РОСС RU.0001.01БИ00, размещенный также на официальном Web-сайте ФСТЭК России по адресу: www.fstec.ru.
2.2. Руководитель Управления принимает решение по определению органа по аттестации объекта информатизации на основании выбора, сделанного Заявителем, исходя из полученного перечня. Принятое решение доводится до органа по аттестации объектов информатизации предписанием и до заявителя уведомлением.
2.3. Управление учитывает информацию:
- об органе по аттестации, который определен организацией-заявителем;
- о сроках проведения работ на объектах информатизации.

3. Разработка программы и методики аттестационных испытаний.
3.1. Программа аттестационных испытаний, согласованная с организацией-заявителем, должна содержать:
перечень работ, их продолжительность, методики испытаний, перечни используемой контрольной и контрольно-измерительной аппаратуры, а также средств тестирования на аттестуемом объекте информатизации (с учетом различных видов объектов информатизации и действующих нормативных и методических документов);
мероприятия по контролю состояния защищенности информации в процессе эксплуатации объекта информатизации;
мероприятия по контролю неизменности условий эксплуатации объекта информатизации;
работы в испытательных лабораториях по сертификации средств (систем) защиты информации по требованиям безопасности информации (в случае если на аттестуемом объекте информатизации используются несертифицированные средства (системы) защиты информации). Такие работы в отдельных случаях могут проводиться непосредственно на аттестуемом объекте информатизации;
состав аттестационной комиссии.
3.2. До начала работ по аттестации объектов информатизации Управлением согласовываются программа и методика аттестационных испытаний объектов информатизации 1-й категории и собственных объектов информатизации вне зависимости от категории (в случае если организация-заявитель аккредитована в качестве органа по аттестации).

4. Заключение договора на проведение аттестации объектов информатизации.
Этап подготовки завершается заключением договора между заявителем и органом по аттестации на проведение аттестации, заключением договоров (контрактов) органа по

аттестации с привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

3.8.3 Результаты и выводы:

Студенты ознакомились с методикой сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров.

3.9 Практическое занятие №9 (2 часа).

Тема: «Краткие сведения по акустике. Звуковое поле»

3.9.1 Задание для работы:

1. РД 50-716-92. Методические указания. Информационная технология.

2. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники.

3. Правила разработки, построения, изложения, оформления документов.

3.9.2 Краткое описание проводимого занятия:

1.1. Испытания СВТ на соответствие требованиям ГОСТ 29339 проводят после климатических и механических испытаний, испытаний на надежность и по требованиям электромагнитной совместимости при условии, что испытуемое СВТ удовлетворяет общим техническим требованиям, установленным в КД и ЭД на СВТ.

1.2. Испытания СВТ проводят в нормальных климатических условиях, если иные условия не оговорены в ПМ (ТУ, предписании на эксплуатацию) на конкретные СВТ.

Нормальные климатические условия испытаний характеризуются:

— температурой окружающего воздуха (20 ± 5) "С;

— относительной влажностью (60 ± 15) %;

— атмосферным давлением от 84 до 107 кПа (от 630 до 800 мм рт. ст.).

1.3. Подготовка к проведению испытаний

1.3.1. При разработке и серийном изготовлении (модернизации) СВТ производят рассмотрение актов (протоколов) проверки выполнения общих технических требований, оказывающих влияние на обеспечение защиты обрабатываемой информации (конструктивные требования, требования к электрическим параметрам, уровню индустриальных помех и т. д.), проводимых техническими службами предприятий–разработчиков (предприятий–изготовителей).

При испытаниях опытных и модернизируемых образцов дополнительно производят оценку КД и ПД в части защиты обрабатываемой информации, которую осуществляют рассмотрением их на соответствие действующим стандартам, руководящим указаниям по конструированию (РУК), ведомостям спецификаций, а также проверкой наличия подписей в КД (ПД) должностных лиц (см. приложение А).

1.3.2. При сертификации СВТ (опытных, серийно изготовляемых и модернизируемых образцов) производят:

— рассмотрение актов проведенных испытаний в части защиты обрабатываемой информации;

— определение целесообразности сертификации представляемых образцов СВТ;

— уточнение состава испытательного оборудования и КИА, необходимых для проверки испытаний.

1.3.3. При аттестации объекта информатики и в процессе эксплуатации СВТ производят:

— рассмотрение акта обследования и результатов оценки защищенности объекта;

— рассмотрение предписаний на эксплуатацию СВТ с целью предварительной оценки возможности их использования на данном объекте. При отсутствии предписаний на эксплуатацию СВТ определяют целесообразность проведения испытаний этих СВТ.

1.4. Проведение испытаний

1.4.1 Испытания СВТ на соответствие требованиям ГОСТ 29339 включают:

· проверку выполнения требований к размерам зон 1, 2;

· проверку наличия в СВТ паразитной генерации.

1.4.2 Проверка выполнения требований к размерам зон включает:

· измерение напряженности электрической и магнитной составляющих поля ПЭМИ;

· расчет размеров зон 1, 2;

· оценку их по результатам специальных исследований.

1.4.3. Измерение напряженности электрической составляющей электромагнитного поля проводят в интервале частот от 10 Гц до 1000 МГц.

Измерение напряженности магнитной составляющей электромагнитного поля проводят в интервале частот от 10 до 30 МГц.

Порядок проведения измерений изложен в приложении Б.

1.4.4. Все испытания, кроме объектовых, проводят в безэховых камерах, радиопрозрачных павильонах (помещениях) или на открытых площадках, удовлетворяющих требованиям ГОСТ 16842. Допускается проводить испытания в специально оборудованных экранированных помещениях.

Объектовые испытания проводят в реальных условиях размещения СВТ при минимальном уровне посторонних радиопомех.

1.4.5. В помещениях, где проводят испытания, не должно быть отражений электромагнитных волн. Размеры помещений для проведения измерений должны быть такими, чтобы расстояния от испытуемого СВТ, включая все ТС и соединительные кабели, входящие в состав СВТ, до посторонних отражающих предметовбыли не менее 1,5 м.

1.4.6. Напряженность поля посторонних радиопомех на каждой частоте измерений должна быть на 20 дБ меньше реальных значений напряженности поля побочных излучений исследуемого СВТ.

Допускается проводить измерения при более высоком уровне посторонних радиопомех, не превышающем уровень тестового сигнала, учитывая их влияние при проведении расчетов.

1.4.7. Взаимное расположение и подключение ТС, входящих в состав СВТ, должны соответствовать требованиям КД на СВТ. Условия размещения СВТ должны соответствовать требованиям ГОСТ 16842.

Дополнительно (для опытных образцов) проводят испытания с отступлением от требований КД с целью определения влияния расположения ТС и соединительных кабелей на повышение уровня побочных излучений СВТ. Эти отступления вместе с результатами указывают в протоколах испытаний.

1.4.8. При испытаниях используют соединительные кабели, требования к которым указаны в КД на СВТ. Если допустимы различные длины кабелей, то выбирают такие, при которых создаваемый испытуемым СВТ уровень ПЭМИ имеет максимальное значение.

1.4.9. Двери экранированных шкафов, различные съемные щиты, крышки и корпуса испытуемых СВТ должны быть закрыты, если другие условия не оговорены в ПМ (ТУ, предписании на эксплуатацию СВТ), и опечатаны.

Во время проведения испытаний нельзя подстраивать и регулировать ТС, подтягивать крепежные детали, а также вносить изменения в схемы, конструкцию, монтаж, программные средства, за исключением случаев, указанных в ПМ (ТУ, предписании на эксплуатацию или в ЭД на СВТ).

1.4.10. Технические параметры КИА, используемой для проведения испытаний, должны отвечать требованиям ГОСТ 11001 и ГОСТ 29339. При отсутствии стандартизованных средств измерений допускается применять нестандартизованные средства измерений, прошедшие метрологическую аттестацию в соответствии с ГОСТ 8.326. Конкретный состав КИА указывают в ПМ (ТУ, предписании на эксплуатацию СВТ).

Перечень и основные технические параметры КИА, рекомендуемой для проведения испытаний, приведены в приложении В.

1.4.11. Для проведения испытаний используют специальные тест-программы, обеспечивающие задействование всех цепей прохождения обрабатываемой информации, максимально возможные частоту повторения и уровень излучения тестовых сигналов.

Комплект ПД, включающий специальные тест-программы для проведения испытаний, должен отвечать требованиям ГОСТ 29339.

1.4.12. Измерения проводят во всех режимах работы СВТ.

1.4.13. По результатам измерений производят расчет размеров зон 1, 2 и их оценку на соответствие значениям, установленным в ПМ(ТУ, предписании на эксплуатацию СВТ).

Для СВТ, установленных на объектах информатики, и не имеющих предписаний на эксплуатацию, после проведения специальных исследований производят оценку соответствия рассчитанных значений размеров зон 1, 2 заданным значениям.

1.4.14. Проверку наличия паразитной генерации в СВТ осуществляют в диапазоне частот от 10 Гц до 1000 МГц в двух состояниях:

· в исходном состоянии;

· при прогоне в каждом режиме работы с использованием специальной тест-программы.

5. Результаты испытаний СВТ на соответствие требованиям ГОСТ 29339, кроме объектовых, оформляют согласно РД 50—715.

Результаты объектовых испытаний оформляют актами (протоколами) в произвольной форме с обязательным указанием значений радиусов зон 1 и 2.

6. Испытания встраиваемых в СВТ средств защиты на соответствие требованиям ГОСТ 29339 осуществляют в комплексе с другими средствами защиты обрабатываемой информации от утечки за счет ПЭМИ.

Оценку их эффективности, при необходимости, производят сравнением показателей защищенности обрабатываемой информации при включенных и выключенных испытуемых встроенных средствах защиты по результатам измерений ПЭМИ СВТ.

2. ОЦЕНКА РЕЗУЛЬТАТОВ ИСПЫТАНИЙ

2.1. Результаты испытаний опытных и серийно изготовляемых (модернизируемых) образцов СВТ на соответствие требованиям ГОСТ 29339 в части оценки эффективности защиты обрабатываемой информации от утечки за счет ПЭМИ считают положительными, а образец (партию) — выдержавшим испытания, если полученные значения радиусов зон 1, 2 образца (партии) не превышают размеров радиусов этих зон, установленных в ПМ (ТУ, предписании на эксплуатацию СВТ), и в СВТ отсутствует паразитная генерация.

В случае несоответствия испытуемого образца (партии) СВТ установленным требованиям проводят анализ причин, принимают соответствующие меры и проводят повторные испытания в установленном порядке.

2.2. Результаты сертификационных испытаний образцов (партии) СВТ на соответствие требованиям по защите обрабатываемой информации считают положительными и на образец (партию, серию) выдают сертификат соответствия, если полученные значения радиусов зон 1, 2 удовлетворяют требованиям НД Гостехкомиссии России к сертифицируемой продукции и в СВТ отсутствует паразитная генерация.

При отрицательных результатах испытаний сертификат соответствия требованиям по защите обрабатываемой информации на образец СВТ (партию, серию) не выдается.

2.3. Результаты объектовых испытаний СВТ на соответствие требованиям по защите обрабатываемой информации считают положительными, если полученные значения их радиусов зон 1, 2 не превышают заданных значений, и в СВТ отсутствует паразитная генерация.

В случае несоответствия СВТ установленным требованиям проводят анализ причин несоответствия и принимают соответствующие **меры по защите объекта информатики в установленном порядке.**

3.9.3 Результаты и выводы:

Студенты рассмотрели правила разработки, построения, изложения, оформления документов.