Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

А. Г. Жестовский

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности
10.05.03 – Информационная безопасность автоматизированных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2023

Рецензент:
заведующий кафедрой информационной безопасности
Института цифровых технологий ФГБОУ ВО
«Калининградский государственный технический университет»,
кандидат физико-математических наук, доцент
Н. Я. Великите

Жестовский, А. Г.

Защита информации от утечки по техническим каналам: учебно-методическое пособие по изучению дисциплины для студентов специальности 10.05.03 – Информационная безопасность автоматизированных систем / А. Г. Жестовский. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 70 с.

В учебно-методическом пособии приведен тематический план по дисциплине и даны методические указания по ее самостоятельному изучению, подготовке к лабораторным занятиям, подготовке и сдаче экзамена, выполнению самостоятельной работы.

Табл. 3, список лит. – 19 наименований

Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы модуля «Методы и средства обеспечения информационной безопасности автоматизированных систем» 10.05.03 – Информационная безопасность автоматизированных систем.

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала на заседании кафедры ИБ ФГБОУ ВО «Калининградский государственный технический университет» 18.01.2023, протокол № 4.

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 17.02.2023, протокол № 1.

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 – Информационная безопасность автоматизированных систем, изучающих дисциплину «Защита информации от утечки по техническим каналам».

Цель освоения дисциплины – теоретическая и практическая подготовка студента к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в защищаемых помещениях.

Задачи дисциплины – изучение:

- технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- технических каналов утечки акустической (речевой) информации;
- способов и средств защиты информации, обрабатываемой техническими средствами;
- способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- основ организации технической защиты информации на объектах информатизации.

В результате изучения дисциплины студенты должны:

– **знать** технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам;

– **уметь** анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, пользоваться нормативными документами по защите информации;

– **владеть** методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

Дисциплина «Защита информации от утечки по техническим каналам» является дисциплиной модуля «Методы и средства обеспечения информационной безопасности автоматизированных систем» и базируется на знаниях, полученных при изучении дисциплин: «Физика», «Математические модели в информационной безопасности», «Математический анализ», «Электроника и схемотехника», «Основы информационной безопасности»,

«Интегрированные системы безопасности», «Организационное и правовое обеспечение информационной безопасности».

Дисциплина «Защита информации от утечки по техническим каналам» выступает одним из важных и неотъемлемых элементов в формировании общей профессиональной составляющей в системе подготовки специалистов по защите информации. В условиях стремительного технического прогресса проблемы технического направления информационной безопасности усложняются и приобретают все большее практическое значение. Знания, получаемые по данной дисциплине, позволяют овладеть инструментарием предотвращения утечки информации по техническим каналам.

В пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины; возможно, вам потребуется больше времени на выполнение отдельных заданий или проработку отдельных тем.

Реализация компетентностного подхода при изучении дисциплины «Защита информации от утечки по техническим каналам» предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов.

В разделе «Содержание дисциплины» приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки; каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделе ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу. Все занятия, проводимые по дисциплине, в том числе и самостоятельная работа студентов, предусматривают сочетание передовых методических приемов с новыми образовательными информационными технологиями.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем:

- программное обеспечение: Microsoft Desktop Education (операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 от 2016-06-30 Open Value Subscription);
- антивирусное программное обеспечение: Kaspersky Total Space Security Russian Edition.

На занятиях используются современные формы и методы обучения (тренинги, исследовательские методы, проблемное и проектное обучение), направленные на развитие творческих способностей и самостоятельности студентов, привитие им интереса к исследовательской работе, формирование убеждения о необходимости при решении любых прикладных задач использования инновационных информационных технологий.

Лекционные занятия проводятся в специализированных аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с использованием рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов сети Интернет.

В ходе проведения лабораторных занятий используется специализированное техническое оборудование:

- комплекс оценки эффективности защиты речевой информации от утечки по каналам акустоэлектрических преобразований «СМАРТ»;
- комбинированный поисковый прибор ST 600 «ПИРАНЬЯ»;
- прибор активной защиты конфиденциальной информации «Шаман»;
- портативный измеритель частоты и мощности MFP-8000;
- детектор поля ST 107;
- виртуальный тренажер «Системы контроля и управления доступом»;
- виртуальный комплекс «Защита объекта от утечек информации по техническим каналам».

В ходе самостоятельной работы, при подготовке к плановым занятиям и экзамену студенты анализируют поставленные преподавателем задачи с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет.

2. ТЕМАТИЧЕСКИЙ ПЛАН

Общая трудоемкость дисциплины составляет 7 зачетных единиц (ЗЕТ), т. е. 252 академических часа контактной (лекционных, лабораторных занятий, а также контактной работы посредством электронной информационно-образовательной среды) и самостоятельной работы студента, в т. ч. связанной с текущей и промежуточной аттестацией по дисциплине. Относится к модулю «Методы и средства обеспечения информационной безопасности автоматизированных систем».

Формы промежуточной аттестации по дисциплине:

очная форма, седьмой семестр – зачет;

очная форма, восьмой семестр – экзамен.

Таблица 1 – Объем (трудоемкость освоения) в осеннем семестре очной формы обучения и структура дисциплины

	Номер и наименование темы, вид учебной работы	**Объем контактной работы, ч**	**СРС**
Семестр – 7 (3 ЗЕТ, 108 ч)			
Лекции			
1	Цели и задачи защиты информации от утечки информации по техническим каналам	4	4
2	Электромагнитные технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ)	6	5,4
3	Технические каналы утечки акустической (речевой) информации	7	6
		17	**15,4**
Лабораторные занятия			
1	Защита акустической информации в выделенном помещении с помощью устройств активной защиты конфиденциальной информации	4	6,25
2	Обнаружение и локализация радиоизлучающих технических средств с помощью детектора электромагнитного поля	8	6,2
3	Выявление при помощи портативного измерителя частоты и мощности акустических каналов утечки информации	10	6
4	Обнаружение работающих электронных устройств и трассировки кабельных линий с помощью комбинированного поискового прибора ST 600	12	6
		34	**24,45**
	ИТОГО семестр:	**51**	**39,85**

Таблица 2 – Объем (трудоемкость освоения) в весеннем семестре очной формы обучения и структура дисциплины

	Номер и наименование темы, вид учебной работы	Объем контактной работы, ч	СРС
Семестр – 8 (4 ЗЕТ, 144 ч)			
Лекции			
1	Способы и средства защиты объектов информатизации от утечки информации по техническим каналам.	4	2
2	Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам	4	2
3	Методы и средства контроля защищенности информации, обрабатываемой СВТ	4	2
4	Методы и средства контроля защищенности речевой информации от утечки по техническим каналам	5	4
		17	**10**
Лабораторные занятия			
1	Количественная оценка качества шумовых сигналов, формируемых средствами защиты речевой информации	6	6
2	Количественная оценка словесной разборчивости речи при оценке защищенности речевой информации от утечки по акустическому каналу	6	6
3	Количественная оценка коэффициентов виброизоляции ограждающих конструкций при оценке защищенности речевой информации от утечки по виброакустическому каналу	6	6
4	Количественная оценка коэффициентов звукоизоляции ограждающих конструкций при оценке защищенности речевой информации от утечки по акустическому каналу	8	6
5	Оценка эффективности защиты речевой информации от утечки по электроакустическому каналу	8	6
		34	**30**
	ИТОГО семестр:	**51**	**40**

Более подробные рекомендации по выполнению лабораторного практикума, включая задание, методические указания по выполнению работы, контрольные вопросы приведены в учебно–методическом пособии.

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Цели и задачи защиты информации от утечки информации по техническим каналам

Перечень изучаемых вопросов:

Цели и задачи технической защиты информации. Принципы технической защиты информации. Уровни безопасности информации. Методы защиты информации.

Термины и определения в области защиты информации от утечки по техническим каналам: объект информатизации, выделенное помещение, ОТСС, ВТСС, посторонние проводники, контролируемая зона, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, технический канал утечки информации.

Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Виды технических каналов утечки информации. Типовая структура технического канала утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации.

Методические указания к изучению:

С целью успешного усвоения материала по теме лекции необходимо последовательно изучить вопросы лекции, изложенные выше, используя при этом нижеприведенный краткий теоретический материал и рекомендованную литературу. При самостоятельной работе над материалом лекции ответить на контрольные вопросы.

Концепция технической защиты информации определяет основные принципы, методы и средства обеспечения информационной безопасности объектов. Она представляет собой общий замысел и принципы обеспечения информационной безопасности объекта в условиях угроз и включает в себя:

- оценку угроз;
- систему защиты информации;
- принцип построения системы защиты информации.

Техническая защита представляет собой совокупность специальных органов, технических средств и мероприятий по их использованию для защиты конфиденциальной информации. Эффективная техническая защита информационных ресурсов является неотъемлемой частью комплексной системы обеспечения информационной безопасности и способствует

оптимизации финансовых затрат на организацию защиты информации. Техническая защита информации предполагает комплекс мероприятий по защите информации от несанкционированного доступа по различным каналам, а также нейтрализацию специальных воздействий на нее – уничтожения, искажения или блокирования доступа.

Цели и задачи технической защиты:

• предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;

• защита носителей информации от уничтожения в результате различных природных и техногенных воздействий;

• предотвращение утечки информации по различным техническим каналам.

Принципы проектирования систем технической защиты:

1. Непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности.

2. Многозональность защиты – задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности.

3. Избирательность, заключающаяся в предотвращении угроз в первую очередь для наиболее важной информации.

4. Интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности.

5. Создание централизованной службы безопасности в интегрированных системах.

По функциональному назначению средства технической защиты подразделяются на следующие группы:

1. Инженерные средства, представляющие собой различные устройства и сооружения, противодействующие физическому проникновению злоумышленников на объекты защиты.

2. Аппаратные средства (измерительные приборы, устройства, программно-аппаратные комплексы и др.), предназначенные для выявления каналов утечки информации, оценки их характеристик и защиты информации.

3. Программные средства, программные комплексы и системы защиты информации в информационных системах различного назначения и в основных средствах обработки данных.

4. Криптографические средства, специальные математические и алгоритмические средства защиты компьютерной информации, передаваемой по открытым системам передачи данных и сетям связи. В концепции инженерно-технической защиты информации, кроме целей и задач системы безопасности, определяются принципы ее организации и функционирования; правовые

основы; виды угроз и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности, включая: физическую, правовую, организационную, экономическую, инженерно-техническую, программно-математическую защиту, информационно-аналитическое обеспечение и консультативную помощь.

Создание новой системы защиты или оценка эффективности существующей системы безопасности объекта начинается с анализа возможных угроз и оценки их реального появления. Основой для анализа является исследование объекта на наличие уязвимостей в защите, изучение расположения и особенностей инженерных конструкций, коммуникаций и т. п.

На следующем этапе построения системы защиты информации осуществляется выбор соответствующих методов и средств адекватной защиты. При оценке вероятных угроз объекту должны учитываться угрозы здоровью и безопасности персонала; угрозы целости и сохранности материальных ценностей и оборудования; безопасность информации, сохранность государственной или коммерческой тайны.

Для получения максимально реальной оценки угроз необходимы изучение и анализ статистических данных, связанных с попытками разведывательной деятельности на объекте в прошлом; оценка риска по каждому виду угроз; оценка ситуации на объекте и прилегающих к нему территориях на определенном интервале времени; изучение статистики по фактам разведдеятельности на подобных объектах.

Важным моментом в объективной оценке угроз и в разработке концепции защиты объекта является привлечение независимых экспертных организаций или специализированных государственных учреждений, имеющих квалифицированный персонал. В этом случае исключается субъективная оценка разведдоступности объекта и проводится квалифицированная разработка концепции защиты.

Несмотря на большое разнообразие возможных информационных угроз, проектирование защиты от каждой из них должно вписываться в комплексную систему защиты. Комплексная система защиты предусматривает надежное перекрытие всех опасных каналов утечки информации. Эффективность системы защиты основных и вспомогательных технических средств от утечки информации по техническим каналам оценивается по различным критериям, которые определяются физической природой информационного сигнала, но чаще всего по соотношению «сигнал/шум».

Все способы защиты согласно руководящей документации делятся на две группы:

- скрытие;
- дезинформация.

К первой группе относятся:

• пассивное скрытие;

• активное скрытие;

• специальная защита.

Ко второй группе относятся:

• техническая дезинформация;

• имитация;

• легендирование.

Суть пассивного скрытия заключается в исключении или значительном затруднении обнаружения объектов, а также в ослаблении до необходимого уровня их демаскирующих признаков.

Пассивное скрытие состоит из организационных мероприятий и технических мер.

К организационным мероприятиям относятся:

• территориальное, пространственно-временное, энергетическое и частотное ограничения на функционирование объектов;

• затруднения для ведения технической разведки путем использования маскирующих свойств местности, местных предметов, времени суток;

• установление контролируемых зон в месте расположения скрываемых видовых объектов.

К техническим мерам пассивного скрытия относятся:

• снижение контрастности демаскирующих признаков скрываемых видовых объектов по отношению к фону;

• снижение уровня информационных физических полей, создаваемых функционирующим объектом;

• применение маскирующих покрытий для видовых объектов;

• камуфлирование техники;

• применение при настройке радиоэлектронной аппаратуры эквивалентов антенн, закрытых антенно-фидерных устройств, экранированных камер и сооружений, исключающих электромагнитные излучения в окружающее пространство.

Суть активного скрытия состоит главным образом в создании маскирующих шумовых помех различной физической природы техническим средствам разведки и в создании ложной обстановки по физическим полям скрываемого объекта. Активное скрытие применяется в большинстве случаев как дополнительная мера к пассивному скрытию, когда не обеспечиваются условия снижения уровня физического поля до безопасного значения.

Спецзащита реализуется аппаратными, криптографическими и программными способами. К спецзащите относятся скремблирование телефонных переговоров, кодирование цифровой информации

криптографическими методами, программные методы модификации информации.

Литература:
[3, 4], [10] глава 1, [12].

Контрольные вопросы:

1. Сформулируйте цели и задачи технической защиты информации.
2. Какие должны быть принципы технической защиты информации?
3. Назовите уровни безопасности информации?
4. Какие вы знаете методы технической защиты информации?
5. В чем заключается сущность инженерной защиты и технической охраны источников информации?
6. Сформулируйте понятие информационного портрета объекта защиты.
7. Какие вы знаете способы изменения информационного портрета объекта защиты при маскировке?
8. Какие вы знаете способы изменения информационного портрета объекта защиты при дезинформации?
9. Охарактеризуйте зависимость качества информации от соотношения мощностей носителя информации и помехи.
10. В чем заключается сущность энергетического скрытия?
11. Перечислите показатели эффективности инженерно-технической защиты информации.

Тема 2. Электромагнитные технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ)

Перечень изучаемых вопросов:

Классификация технических каналов утечки информации, обрабатываемой СВТ. Причины возникновения побочных электромагнитных излучений (ПЭМИ) СВТ. Принципы построения средств перехвата ПЭМИ СВТ. Схема технического канала утечки информации, возникающего за счет ПЭМИ СВТ.

Методические указания к изучению:

С целью успешного усвоения материала по теме лекции необходимо последовательно изучить вопросы лекции, изложенные выше, используя при этом нижеприведенный краткий теоретический материал и рекомендованную литературу. При самостоятельной работе над материалом лекции ответить на контрольные вопросы.

К побочным электромагнитным излучениям ТСПИ относятся:

• излучения элементов ТСПИ;

• излучения на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;

• излучения на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электромагнитные излучения элементов ТСПИ

В ТСПИ, в частности и в линиях связи, входящих в их состав, носителем информации является электрический ток, характеристики которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по проводникам ТСПИ вокруг них в окружающем пространстве возникает электрическое и магнитное поле. По этой причине элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, составляющие которого модулированы также по закону изменения информационного сигнала.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования. Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электромагнитные излучения персональных компьютеров

Согласно оценочным данным, по каналу ПЭМИН (побочных электромагнитных излучений и наводок) может быть перехвачено не более 1–2 процентов данных, обрабатываемых на персональных компьютерах и других технических средствах передачи информации (ТСПИ). На первый взгляд может показаться, что этот канал менее опасен по сравнению, например, с акустическим, по которому из помещения может быть перехвачена речевая информации в полном объеме. Но необходимо помнить, что в настоящее время наиболее важная информация, содержащая государственную тайну или технологические секреты, обрабатывается на персональных компьютерах. Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата, – это данные, вводимые с клавиатуры компьютера или отображаемые на мониторе.

Компьютеры порождают электромагнитные излучения, которые не только создают помехи для радиоприема, но также создают технические каналы утечки информации. Соединительные кабели (линии связи), обладающие индуктивностью и емкостью, образуют резонансные контуры, излучающие высокочастотные электромагнитные волны, модулированными сигналами

данных. Аналогичная ситуация имеет место и при взаимном обмене сигналами между параллельно проложенными кабелями.

Исследователями продемонстрировано восстановление сетевых данных через телефонную линию, причем телефонный кабель проходил рядом с кабелем компьютерной сети всего на протяжении двух метров. Еще одна опасность исходит от «активных» атак (высокочастотное навязывание): злоумышленник, знающий резонансную частоту, например, кабеля клавиатуры персонального компьютера, может облучать его на этой частоте, а затем регистрировать коды нажатия клавиш в ретранслируемом резонансном сигнале благодаря вызванным ими изменениям импеданса. Для ПК высокочастотные излучения находятся в диапазоне до 1 ГГц с максимумом в полосе 50–300 МГц. Широкий спектр обусловлен наличием как основной, так и высших гармоник последовательностей коротких прямоугольных информационных импульсов. К появлению дополнительных составляющих в побочном электромагнитном излучении приводит также применение в вычислительных средствах высокочастотной коммутации. Говорить о какой-либо диаграмме направленности электромагнитных излучений ПК не имеет смысла, так как расположение его составных частей имеет много комбинаций. ПК имеет линейную поляризацию. Она определяется расположением соединительных кабелей, являющихся основными источниками излучений в ПК с металлическим кожухом на системном блоке.

Уровни побочных электромагнитных излучений СВТ регламентированы по условиям электромагнитной совместимости целым рядом зарубежных и отечественных стандартов. Так, например, согласно публикации № 22CISPR (специальный международный комитет по радиопомехам) для диапазона 230–1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудованием СВТ, на расстоянии 10 м не должен превышать 37 дБ. Однако излучения такого уровня могут быть перехвачены на значительных расстояниях.

Следовательно, соответствие электромагнитных излучений средств СВТ нормам на электромагнитную совместимость не обеспечивает сохранение конфиденциальности, обрабатываемой в них информации.

Электромагнитные излучения на частотах работы ВЧ генераторов ТСПИ и ВТСС

В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных устройств, генераторы измерительных приборов и т. д.

При внешних воздействиях информационного сигнала (например, электромагнитных полей) на элементах ВЧ генераторов индуктируются электрические сигналы. Приемными антеннами для магнитного поля могут

служить катушки индуктивности колебательных контуров, сглаживающие дроссели в цепях электропитания и т. д.

Приемниками электрического поля являются провода высокочастотных цепей и другие элементы. Индуктированные электрические сигналы могут вызвать модуляцию собственных ВЧ колебаний генераторов и излучение их в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ

Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи т. п.) возможно за счет преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные в результате фазового сдвига сигнала обратной связи на определенных частотах, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения находится в пределах рабочих частот элементов УНЧ (например, полупроводниковых приборов, электровакуумных ламп и т. п.), переходящих в нелинейный режим работы при перегрузке за счет действия положительной обратной связи. Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радиотехнической разведки, размещенными за пределами контролируемой зоны.

Зона, в которой возможен перехват побочных электромагнитных излучений с помощью разведывательного приемника, с последующей расшифровкой, содержащейся в них информации (т. е. зона, в пределах которой отношение «информационный сигнал/помеха» превышает допустимое нормированное значение), называется опасной зоной 2.

Электрические каналы утечки информации образуются за счет:

• наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;

• просачивания информационных сигналов в цепи электропитания ТСПИ;

• просачивания информационных сигналов в цепи заземления ТСПИ.

Наводки возникают при излучении элементами ТСПИ (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины соединительных линий ТСПИ и посторонних проводников. Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше нормированного уровня, называется (опасной) зоной.

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения. Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антенна представляет собой техническое средство небольшого объема, например, телефонный аппарат, громкоговоритель радиотрансляционной сети, реле и т. д. К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами (длинные линии): кабели, провода, металлические трубы и другие токопроводящие устройства.

Просачивание информационных сигналов в цепи электропитания. Просачивание возможно при наличии взаимно индуктивной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания.

Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала. Наводки на вторичные источники питания (ВИП) можно разделить натри вида: наводки в виде переменного напряжения с частотой питающей сети или ее гармоник, высокочастотные наводки, появляющиеся вследствие антенного эффекта проводов питающей сети, наводки, возникающие внутри блока вследствие появления паразитных связей через общие провода питания различных элементов.

Основными причинами появления помехи с частотой питающей сети или ее гармоник являются недостаточное сглаживание пульсаций в ВИП, паразитные связи элементов с первичными цепями ВИП, неэквипотенциальность точек заземления, наличие общих проводов питания, по которым возможна гальваническая связь. Из всех причин только первая не является следствием паразитных процессов. Величина наводки зависит не только от вида паразитной связи, но и от схемы подключения двухфазных ВИП к трехфазной промышленной сети.

Проводники, служащие для непосредственного соединения ТСПИ с контуром заземления, гальванической связи с землей, могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соединительных кабелей, металлические трубы систем отопления и

водоснабжения, металлическая арматура железобетонных конструкций и т. д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, в которой могут наводиться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам специальных устройств съема информации. Для перехвата электромагнитных сигналов используются специальные средства радио- и радиотехнической разведки.

Съем информации по электрическим каналам утечки информации

Для съема информации, обрабатываемой в ТСПИ, применяют главным образом электронные устройства перехвата информации – закладные устройства. Электронные устройства перехвата информации, устанавливаемые в ТСПИ, иногда называют аппаратными закладками. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Закладки устанавливаются в ТСПИ как иностранного так отечественного производства.

Литература:

[3, 4], [10] глава 1, [11] глава 1.

Контрольные вопросы:

1. В чем заключаются особенности радиоэлектронных каналов утечки информации?
2. Что называют техническими средствами приема, обработки и хранения информации (ТСПИ)?
3. Приведите определение случайной распределенной антенны.
4. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля в ближней зоне?
5. В каких границах располагается дальняя зона электромагнитного поля?
6. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля в дальней зоне?
7. Приведите определение вспомогательных технических средств и систем (ВТСС).
8. Приведите определение объекта ТСПИ.
9. Какие вы знаете виды радиоэлектронных каналов утечки информации?

10. Что представляет собой структура радиоэлектронных каналов утечки информации?

11. Приведите определение контролируемой зоны.

12. Что понимают под посторонними проводниками?

13. Приведите определение опасной зоны.

14. Приведите определение опасной зоны 1.

15. Приведите определение случайной антенны.

16. Назовите типы случайных антенн.

17. Приведите определение случайной сосредоточенной антенны.

18. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля, создаваемого магнитным диполем в ближней зоне?

19. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля, создаваемого магнитным диполем в дальней зоне?

20. Назовите электромагнитные каналы утечки информации ТСПИ.

21. За счет чего образуются электрические каналы утечки информации?

22. Каким образом создается параметрический канал утечки информации?

23. Перечислите виды паразитных связей в линиях передачи информации.

Тема 3. Технические каналы утечки акустической (речевой) информации

Перечень изучаемых вопросов:

Акустические сигналы. Линейные и энергетические характеристики акустического поля.

Характеристики речи (семантические, фонетические, физические). Спектр и типовые уровни речевого сигнала. Разборчивость речи. Методы оценки разборчивости речи.

Общая характеристика и классификация технических каналов утечки акустической (речевой) информации.

Методические указания к изучению:

С целью успешного усвоения материала по теме лекции необходимо последовательно изучить вопросы лекции, изложенные выше, используя при этом нижеприведенный краткий теоретический материал и рекомендованную литературу. При самостоятельной работе над материалом лекции ответить на контрольные вопросы.

Под техническим каналом утечки акустической (речевой) информации понимают совокупность объекта разведки, технического средства акустической

(речевой) разведки (ТС АР), с помощью которого перехватывается речевая информация, из физической среды, в которой распространяется информационный (акустический) сигнал.

Первичными источниками акустических колебаний являются механические колебательные системы, например, органы речи человека, а вторичными – преобразователи различного типа, в том числе электроакустические. Последние представляют собой устройства, предназначенные для преобразования акустических колебаний в электрические и обратно. К ним относятся пьез-элементы, микрофоны, телефоны, громкоговорители и другие устройства.

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронный и параметрические.

Средства акустической разведки могут использоваться не только для прослушивания и записи ведущихся в помещении разговоров, но и для перехвата акустических колебаний, возникающих, например, при выводе на печать текста на принтере. Современные специальные комплексы обработки акустической информации позволяют восстановить текст, выводимый на печать по перехваченным акустическим излучениям. В прямых акустических (воздушных) технических каналах утечки информации средой распространения акустических сигналов является воздух. В качестве датчиков средств разведки используются высокочувствительные микрофоны, преобразующие акустический сигнал в электрический. С использованием направленных микрофонов возможно прослушивание разговоров, ведущихся в контролируемом помещении при открытых окнах (форточках) на расстоянии до 100–150 м.

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

В акустовибрационных (вибрационных) технических каналах утечки информации акустические сигналы, возникающие при ведении разговоров в выделенном помещении, при воздействии на строительные конструкции (стены, потолки, полы, двери, оконные рамы и т. п.) и инженерно-технические коммуникации (трубы водоснабжения, отопления, канализации, воздуховоды и т. п.) вызывают в них упругие (вибрационные) колебания, которые и регистрируются датчиками средства разведки.

Для перехвата речевой информации по акустовибрационным каналам в качестве средств акустической разведки используются электронные стетоскопы и закладные устройства с датчиками контактного типа. Наиболее часто для

передачи информации с таких закладных устройств используется радиоканал, поэтому их называют радиостетоскопами.

В качестве датчиков средств акустической разведки используются контактные микрофоны (вибропреобразователи), чувствительность которых составляет от 50 до 100 мкВ/Па, что дает возможность прослушивать разговоры и улавливать слабые звуковые колебания через бетонные и кирпичные стены толщиной более 100 см, инженерные коммуникации через один-два этажа, воздуховоды на расстоянии от 6 до 20 м, а также любые двери и оконные рамы. Электронные стетоскопы и закладные устройства с датчиками контактного типа позволяют перехватывать речевую информацию без физического доступа «агентов» в выделенные помещения. Их датчики наиболее часто устанавливаются на наружных поверхностях зданий, на оконных проемах и рамах, в смежных (служебных и технических) помещениях за дверными проемами, ограждающими конструкциями, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы). Контактные микрофоны, соединенные с электронным усилителем, называют электронными стетоскопами. По вибрационному каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по металлоконструкциям здания).

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС, обладающих «микрофонным эффектом», а также путем «высокочастотного навязывания». Некоторые элементы ВТСС, в том числе трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов, дроссели ламп дневного света, электрореле и т. п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником акустических колебаний. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), изменяющейся по закону воздействующего информационного акустического поля, либо к модуляции токов, протекающих по этим элементам, информационным сигналом.

Например, акустическое поле, воздействуя на якорь электромагнита вызывного телефонного звонка, вызывает его колебание. В результате чего изменяется магнитный поток сердечника электромагнита. Изменение этого потока вызывает появление ЭДС самоиндукции в катушке звонка, изменяющейся по закону изменения акустического поля. ВТСС, кроме указанных элементов, могут содержать непосредственно электроакустические преобразователи. К таким ВТСС относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект электроакустического преобразования акустических колебаний в электрические часто называют «микрофонным эффектом». Причем из ВТСС, обладающих «микрофонным эффектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации.

Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающих «микрофонным эффектом», специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Технический канал утечки информации путем «высокочастотного навязывания» может быть осуществлен путем несанкционированного контактного введения токов высокой частоты от соответствующего генератора в линии (цепи), имеющие функциональные связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие электроакустического преобразования акустических сигналов в электрические. В силу того, что нелинейные или параметрические элементы ВТСС для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов используется специальные приемники с достаточно высокой чувствительностью. Наиболее часто такой канал утечки информации используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны.

Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т. д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по

амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация. Источник лазерного излучения и приемник оптического излучения могут быть установлены в одном или разных местах (помещениях).

Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы, иногда называемые «лазерными микрофонами». Работают они, как правило, в ближнем инфракрасном диапазоне волн. Акустооптический (лазерный) технический канал утечки информации образуется при облучении лазерным лучом вибрирующих в акустическом поле, возникающем при ведении разговоров, тонких отражающих поверхностей (стекол окон, картин, зеркал и т. д.). Данные системы наиболее эффективны для прослушивания разговоров в помещениях небольшого размера, которые по своим акустическим характеристикам близки к объемному резонатору, когда все двери и окна помещения достаточно хорошо герметизированы. Эффективны они и для подслушивания разговоров, ведущихся в салонах автомашин. Лазерные акустические системы разведки имеют дальность действия при приеме диффузноотраженного излучения до 100 м, а при установке на оконных стеклах триппель-призм – более 500 м.

Литература:

[3, 4, 8], [10] глава 1, [11] глава 1, [13, 14, 16].

Контрольные вопросы:

1. Методы и средства съема информации в высокочастотных и волоконно-оптических кабелях.
2. Методы защиты речевой информации. Защита речевой информации с помощью маскирующих сигналов.
3. Системы виброакустического зашумления.
4. Подавители диктофонов.
5. Блокираторы сотовых телефонов.
6. Защита речевой информации от узконаправленных микрофонов и лазерного съема.
7. Классификация и характеристика каналов утечки речевой информации.
8. Технические каналы утечки речевой информации и методы ее съема.
9. Методы дистанционного проникновения в помещение для скрытого съема аудио- и видеоинформации.
10. Технические средства съема аудиоинформации: малогабаритные проводные, радио- и стетоскопные микрофоны.
11. Технические средства съема аудиоинформации: направленные, лазерные и ИК микрофоны.

12. Технические средства съема аудиоинформации: эндовибраторы, аудиотранспондеры и вторичные микрофоны.

13. Технические средства съема аудиоинформации: устройства ВЧ навязывания, устройства с перемодуляцией радиоизлучений на нелинейных элементах, устройства с двойной модуляцией, устройства с питанием и передачей информации по сети, диктофоны.

Тема 4. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам

Перечень изучаемых вопросов:

Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам. Пассивные способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Активные способы и средства защиты объектов информатизации от утечки информации по техническим каналам.

Защищенные ПЭВМ. Экранирование технических средств их соединительных линий. Экранирующие материалы. Экранированные помещения (экранированные камеры). Заземление технических средств. Требования к заземлению ОТСС. Схемы заземления ОТСС.

Методы и средства измерения сопротивления заземления ОТСС. Требования к системе электропитания ОТСС. Требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания СВТ.

Методические указания к изучению:

С целью успешного усвоения материала по теме лекции необходимо последовательно изучить вопросы лекции, изложенные выше, используя при этом нижеприведенный краткий теоретический материал и рекомендованную литературу. При самостоятельной работе над материалом лекции ответить на контрольные вопросы.

Защита информации от утечки по техническим каналам — это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок.

Для защиты информации от утечки по электромагнитным каналам применяются как общие методы защиты от утечки, так и специфические – именно для этого вида каналов. Кроме того, защитные действия можно классифицировать на конструкторско-технологические решения, ориентированные на исключение возможности возникновения таких каналов, и

эксплуатационные, связанные с обеспечением условий использования тех или иных технических средств в условиях производственной и трудовой деятельности.

Конструкторско-технологические мероприятия по локализации возможности образования условий возникновения каналов утечки информации за счет побочных электромагнитных излучений и наводок в технических средствах обработки и передачи информации сводятся к рациональным технологическим решениям, к числу которых относятся:

- экранирование элементов и узлов аппаратуры;
- ослабление электромагнитной, емкостной, индуктивной связи между элементами и токонесущими проводами;
- фильтрация сигналов в цепях питания и заземления и другие меры, связанные с использованием ограничителей, развязывающих цепей, систем взаимной компенсации, ослабителей по ослаблению или уничтожению ПЭМИН.

Экранирование позволяет защитить их от нежелательных воздействий акустических и электромагнитных сигналов и излучений собственных электромагнитных полей, а также ослабить (или исключить) паразитное влияние внешних излучений. Экранирование бывает электростатическое, магнитостатическое и электромагнитное. Электростатическое экранирование заключается в замыкании силовых линий электростатического поля источника на поверхность экрана и отводе наведенных зарядов на массу и на землю. Такое экранирование эффективно для устранения емкостных паразитных связей. Экранирующий эффект максимален на постоянном токе и с повышением частоты снижается.

Магнитостатическое экранирование основано на замыкании силовых линий магнитного поля источника в толще экрана, обладающего малым магнитным сопротивлением для постоянного тока и в области низких частот. С повышением частоты сигнала применяется исключительно электромагнитное экранирование. Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экрана вихревым токам) полем обратного направления. Если расстояние между экранирующими цепями, проводами, приборами составляет 10 % от четверти длины волны, то можно считать, что электромагнитные связи этих цепей осуществляются за счет обычных электрических и магнитных полей, а не в результате переноса энергии в пространстве с помощью электромагнитных волн. Это дает возможность отдельно рассматривать экранирование электрических и магнитных полей, что очень важно, так как на практике преобладает какое-либо одно из полей и подавлять другое нет необходимости.

Заземление и металлизация аппаратуры и ее элементов служат надежным средством отвода наведенных сигналов на землю, ослабления паразитных связей

и наводок между отдельными цепями. Фильтры различного назначения служат для подавления или ослабления сигналов при их возникновении или распространении, а также для защиты систем питания аппаратуры обработки информации. Для этих же целей могут применяться и другие технологические решения.

Эксплуатационные меры ориентированы на выбор мест установки технических средств с учетом особенностей их электромагнитных полей с таким расчетом, чтобы исключить их выход за пределы контролируемой зоны. В этих целях возможно осуществлять экранирование помещений, в которых находятся средства с большим уровнем побочных электромагнитных излучений (ПЭМИ). Электронные и радиоэлектронные средства, особенно средства электросвязи, обладают основным электромагнитным излучением, специально вырабатываемым для передачи информации, и нежелательными излучениями, образующимися по тем или иным причинам конструкторско-технологического характера.

В качестве методов защиты и ослабления электромагнитных полей энергетического помещения используется установка электрических фильтров, применяются пассивные и активные экранирующие устройства, и специальное размещение аппаратуры и оборудования.

Установка экранирующих устройств может производиться либо в непосредственной близости от источника излучения, либо на самом источнике, либо, наконец, экранируется помещение, в котором размещены источники электромагнитных сигналов.

Рациональное размещение аппаратуры и технических средств в энергетическом помещении может существенно повлиять как на результирующую напряженность электромагнитного поля внутри помещения, так и на результирующее электромагнитное поле за его пределами.

Рациональное размещение предполагает перестановку отдельных элементов оборудования помещений или отдельных групп аппаратов и технических средств с тем, чтобы новое расположение приводило к взаимной компенсации напряженности электромагнитных полей опасных сигналов в заданных зонах.

Рациональное размещение аппаратуры в отдельных случаях может оказаться определяющим.

Для реализации мероприятий по рациональному размещению аппаратуры и иного оборудования энергетических помещений с точки зрения ослабления ПЭМИН необходимо:

- иметь методику расчета электромагнитных полей группы источников опасных сигналов;
- иметь методы формализации и алгоритмы решения оптимизационных задач размещения аппаратуры.

Мероприятия по защите информации от ее утечки за счет электромагнитных излучений прежде всего включают в себя мероприятия по воспрещению возможности выхода этих сигналов за пределы зоны и мероприятия по уменьшению их доступности. Следует отметить степень опасности электромагнитных излучений при реализации мероприятий по защите информации. Так как это электромагнитные волны, то особенности их распространения в пространстве по направлению и по дальности определяются диапазоном частот (длин волн) и мощностью излучения.

Дальность и направленность излучения определяются физической природой распространения соответствующего вида электромагнитных волн и пространственного расположения источника опасного сигнала и средств его приема. Учитывая особенности распространения электромагнитных колебаний, определяющихся прежде всего мощностью излучения, особенностями распространения и величинами поглощения энергии в среде распространения, правомерно ставить вопрос об установлении их предельно допустимых интенсивностей (мощностей), потенциально возможных для приема средствами злоумышленников. Эти допустимые значения интенсивностей принято называть нормами или допустимыми значениями. Процесс определения или выработки норм называется нормированием, которое включает в первую очередь собственно выбор критерия нормирования, выбор и обоснование нормируемого параметра и определение его предельно допустимого значения. Нормы могут быть международные, федеральные и отраслевые. Не исключается наличие специальных норм для конкретных изделий и предприятий.

Защита от утечки информации за счет побочных электромагнитных излучений самого различного характера предполагает:

- размещение источников и средств на максимально возможном удалении от границы охраняемой (контролируемой) зоны;
- экранирование зданий, помещений, средств кабельных коммуникаций;
- использование локальных систем, не имеющих выхода за пределы охраняемой территории (в том числе систем вторичной часофикации, радиофикации, телефонных систем внутреннего пользования, диспетчерских систем, систем энергоснабжения и т. д.);
- развязку по цепям питания и заземления, размещенных в границах охраняемой зоны;
- использование подавляющих фильтров в информационных цепях, цепях питания и заземления.

Паразитная генерация усилителей возникает из-за неконтролируемой положительной обратной связи за счет конструктивных особенностей схемы или за счет старения элементов. Самовозбуждение может возникнуть и при отрицательной обратной связи из-за того, что на частоты, где усилитель вместе

с цепью обратной связи вносит сдвиг фазы на 180°, отрицательная обратная связь превращается в положительную. Самовозбуждение усилителей обычно происходит на высоких частотах, выходящих за пределы рабочей полосы частот (вплоть до КВ и УКВ диапазонов). Частота самовозбуждения модулируется акустическим сигналом, поступающим на усилитель, и излучается в эфир как обычным радиопередатчиком. Дальность распространения такого сигнала определяется мощностью усилителя (т. е. передатчика) и особенностями диапазона радиоволн. В качестве защитных мер применяется контроль усилителей на самовозбуждение с помощью радиоприемников типа индикаторов поля, работающих в достаточно широком диапазоне частот, что обеспечивает поиск опасного сигнала. Циркулирующая в тех или иных технических средствах конфиденциальная информация может попасть в цепи и сети электрического питания и через них выйти за пределы контролируемой зоны. Например, в линию электропитания высокая частота может передаваться за счет паразитных емкостей трансформаторов блоков питания.

В качестве мер защиты широко используются методы развязки (разводки) цепей питания с помощью отдельных стабилизаторов, преобразователей, сетевых фильтров для отдельных средств или помещений. Возможно использование отдельных трансформаторных узлов для всего энергоснабжения объекта защиты расположенного в пределах контролируемой территории. Это более надежное решение локализации данного канала утечки.

Одним из важных условий защиты информации от утечки по цепям заземления является правильное их оборудование.

Заземление – это устройство, состоящее из заземлителей – проводников, соединяющих заземлители с электронными и электрическими установками, приборами, машинами. Заземлители могут быть любой формы: в виде трубы, стержня, полосы, листа. Заземлители выполняют защитную функцию и предназначаются для соединения с землей приборов защиты Отношение потенциала заземлителя к стекающему с него току называется сопротивлением заземления Величина заземления зависит от удельного сопротивление. При устройстве заземления в качестве заземлителей, чаще всего применяются стальные трубы длиной 2–3 м и диаметром 25–50 мм и стальные полосы сечением 50–100 мм^2. Заземлители следует соединять между собой шинами с помощью сварки. Сечение шин и магистралей заземления по условиям механической прочности и получения достаточной проводимости рекомендуется брать не менее 24 х 4 мм^2.

Магистрали заземления вне здания надо прокладывать на глубине около 1,5 м, а внутри здания – по стенам или специальным каналам таким образом, чтобы их можно было внешне осматривать на целостность и на наличие контактного подключения. Следует отметить, что использовать в качестве

заземления металлические конструкции зданий и сооружений, имеющих соединения с землей (отопление, водоснабжение), не рекомендуется.

Литература:

[3, 4, 9], [10] глава 1, [11] глава 1.

Контрольные вопросы:

1. Какие существуют требования к средствам подавления сигналов побочных электромагнитных излучений и наводок?
2. Опишите методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей.
3. Как осуществляется экранирование электрических, магнитных и электромагнитных полей?
4. Как осуществляется экранирование проводов и кабелей?
5. Какие используются материалы для экранирования?
6. Какие существуют требования к заземлению?
7. Опишите известные конструкции конструкция заземлителей.
8. Как осуществляется развязка цепей электропитания и в чем состоит ее назначение?
9. Как осуществляется фильтрация цепей электропитания и в чем состоит ее назначение?
10. Каково назначение средств активного линейного зашумления?
11. Каково назначение средств пространственного зашумления?

Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Перечень изучаемых вопросов:

Пассивные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Активные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Звуко- и виброизоляция выделенных помещений, глушители шума. Звукопоглощающие материалы. Специальные защищенные помещения.

Требования к системе виброакустической маскировки. Принципы построения низкочастотных генераторов шума. Принципы построения акустических излучателей и виброизлучателей.

Пассивные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам (ограничение сигналов малой амплитуды, фильтрация высокочастотных сигналов навязывания, отключение акустоэлектрических преобразователей опасных сигналов). Активные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам.

Методические указания к изучению:

С целью успешного усвоения материала по теме лекции необходимо последовательно изучить вопросы лекции, изложенные выше, используя при этом нижеприведенный краткий теоретический материал и рекомендованную литературу. При самостоятельной работе над материалом лекции ответить на контрольные вопросы.

Защита информации от утечки по акустическому каналу – это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей.

Основными мероприятиями в этом виде защиты выступают организационные и организационно-технические меры. Организационные меры предполагают проведение архитектурно-планировочных, пространственных и режимных мероприятий, а организационно-технические – пассивных (звукоизоляция, звукопоглощение) и активных (звукоподавление) мероприятий. Не исключается проведение и технических мероприятий за счет применения специальных защищенных средств ведения конфиденциальных переговоров.

Архитектурно-планировочные меры предусматривают предъявление определенных требований на этапе проектирования зданий и помещений или их реконструкцию и приспособление с целью исключения или ослабления неконтролируемого распространения звуковых полей непосредственно в воздушном пространстве или в строительных конструкциях в виде структурного звука. Эти требования могут предусматривать как выбор расположения помещений в пространственном плане, так и их оборудование необходимыми для акустической безопасности элементами, исключающими прямое или отраженное в сторону возможного расположения злоумышленника распространение звука. В этих целях двери оборудуются тамбурами, окна ориентируются в сторону охраняемой (контролируемой) от присутствия посторонних лиц территории и пр.

Режимные меры предусматривают строгий контроль пребывания в контролируемой зоне сотрудников и посетителей.

Организационно-технические меры предусматривают использование звукопоглощающих средств. Пористые и мягкие материалы типа ваты, ворсистые ковры, пенобетон, пористая сухая штукатурка являются хорошими звукоизолирующими и звукопоглощающими материалами – в них очень много поверхностей раздела между воздухом и твердым телом, что приводит к многократному отражению и поглощению звуковых колебаний. Для облицовки поверхностей стен и потолков широко используются специальные герметические акустические панели, изготавливаемые из стекловаты высокой плотности и различной толщины (от 12 до 50 мм). Такие панели обеспечивают поглощение звука и исключают его распространение в стеновых конструкциях.

Степень отражения и поглощения звуковой энергии определяется частотой звука и материалом отражающих (поглощающих) конструкций (пористостью, конфигурацией, толщиной). Устраивать звукоизолирующие покрытия стен целесообразно в небольших по объему помещениях, так как в больших помещениях звуковая энергия максимально поглощается, еще не достигнув стен. Известно, что воздушная среда обладает некоторой звукопоглощающей способностью и сила звука убывает в воздухе пропорционально квадрату расстояния от источника. Внутри помещения уровень громкости звучит выше, чем на открытом пространстве, из-за многократных отражений от различных поверхностей, обеспечивающих продолжение звучания даже после прекращения работы источника звука (реверберация). Уровень реверберации зависит от степени звукопоглощения.

Величина звукопоглощения определяется коэффициентом звукопоглощения, а и размерами звукопоглощающей поверхности. Значения коэффициентов звукопоглощения различных материалов известны. Для обычных пористых материалов – войлок, вата, пористая штукатурка – оно колеблется в пределах 0,2–0,8.

Кирпич и бетон почти не поглощают звук (а = 0,01–0,03).

Степень ослабления звука при применении звукопоглощающих покрытий определяется в децибелах. Например, при обработке кирпичных стен (а = 0,03) пористой штукатуркой (а = 0,3) звуковое давление в помещении ослабляется на 10 дБ.

Для определения эффективности защиты звукоизоляции используются шумомеры.

Шумомер — это измерительный прибор, который преобразует колебания звукового давления в показания, соответствующие уровню звукового давления. В сфере акустической защиты речи используются аналоговые шумомеры. По точности показаний шумомеры подразделяются на четыре класса. Шумомеры нулевого класса служат для лабораторных измерений, первого – для натурных измерений, второго – для общих целей; шумомеры третьего класса используются для ориентированных измерений. На практике для оценки степени защищенности акустических каналов используются шумомеры второго класса, реже – первого.

Измерения акустической защищенности реализуются методом образцового источника звука. Образцовым называется источник с заранее известным уровнем мощности на определенной частоте (частотах).

Выбирается в качестве такого источника магнитофон с записанным на пленку сигналом на частотах 500 Гц и 1000 Гц, модулированным синусоидальным сигналом в 100–120 Гц. Имея образцовый источник звука и шумомер, можно определить поглощающие возможности помещения.

Величина акустического давления образцового источника звука известна. Принятый с другой стороны стены сигнал замерен по показаниям шумомера. Разница между показателями и дает коэффициент поглощения.

В зависимости от категории выделенного помещения эффективность звукоизоляции должна быть разной. Рекомендуются следующие нормативы поглощения на частотах 500 и 1000 Гц соответственно.

Для проведения оценочных измерений защищенности помещений от утечки по акустическим и вибрационным каналам используются так называемые электронные стетоскопы. Они позволяют прослушивать ведущиеся в помещении переговоры через стены, полы, потолки, системы отопления, водоснабжения, вентиляционные коммуникации и другие металлоконструкции. В качестве чувствительного элемента в них используется датчик, преобразующий механические колебания звука в электрический сигнал. Чувствительность стетоскопов колеблется от 0,3 до 1,5 v/дБ. При уровне звукового давления 34–60 дБ, соответствующем средней громкости разговора, современные стетоскопы позволяют прослушивать помещения через стены и другие ограждающие конструкции толщиной до 1,5 м. После проверки с помощью такого стетоскопа возможных каналов утечки принимаются меры по их защите.

В качестве примера можно привести электронный стетоскоп «Бриз» («Элерон»). Рабочие диапазоны частот – 300–4000 Гц, питание автономное. Предназначен для выявления вибрационно-акустических каналов утечки информации, циркулирующей в контролируемом помещении, через ограждения конструкции или коммуникации, а также для контроля эффективности средств защиты информации.

В тех случаях, когда пассивные меры не обеспечивают необходимого уровня безопасности, используются активные средства. К активным средствам относятся генераторы шума – технические устройства, вырабатывающие шумоподобные электронные сигналы. Эти сигналы подаются на соответствующие датчики акустического или вибрационного преобразования. Акустические датчики предназначены для создания акустического шума в помещениях или вне их, а вибрационные – для маскирующего шума в ограждающих конструкциях. Вибрационные датчики приклеиваются к защищаемым конструкциям, создавая в них звуковые колебания посредством генератора шума.

В качестве примера генераторов шума можно привести систему виброакустического зашумления «Заслон». Система позволяет защитить до 10 условных поверхностей, имеет автоматическое включение вибропреобразователей при появлении акустического сигнала. Эффективная шумовая полоса частот 100–6000 Гц.

Современные генераторы шума обладают эффективной полосой частот в пределах от 100–200 Гц до 5000–6000 Гц. Отдельные типы генераторов имеют

полосу частот до 10 000 Гц. Число подключаемых к одному генератору датчиков различно: от 1–2 до 20–30 штук. Это определяется назначением и конструктивным исполнением генератора.

Используемые на практике генераторы шума позволяют защищать информацию от утечки через стены, потолки, полы, окна, двери, трубы, вентиляционные коммуникации и другие конструкции с достаточно высокой степенью надежности.

Фильтры и аналогичные приспособления встраиваются в разрыв линии или в аппарат, блокируют возможность перехвата и дешифровки побочных излучений (ПЭМИН). Они способны обеспечить предотвращение перехвата:

- акустических данных при помощи метода ВЧ-навязывания;
- речевой информации, которую могут перехватить из-за микрофонного эффекта телефонного аппарата;
- речевой информации в помещениях с помощью микрофонов, передающих данные по телефонной линии на высоких частотах.

Основной минус средств – ограниченность действия, они блокируют закладные устройства, работающие по принципам ПЭМИН, но не способны справиться с акустическими закладками.

Приборы для постановки активной заградительной помехи работают с широким диапазоном закладных электронных устройств. Задача решается способами зашумливания – добавления в телефонную линию различного вида сигналов (заградительных помех), а также модификацией стандартных параметров напряжения телефонной линии. Помехи при прохождении по линии в несколько раз превосходят уровень стандартного сигнала и компенсируются, гасятся дополнительными устройствами при достижении речевой информацией абонента. Помехи могут обеспечить смещение или «размывание» несущей частоты передатчика, внезапные скачки передающей частоты, искажение высокочастотного сигнала, дополнительную модуляцию, снижение мощности электромагнитного излучения, передаваемого по телефонным каналам утечки информации.

Итак, защита от утечки по акустическим каналам реализуется:

- применением звукопоглощающих облицовок, специальных дополнительных тамбуров дверных проемов, двойных оконных переплетов;
- использованием средств акустического зашумления объемов и поверхностей;
- закрытием вентиляционных каналов, систем ввода в помещения отопления, электропитания, телефонных и радиокоммуникаций;
- использованием специальных аттестованных помещений, исключающих появление каналов утечки информации.

Литература:

[3, 4], [10] глава 1, [11] глава 1, [16, 20].

Контрольные вопросы:

1. Назовите методы энергетического скрытия акустических сигналов.
2. Проведите классификацию звукоизоляции ограждений, кабин, акустических экранов, глушителей. Способы повышения звукоизоляции окон и дверей.
3. Как реализуется звукоизоляция и звукопоглощение?
4. Назовите основные параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей.
5. Какие есть способы повышения звукоизоляции окон?
6. Какие есть способы повышения звукоизоляции дверей?
7. Назовите основные звукопоглощающие материалы.
8. Какие вы знаете способы применения основных звукопоглощающих материалов?
9. Назовите типы и способы применения генераторов акустического и вибрационного зашумления.
10. Какие существуют способы оценки энергетических и информационных показателей безопасности речевой информации?

Тема 6. Методы и средства контроля защищенности информации, обрабатываемой СВТ

Перечень изучаемых вопросов:

Показатели эффективности защиты информации, обрабатываемой СВТ, от утечки по техническим каналам. Методы контроля эффективности защиты информации, обрабатываемой СВТ. Требования к средствам измерения ПЭМИН СВТ и условиям проведения измерений.

Порядок проведения аттестационных испытаний СВТ при контролях эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИ.

Порядок проведения аттестационных испытаний СВТ при контроле эффективности защиты СВТ от утечки информации, возникающей за счет наводок информативных сигналов на токопроводящие коммуникации.

Методические указания к изучению:

С целью успешного усвоения материала по теме лекции необходимо последовательно изучить вопросы лекции, изложенные выше, используя при этом нижеприведенный краткий теоретический материал и рекомендованную

литературу. При самостоятельной работе над материалом лекции ответить на контрольные вопросы.

Использование компьютеров и другой техники при обработке конфиденциальной информации создает побочные электромагнитные излучения. Они могут быть использованы: перехвачены и преобразованы в данные. Утечка информации по каналам ПЭМИН (побочные электромагнитные излучения и наводки) стала благоприятной средой для работы злоумышленников уже в 70-е годы XX века, и технологии продолжают совершенствоваться.

Основой технологии перехвата становится техническое закладное устройство, скрытно внедренное в компьютер или помещение, где он находится. Впервые технология начала использоваться в период Первой мировой войны для перехвата сигналов военных телефонов и радиостанций. Тогда выяснилось, что при работе проявляются демаскирующие признаки в виде побочных излучений оборудования и это излучение может использоваться для получения информации. По мере развития технологий создавались средства ПЭМИН-нападения и ПЭМИН-защиты. Иногда в научной и технической литературе встречается термин ПЭМИ (паразитные электромагнитные излучения), определение термина приводит ГОСТ Р 50922-2006, который под ПЭМИ понимает паразитные электромагнитные излучения, возникающие при работе средств электронной обработки информации.

Первой серьезной демонстрацией возможности перехвата побочных излучений стала выставка в Каннах, проходящая в рамках Международного конгресса по вопросам безопасности ЭВМ 1985 года. Участникам показали, что данные, выведенные на экран компьютера, можно перехватить путем анализа электромагнитных полей.

Электромагнитное излучение, возникающее в процессе обработки информации, имеет различную природу. Это значит, что для снятия данных необходимо использовать различные технологии и типы электронных закладных устройств. Наиболее часто разведки или конкуренты используют:

- излучение отдельных элементов технических средств обработки данных и передачи информации (ТСПИ), включая кабели электропитания и заземления;
- излучения на частотах работы высокочастотных генераторов;
- излучения на частотах самовозбуждения усилителей низкой частоты.

В техническом канале утечки информации (ТКУИ) носителем данных становится электроток и колебания его напряжения. Помимо напряжения изменяются сила тока, частота и фаза, колебания могут являться носителями информационного сигнала. Электрические и магнитные поля возникают при прохождении тока через детали техники, провода. Побочные излучения наводятся на металлические (токопроводящие) элементы строительных

конструкций, с возникающих полей производят съем данных. Перехват информации осуществляют или в пределах контролируемой зоны, попадание в которую невозможно без пропусков, или вне ее, где снятие напряжения происходит с выходящих из зоны проводников: строительных конструкций, элементов систем водоснабжения, отопления, вентиляции, проводов электрооборудования, систем кондиционирования – посторонних проводников.

Раньше практиковалось параллельное подключение закладных устройств к линиям связи, но развитие технологий привело к созданию возможности быстрого выявления при измерении напряжения, его падение меняет рабочие характеристики линии связи. Сейчас средства перехвата подключаются к линии связи через согласующее устройство, незначительно снижающее падение напряжения, или через специальное устройство компенсации падения напряжения. Контактный способ все еще применяется, но только для снятия данных с коаксиальных и низкочастотных кабелей связи.

Некоторые кабели связи производятся так, что внутри них предусмотрено повышенное давление воздуха. Его снижение вызывает срабатывание сигнализации, поэтому закладные устройства используют механизм, исключающий риск снижения давления.

Среди устройств, которые дают возможность для снятия информации, могут быть различные приспособления: задающие генераторы, генераторы тактовой частоты, гетеродины радиоприемных и телевизионных устройств, видеокамер, генераторы измерительных приборов.

Более подробная классификация каналов ПЭМИН предложена ГОСТ, на первом уровне разделившим их на электрические и магнитные. Каналы утечки информации подразделяются на:

- ПЭМИ от информационных цепей;
- ПЭМИ от электрических сетей технических средств обработки информации;
- паразитное электромагнитное излучение;
- наводки.

Далее стандарт дает классификацию наводок:

- наводки в электрических цепях, имеющих собственный выход за пределы объекта обработки информации;
- наводки в линиях связи;
- наводки, вызванные побочными и паразитными излучениями, содержащими информацию;
- наводки в цепях электропитания, вызванные побочными и паразитными излучениями, содержащими информацию;
- наводки в цепях заземления.

Побочные электромагнитные излучения возникают при работе с компьютером в следующих случаях:

- вывод данных на монитор;
- ввод текста с клавиатуры;
- запись данных на съемные носители;
- считывание информации со съемных носителей;
- передача данных по телекоммуникационным каналам связи;
- вывод данных на периферийные устройства печати – принтеры, плоттеры;
- общение по голосовым мессенджерам или в режиме телеконференции;
- сканирование документов;
- запись информации от сканера на магнитный носитель.

Для перехвата данных используются устройства:

- радиотехнической разведки;
- технические средства разведки (ТСР) побочных электромагнитных излучений и наводок (ПЭМИН).

Устройства радиоперехвата требуют размещения в том же помещении, где находится техника, ТСР ПЭМИН могут размещаться за пределами охраняемого периметра.

Если контактный способ снятия информации исключен из-за риска выявления закладных устройств, применяется индукционный метод. При этом используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов. Их и снимают индукционные датчики. Обычно этот способ применяется для получения данных с симметричных кабелей токов высокой частоты.

Современным средствам снятия информации не мешает изоляция кабеля. Они способны получить данные, даже если он защищен на двух уровнях: сначала обмотан металлической проволокой, а затем помещен в металлический футляр. Если необходимо получить информацию бесконтактно с телефонных линий, не обладающих дополнительной защитой, применяются высокочувствительные низкочастотные усилители, оборудованные антеннами, которые работают на магнитном принципе. Часто устройства съема информации дополнительно оснащены радиопередатчиками для пересылки данных на приемник, иногда он может быть установлен за несколько километров от охраняемой зоны. Фиксация радиоизлучения создает дополнительные возможности выявления закладных устройств.

Пространство вокруг работающего компьютера, в котором напряжение электромагнитного поля превышает фоновые значения, начинается, в зависимости от мощности и защищенности компьютера, с радиуса в

10-15 метров и достигает нескольких десятков. Оно называется зоной R2, и в нем возможен перехват данных работающим средством электромагнитной разведки. Обычно параметры зоны указываются в сертификате соответствия оборудования.

В работе государственных органов власти — МИД, ряда правоохранительных органов – часто используются тщательно защищенные компьютеры семейства Secret. Эти машины представляют собой модификацию серийных отечественных или зарубежных ПЭВМ, доработанных для повышения характеристик защищенности информации от утечки по техническим каналам. Это достигается за счет побочных электромагнитных излучений и наводок (ПЭМИН) и НСД. Для компьютеров этого семейства зона R2 не превышает 8–10 м. Такие ПЭВМ после доработки и в целях сертификации проходят специальные проверки и исследования, предназначенные для выявления при помощи контрольно-измерительной техники возможных технических каналов утечки данных.

Доработка проводится без использования специальных средств зашумливания, параметры желаемой зоны R2 устанавливаются заказчиком при подготовке ТЗ.

Комплекс средств для защиты информации от утечки по каналам ПЭМИН делится на активные и пассивные механизмы. Нецелесообразно внедрять их в качестве реакции на угрозу, когда утечка уже произошла. Предварительно требуется составить план мероприятий, в котором будут учтены все возможные каналы и угрозы, уже реализованные злоумышленниками и гипотетические.

При разработке плана мероприятий отдельно рассматриваются:

- способы выявления побочных электромагнитных излучений и наводок;
- организационные меры борьбы;
- защита электромагнитного поля;
- меры защиты компьютерного оборудования;
- меры защиты линий связи.

Организационные меры реализуются в любом случае, меры защиты ПЭВМ и линий связи – исходя из результатов аудита безопасности.

Вне зависимости от того, используются ли злоумышленниками побочные излучения и наводки от компьютеров, первым этапом борьбы с ними становится изолирование рабочих машин от Интернета, чтобы избежать передачи вовне перехваченной информации. Маршрутизатор является обязательным средством, но не единственным. Серьезную дополнительную защиту от утечек данных по каналам ПЭМИН, несанкционированного взаимодействия приложений, способных передавать информацию друг другу и обеспечивать ее утечку по менее контролируемым каналам, от проникновения в информационную систему организации вредоносных программ дает межсетевой экран.

В государственных организациях неуклонно соблюдается принцип изоляции компьютеров, на которых обрабатываются данные повышенного уровня конфиденциальности, от общей сети Интернет. Иногда это решается полным отказом от взаимодействия, иногда оборудование подключается к государственным и ведомственным сетям Рунета с повышенным уровнем защиты.

Если сотруднику предоставляются две рабочие машины, одна из которых подключена к Интернету, вторая – нет, это не решает задачу. Информация, обрабатываемая в локальной сети, и побочные излучения компьютеров, направленные на кабели локальной сети, с легкостью наводятся на провода машины, подключенной к Интернету. Кабели открытой сети часто выходят за пределы охраняемого помещения, и подключить к ним закладное устройство несложно. Это создает необходимость прокладывания кабелей с соблюдением рекомендованных ФСТЭК правил безопасности. Разработку топологии прокладки проводов лучше проводить на первом этапе обустройства помещения, до установки оборудования. Правильность построения защищенной от перехвата данных по каналам ПЭМИН сети подтверждается аттестацией.

Дополнительный риск создает использование вредоносных программ. Выполняя формально не запрещенные операции, они генерируют дополнительное излучение, модулированное информационным сигналом, которое считывается закладными устройствами. Интересно, что в рамках программы реализуются и защитные меры, разработаны специальные шрифты, которые при вводе данных способны погасить побочные излучения.

При анализе оборудования на побочные излучения нельзя ограничиваться компьютерами, дополнительно проверяются:

- средства связи;
- средства звукоусиления и звукозаписи;
- факсовые аппараты;
- оборудование для проведения видеоконференций;
- элементы умного дома;
- сигнализации всех типов;
- диспетчерская связь;
- оргтехника;
- метрологическая аппаратура;
- световые приборы, передающие информацию путем преобразования электромагнитного излучения в световое;
- СКУД.

Проверка ведется при помощи специального оборудования по заранее составленному плану. Закладные устройства могут быть подключены к оборудованию, проводам питания и заземления, электророзеткам. Информация

по наводкам легко переходит от одного кабеля к другому, поэтому проверке подлежат все провода и сети, если они заранее не размещены недоступным способом или не экранированы. Также в зоне риска находятся пульты управления технологическим оборудованием, распределительные щиты.

Основной организационной мерой становится защита помещения, при необходимости – с дальнейшей сертификацией степени защищенности по методике ФСТЭК. Чаще всего мерой защиты становится «клетка Максвелла» – решетка из металла, встроенная в стены помещения. Побочные излучения распространяются по ней, выходя за пределы комнаты в состоянии, непригодном для качественного съема информации. Аттестация помещения станет необходимой мерой, гарантирующей защиту. Для защиты от ЗУ, которые могут установить внутри такого помещения, используется контроль доступа лиц и их проверка на входе в организацию на предмет проноса закладных устройств.

Существует комплекс мероприятий, изменяющих параметры электромагнитного поля и снижающих риск утечки данных по каналам ПЭМИН.

Существуют многочисленные способы активного подавления электромагнитных излучений:

- метод «синфазной» низкочастотной маскирующей помехи: в провод по определенному временному алгоритму подаются сигналы маскирующего низкочастотного шума. Уровень сигнала в разы превосходит передаваемый, и снятие данных становится невозможным;
- использование высокочастотной маскирующей помехи. Низкочастотный сигнал подавляет речевой при передаче по линии. Для маскировки применяются широкополосные аналоговые сигналы типа «белого шума» или дискретные сигналы типа псевдослучайной последовательности электромагнитных импульсов;
- применение ультразвуковой маскирующей помехи. Принцип работы аналогичен предыдущему, создавать ультразвуковые помехи проще, но качество маскировки снижается;
- использование низкочастотной маскирующей помехи. Способ рассчитан на подавление работы подключенных диктофонов, вместо речи на них записывается «белый шум»;
- повышение напряжения. Оно переводит закладки в нелинейный режим работы, ЗУ с параллельным подключением отключаются;
- понижение напряжения. Оно также подавляет работу устройств съема информации;
- компенсационный способ, на линию подается чистый шум;
- метод «выжигания». На линию направляются высоковольтные импульсы, выжигающие входные каналы ЗУ.

Выбор технических средств подавления напряжения электромагнитного поля в каналах утечки информации ПЭМИН выбирается в зависимости от частоты использования городской телефонной связи.

При защите информации от утечек основным принципом становится снижение уровня излучения или использование шумов, которые сделают ПЭМИН нечитаемым, не дадут возможность преобразования. В первую очередь защищаются компьютеры.

Если нет возможности приобрести уже защищенное по модели Secret оборудование, возможна доработка имеющегося силами специальных лицензированных организаций по направлениям:

- использование фильтра-генератора для защиты цепей питания и заземления;
- применение устройств зашумливания.

Дополнительно, если компьютер не защищен при помощи сертифицированных ФСТЭК технологий, используются генераторы шума. Уровень маскирующего сигнала обычно на 10–20 дБ превышает уровень побочных излучений. Государственная комиссия по радиочастотам при Минсвязи выделила для генераторов шума полосу радиочастот 0,1–1000 МГц. Пиковые значения напряженности электромагнитного поля для каждой из подгрупп частот установлены в ГОСТ, и они проявляются в пределах 10 м от работающего компьютера. Активная форма защиты иногда предполагает использование одновременно нескольких генераторов для стоящих рядом машин, что ставит перед специалистами задачу сложить напряжения и избежать их конфликта, приводящего к появлению неконтролируемых зон.

Интересно, что использование генераторов шума в повышенном количестве является демаскирующим признаком, способным оповестить заинтересованных лиц о том, что в помещении обрабатывается информация ограниченного доступа.

Литература:

[3, 4], [10] глава 1, [11] глава 1.

Контрольные вопросы:

1. Что понимают под аттестационной проверкой?
2. Сущность контроля эффективности защиты информации.
3. Определение показателя эффективности защиты информации.
4. Что понимают под нормами эффективности защиты информации?
5. Что понимают под методом контроля эффективности защиты информации?
6. Виды методов технического контроля.

7. Цель и сущность технического контроля эффективности защиты информации.

8. Виды контроля эффективности защиты информации.

9. Каким может быть технический контроль эффективности технической защиты информации по характеру проведения и содержанию?

10. Средство контроля эффективности защиты информации (определение).

Тема 7. Методы и средства контроля защищенности речевой информации от утечки по техническим каналам

Перечень изучаемых вопросов:

Показатели защищенности речевой информации от утечки речевой информации по техническим каналам. Методы контроля эффективности защиты ВП от утечки речевой информации по техническим каналам.

Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по прямым акустическим, акустовибрационным и акустооптическому каналам.

Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по акустоэлектрическим каналам. Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по прямым акустическим каналам.

Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по акустовибрационным и акустооптическому каналам.

Порядок проведения контроля ВТСС на подверженность акустоэлектрическим преобразованиям. Порядок проведения контроля ВТСС на подверженность «высокочастотному навязыванию».

Методические указания к изучению:

С целью успешного усвоения материала по теме лекции, не обходимо последовательно изучить вопросы лекции, изложенные выше, используя при этом нижеприведенный краткий теоретический материал и рекомендованную литературу. При самостоятельной работе над материалом лекции ответить на контрольные вопросы.

Под информацией понимаются сведения (сообщения, данные) независимо от формы их представления. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). К информации ограниченного доступа относятся информация, содержащая сведения, составляющие государственную, коммерческую, служебную, личную или семейную и иную тайну, персональные данные граждан (физических лиц) и т. п.

К защищаемой информации относится информация ограниченного доступа, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми обладателем информации, то есть лицом, самостоятельно создавшим информацию либо получившим на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Кроме отдельных граждан (физических лиц) обладателем информации может быть юридическое лицо Российской Федерации, субъект Российской Федерации или муниципальное образование.

К основным угрозам безопасности защищаемой информации относятся: несанкционированное распространение сведений (утечка информации) и несанкционированное целенаправленное или непреднамеренное воздействие на информацию или ее носитель. Утечка информации может происходить в трех формах: разглашение, разведка и несанкционированный доступ к информации.

Под разведкой понимается целенаправленная деятельность по добыванию сведений в интересах информационного обеспечения военно-политического руководства иностранного государства либо конкурирующей организации. Разведку, ведущуюся в интересах конкурирующий организации, часто называют промышленным шпионажем.

Разведка может быть агентурной и технической.

Агентурная разведка ведется штатными (оперативными) сотрудниками (лицами, состоящими в штате спецслужбы иностранного государства или конкурирующей организации) с привлечением агентов (лиц, конфиденциально сотрудничающих со спецслужбой иностранного государства или конкурирующей организацией).

Техническая разведка ведется с использованием специальных технических систем, средств и аппаратуры разведки.

Доступ к защищаемой информации с применением технических средств разведки часто называют техническим каналом утечки информации, под которым понимают совокупность объекта разведки, на котором обрабатывается защищаемая информация, среды распространения информационных сигналов и технического средства разведки (ТСР), с помощью которого регистрируются, измеряются и анализируются перехватываемые сигналы.

Защищаемая информация может быть представлена в различных формах, основными из которых являются: - документированная информация; - телекоммуникационная информация; - акустическая (речевая) информация и т. п.

К документированной информации относится зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

К телекоммуникационной информации относится информация, обрабатываемая техническими средствами или передаваемая по линиям (каналам) связи. Причем под обобщенным термином «обработка информации» понимают совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения информации.

Под акустической информацией обычно понимается информация, носителями которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой.

Частоты акустических колебаний в пределах 20−20 000 Гц называют звуковыми (их может воспринимать человеческое ухо), ниже 20 Гц − инфразвуковыми, а выше 20 000 Гц − ультразвуковыми.

Первичными источниками акустических сигналов являются механические колебательные системы, например, органы речи человека, а вторичными − преобразователи различного типа, например, громкоговорители.

Акустические сигналы представляют собой продольные механические волны. Они испускаются источником − колеблющимся телом − и распространяются в газах, жидкостях и твердых телах, в виде акустических колебаний (волн), т. е. колебательных движений частиц среды под действием различных возмущений.

В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. Тональный – это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает целый спектр гармонических составляющих.

Речевой сигнал является сложным акустическим сигналом. Речь может быть охарактеризована тремя группами характеристик: • семантическая или смысловая сторона речи − характеризует смысл тех понятий, которые передаются при ее помощи; • фонетические характеристики речи − данные, характеризующие речь с точки зрения ее звукового состава. Основной фонетической характеристикой звукового состава является частота встречаемости в речи различных звуков и их сочетаний; • физические характеристики − величины и зависимости, характеризующие речь как акустический сигнал. Помимо того, что звуки речи, объединяясь в определенные фонетические комбинации, образуют некоторые смысловые элементы, они также различаются и чисто физическими параметрами: мощностью, звуковым давлением, частотным спектром, длительностью звучания. В образовании звуков речи принимают участие легкие, гортань с голосовыми связками, область носоглотки, язык, зубы и губы. В процессе произношения речи легкие через бронхи продувают воздух в гортань и далее и через вибрирующие голосовые связки − в полость рта. Голосовые связки, то сжимая, то открывая голосовую

щель, пропускают воздух импульсами, частота которых лежит в пределах от 80 до 180 Гц у мужчин и от 160 до 300 Гц − у женщин.

Согласно проведенным исследованиям, частота основного тона изменяется в пределах от 60−70 Гц (для низких мужских голосов) до 450−500 Гц (для высоких женских голосов). Средняя частота основного тона составляет для мужских голосов 130−150 Гц и 250 Гц − для женских. Частотный спектр образованных голосовой щелью звуков речи содержит большое число гармонических составляющих, амплитуды которых уменьшаются с ростом частоты. Высота основного тона (первой гармоники) этого ряда характеризует собой тип голоса говорящего: бас, баритон, тенор, альт, контральто, сопрано. Однако это в большинстве случаев почти не играет роли для различения друг от друга звуков речи. Далее воздушная струя встречает на своем пути систему резонаторов, которые образуются воздушными объемами полости рта и носоглотки и видоизменяются в процессе произнесения различных звуков положением языка и зубов. Проходя через эту систему резонаторов, одни гармонические составляющие получают усиление, а другие, наоборот, подавляются. Эти усиленные области частот называются формантными областями или просто формантами, а подавленные – антиформантами. Поскольку форманты значительно мощнее других составляющих, то они-то главным образом и воздействуют на ухо слушающего, формируя звучание того или иного звука. Некоторое влияние на этот процесс оказывают и антиформанты. Изменяя положение языка, зубов и губ человек имеет возможность изменять характер звучания и произносить различные гласные звуки. Согласные звуки в большинстве случаев произносятся без участия голосовых связок. В русском языке различают сорок один звук речи (фонем).

По спектральному составу звуки речи различаются друг от друга числом формант и их расположением в частотном спектре. Следовательно, разборчивость речи зависит прежде всего от того, какая часть формант дошла до уха слушающего без искажений, и какая − исказилась.

Таким образом, речевой сигнал как процесс, развивающийся во времени и по частоте, можно рассматривать как взаимное наложение друг на друга его гармонической и формантной структуры. Смысловое содержание речевого сообщения определяется динамикой перестройки формантной структуры или огибающей спектра.

Процесс речеобразования, связанный с динамикой этой огибающей, часто называемой фонетической функцией Пирогова, удобно исследовать посредством цифрового спектрально-временного анализа спектрограмм.

Пространство, в котором происходит распространение акустических колебаний, называют акустическим полем, направление распространения акустических колебаний − акустическим лучом, а поверхность, соединяющую все смежные точки поля с одинаковой фазой колебания частиц среды, − фронтом

волны. В акустических измерениях в качестве измеряемой величины наиболее часто используется звуковое давление L. Звуковое давление – это избыточное давление, возникающее в упругой среде при прохождении через нее звуковой волны. Если в качестве упругой среды рассматривать воздушную среду, то звуковое давление – это среднеквадратичное отклонение давления относительно атмосферного давления.

Обычно при проведении измерений время интегрирования Т составляет 30–60 с и более. Различным видам речи соответствуют типовые интегральные уровни речевых сигналов, измеренные на расстоянии 1 м от источника речи (говорящий человек, звуковоспроизводящее устройство): L = 64 дБ – тихая речь; L = 70 дБ – речь средней громкости; L = 76 дБ – громкая речь; L = 84 дБ – очень громкая речь, усиленная техническими средствами.

Для обсуждения информации ограниченного доступа (совещаний, обсуждений, конференций, переговоров и т. п.) используются специальные помещения (служебные кабинеты, актовые залы, конференц-залы и т. д.), которые называются защищаемыми помещениями (ЗП).

Перехват речевой информации из ЗП возможен по прямому акустическому, акустовибрационному, акустооптическому, акустоэлектрическому и акустоэлектромагнитному каналам с применением различных технических средств акустической разведки, к которым относятся направленные микрофоны, лазерные акустические средства разведки, акселерометры и другие средства разведки.

Техническая акустическая разведка базируется на временном, спектральном и спектрально-временном анализе перехватываемых сигналов. Технология разведки при этом сводится к следующему: - перехват (регистрация) сигнала; - предварительная обработка (сортировка и т. д.) перехваченных сигналов; - восстановление информации, содержащейся в перехваченных сигналах, записанных в условиях высокого уровня шумов; - собственно анализ перехваченной речевой информации.

Особенностью акустической разведки является то, что анализ перехваченной с помощью технических средств разведки информации производит человек. Поэтому в качестве нормативного показателя оценки эффективности защиты ЗП от утечки речевой информации по техническим каналам используется словесная разборчивость речи W, под которой понимается относительное количество (в процентах) правильно понятых человеком слов, перехваченных (зарегистрированных) средством разведки.

Словесная разборчивость речи отражает качественную область понятности, которая выражена в категориях подробности составляемой справки о перехваченном с помощью технических средств разведки разговоре. Критерии эффективности защиты речевой информации во многом зависят от целей, преследуемых при организации защиты, например: скрыть смысловое

содержание ведущегося разговора, скрыть тематику ведущегося разговора или скрыть сам факт ведения переговоров. Из практических соображений может быть установлена некоторая шкала оценок качества перехваченного речевого сообщения:

1. Перехваченное речевое сообщение содержит количество правильно понятых слов, достаточное для составления подробной справки о содержании перехваченного разговора.

2. Перехваченное речевое сообщение содержит количество правильно понятых слов, достаточное только для составления краткой справки-аннотации, отражающей предмет, проблему, цель и общий смысл перехваченного разговора.

3. Перехваченное речевое сообщение содержит отдельные правильно понятые слова, позволяющие установить предмет разговора.

4. При прослушивании фонограммы перехваченного речевого сообщения возможно установить факт наличия речи, но нельзя установить предмет разговора.

5. При прослушивании фонограммы перехваченного речевого сообщения невозможно установить факт наличия речи.

Практический опыт показывает, что составление подробной справки о содержании перехваченного разговора невозможно при словесной разборчивости менее 70–80 %, а краткой справки-аннотации – при словесной разборчивости менее 40–60 %. При словесной разборчивости менее 20–40 % значительно затруднено установление даже предмета ведущегося разговора, а при словесной разборчивости менее 10–20 % − это практически невозможно. При словесной разборчивости менее 10 % значительно затруднено определение в перехваченном сообщении признаков речи.

При защите речевой информации необходимо исходить из возможностей использования злоумышленником для перехвата речевой информации технических средств акустической разведки, а также возможности прослушивания разговоров, ведущихся в них, посторонними лицами (посетителями, техническим персоналом) при их нахождении в коридорах и смежных с защищаемым помещением без применения технических средств разведки (непреднамеренное прослушивание).

Таким образом, при использовании изложенного выше методического подхода для оценки эффективности защиты речевой информации необходимо оценить звуковые давления скрываемого речевого сигнала и шума в местах возможного размещения датчиков аппаратуры акустической разведки или в месте возможного прослушивания речи без применения технических средств и затем рассчитать значение словесной разборчивости речи W.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект

соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

К нормативно-техническим документам относятся Нормы противодействия акустической речевой разведке (предельные возможности инженерно-технической разведки по добыванию информации), Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от ее утечки по техническим каналам (СТР), а также нормы и требования по защите информации от утечки по каналу ПЭМИН.

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. Состав видов технической разведки и их возможности, угрозы безопасности информации и каналы ее утечки, подлежащие контролю, определяются ФСТЭК России в соответствующих моделях технических разведок и концепциях защиты.

Технический контроль осуществляется в соответствии с методиками контроля состояния технической защиты информации, утвержденными или согласованными с ФСТЭК России. Не допускается физическое подключение технических средств контроля, а также формирование тестовых режимов, запуск тестовых программ на образцах, средствах и информационных системах в процессе выполнениями обработки информации или технологического процесса. При оценке защиты информации различного уровня конфиденциальности, циркулирующей на объектах информатизации (ОИ) той или иной организации, всегда акцентируется внимание на типе защищаемой информации (речевая, документальная или цифровая) и физическом расположении центров ее циркуляции (выделенные помещения или автоматизированные системы). После оценки оптимальности расположения ОИ решаются следующие вопросы: по каким каналам информация может покидать пределы ОИ, как и в каких объемах необходимо защищать эти каналы от утечки и соответствует ли защита предъявляемым или разрабатываемым самостоятельно критериям безопасности – соответственно разведдоступность, защищенность и аттестация.

Оценка разведдоступности включает в себя проверку возможности утечек информации по техническим каналам, проверку системы разграничения доступа физических лиц к конфиденциальной информации согласно их допуску и проверки режимности работы сотрудников (соответствия доступа к информации его допуску).

Аттестация объекта информатизации является заключительным этапом работ по защите информации, в который входит оценка требований, предъявляемых для исследуемых объектов информатизации организации заказчика, и соответствие этим требованиям аттестуемых объектов. Результатом

данной работы является аттестат соответствия, дающий право аттестующийся организации работать на своих ОИ с конфиденциальной информацией или как минимум уверенность в ее защищенности. Аттестат выделенного помещения – документ, выдаваемый органом по аттестации (сертификации) или другим специально уполномоченным органом, подтверждающий наличие необходимых условий, обеспечивающих надежную акустическую защищенность выделенного помещения в соответствии с установленными нормами и правилами.

Литература:

[3, 4], [10] глава 1, [11] глава 3, 4, [21].

Контрольные вопросы:

1. Что понимают под аттестацией объектов информатизации?
2. Какие документы являются нормативно-техническими при проведении аттестации объектов?
3. Какие полномочия предоставляет действующий «Аттестат соответствия»?
4. Какие объекты подлежат обязательной аттестации?
5. Какие оценки включает в себя разведдоступность объекта информатизации?
6. Из какого комплекса работ состоит проверка возможности утечки информации по техническим каналам?
7. Что представляют собой специальные проверки объекта защиты?
8. Комплекс каких мероприятий входит в специальные обследования объекта защиты?
9. Для чего производится легендирование специальных обследований выделенных помещений?
10. Из каких действий состоят поисковые мероприятия на объекте?
11. С какой целью проводятся специальные исследования?
12. Что является конечным результатом специальных исследований?
13. Какие объекты являются исследуемыми при проведении специальных исследований в области акустики?
14. На чем базируется действующая методика измерений акустических и виброакустических характеристик различных сред?

4. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Текущий контроль успеваемости

Оценивание поэтапного формирования результатов освоения дисциплины осуществляется в процессе текущего контроля, который представляет собой единый непрерывный процесс оценки знаний, умений, формирования и сформированности компетенций у обучающихся.

Текущий контроль предназначен для проверки хода и качества усвоения обучающимися учебного материала и стимулирования учебной работы студентов. Он может осуществляться в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной рабочей программой дисциплины. Текущий контроль предполагает постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим обучающимся для самоконтроля на разных этапах обучения. Результаты контроля учитываются выставлением оценок в журнале учета успеваемости.

Для текущего контроля успеваемости используются следующие оценочные средства:

- контрольные вопросы для устного опроса по темам дисциплины;
- задания и контрольные вопросы по лабораторным работам;
- задания по подготовке докладов;
- тестовые задания.

Типовые контрольные вопросы для устного опроса по темам дисциплины приведены в п. 3 настоящего пособия.

Положительная оценка («зачтено») по результатам каждого контроля (опроса) выставляется в соответствии с универсальной системой оценивания, приведенной в табл. 3. В случае получения оценки «не зачтено» студент должен пройти повторный контроль по данной теме в ходе последующих консультаций.

Текущий контроль в виде защиты лабораторных работ проводится на лабораторном практикуме, целью которого является формирование умений и практических навыков по использованию специальных технических приборов по выявлению и локализации технических каналов утечки информации. Оценка результатов выполнения задания по каждой лабораторной работе производится при представлении студентом отчета по лабораторной работе и на основании ответов студента на вопросы по тематике лабораторной работы. Студент, самостоятельно выполнивший задание, продемонстрировавший знание

использованных им технических средств, получает по лабораторной работе оценку «зачтено».

Таблица 3 – Система оценок и критерии выставления оценки при прохождении контроля (опроса)

Критерий	Система оценок			
	«незачтено»	**«зачтено»**		
Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно корректно связывать между собой (только некоторые из них может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект

Критерии оценивания отчета по лабораторным работам

а) разделы отчета

- наименование лабораторной работы;
- постановка задачи, исходные данные;
- описание методов и способов решения;
- этапы решения задачи и (или) ее алгоритмическое обеспечение;
- результаты, представленные в виде таблиц, графиков и т. п. с краткими пояснениями;
- выводы.

б) критерии оценивания

Студент должен продемонстрировать:

- умения применять математические методы для формализации и решения прикладных задач; строить модели экономических процессов, исследовать их и вырабатывать рекомендации к их применению на практике; организовывать вычислительный эксперимент на компьютере для исследования поведения систем, процессов;
- владение навыками работы с пакетами прикладных программ для моделирования и анализа экономических процессов.

в) описание шкалы оценивания

- **«Зачтено»** выставляется в случае, если студент выполнил в полном объеме лабораторную работу, не допустил ошибок в расчетах, сделал выводы, свободно излагает этапы решения и результаты работы.

- **«Незачтено»** выставляется в случае, если студент не выполнил лабораторную работу, либо выполнил, но допустил существенные ошибки в расчетах и (или) не сделал выводы, и (или) не может изложить этапы решения и результаты работы.

Примерная тематика докладов

1. Основные параметры системы защиты информации.
2. Понятия безопасности и системы безопасности информации. Фрагментарный и системный подход к защите информации.
3. Физические процессы подавления опасных сигналов.
4. Физические основы побочных электромагнитных излучений и наводок.
5. Модель построения системы информационной безопасности предприятия
6. Основы защиты информации от фотографической и оптико-электронной разведок.
7. Основы защиты информации от радиотехнической разведки.
8. Процессы подавления опасных сигналов.
9. Основные определения и классификация радиоэлектронных помех.
10. Методы и средства инженерной защиты и технической охраны объектов.
11. Классификация и характеристика охранных, пожарно-охранных и пожарных извещателей.
12. Технические средства несанкционированного доступа к информации.
13. Направления обеспечения безопасности.
14. Аттестация объектов, лицензирование деятельности по защите информации и сертификации ее средств.
15. Особенности инструментального контроля эффективности инженерно-технической защиты информации.
16. Классификация средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.
17. Технические средства для тестирования и контроля систем обеспечения безопасности информации.
18. Принципы моделирования объектов защиты.
19. Экранирование технических средств и помещений.
20. Детекторы видеокамер.
21. Защита информации от утечки за счет паразитной генерации, по цепям питания и по цепям заземления.
22. Защита информации от утечки за счет взаимного влияния проводов и линий связи и высокочастотного навязывания.

23. Защита линий связи. Защита информации от утечки в волоконно-оптических линиях связи.

Критерии оценивания за устное выступление при обсуждении вопроса

«Отлично»	Выступление (доклад) отличается последовательностью, логикой изложения. Легко воспринимается аудиторией. При ответе на вопросы выступающий (докладчик) демонстрирует глубину владения представленным материалом. Ответы формулируются аргументировано, обосновывается собственная позиция в проблемных ситуациях.
«Хорошо»	Выступление (доклад) отличается последовательностью, логикой изложения. Но обоснование сделанных выводов не достаточно аргументировано. Неполно раскрыто содержание проблемы.
Удовлетворительно»	Выставляется, если выступающий (докладчик) передает содержание проблемы, но не демонстрирует умение выделять главное, существенное. Выступление воспринимается аудиторией сложно.
«Неудовлетворительно»	Выступление (доклад) краткий, неглубокий, поверхностный.

Критерии оценивания доклада с презентацией

«Неудовлетворительно»	Студент демонстрирует первичное восприятие некоторых основных элементов медиаработы. Она проста и незакончена. Проблема не раскрыта. Отсутствуют выводы. Не использованы возможности визуализации материала в PowerPoint. Больше четырех ошибок в представляемой информации.
«Удовлетворительно»	Некоторая степень владения большинством элементов медиаработы. Частично присутствует гармоничная интеграция элементов в целое, но работа незавершенная. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не

	обоснованы. Частично использованы возможности визуализации материала в PowerPoint. Три-четыре ошибки в представляемой информации.
«Хорошо»	Студент показывает владение элементами медиаработы. В основном она ясная и целостная. Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы. Использованы информационные технологии (PowerPoint). Не более двух ошибок в представляемой информации.
«Отлично»	Студент продемонстрировал уверенное владение и интеграцию всех элементов медиаработы. Работа целостна, креативна. Использован творческий подход. Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы. Широко использованы информационные технологии (PowerPoint). Отсутствуют ошибки в представляемой информации.

Примерный перечень тестовых вопросов для самостоятельной работы

1.	Каким свойством не обладает информация в форме сообщения? а) материальность б) измеримость г) простота д) проблемная ориентированность
2.	Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия, является угрозой: а) конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности б) информационному обеспечению государственной политики РФ г) развитию отечественной индустрии информации, включая индустрию телекоммуникации, связи и средств информатизации д) безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России
3.	Информационным ресурсом является:

	а) вся накопленная информация, в том числе и недостоверная, представленная сомнительными фактами, ложными положениями, потерявшая конкретность б) только достоверная информация из проверенных источников г) вся накопленная информация, в том числе и недостоверная, представленная сомнительными фактами, ложными положениями, но не потерявшая своей конкретности д) достоверная информация из проверенных источников, включая устаревшую информацию
4.	Утечка информации – это … а) несанкционированный процесс переноса информации от источника к злоумышленнику б) процесс раскрытия секретной информации в) процесс уничтожения информации г) непреднамеренная утрата носителя информации
5.	Информация, поступающая к человеку, обладает следующими свойствами: а) идеальность, объективность, динамичность б) идеальность, объективность, простота г) динамичность, субъективность, накапливаемость д) субъективность, неидеальность, информационная неуничтожаемость
6.	Преднамеренной угрозой безопасности информации является: а) наводнение б) повреждение кабеля, по которому идет передача, в связи с погодными условиями в) кража г) ошибка разработчика
7.	Концепция системы защиты от информационного оружия не должна включать… а) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры б) средства нанесения контратаки с помощью информационного оружия в) признаки, сигнализирующие о возможном нападении г) процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

8.	В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на … а) соблюдение норм международного права в сфере информационной безопасности б) выявление нарушителей и привлечение их к ответственности в) разработку методов и усовершенствование средств информационной безопасности г) соблюдение конфиденциальности информации ограниченного доступа
9.	Информация, составляющая государственную тайну, не может иметь гриф… а) «для служебного пользования» б) «секретно» в) «совершенно секретно» г) «особой важности»
10.	Одной из основных угроз доступности информации является: а) злонамеренное изменение данных б) хакерская атака в) непреднамеренные ошибки пользователей г) перехват данных
11.	Что не относится к компьютерной преступности? а) подделка компьютерной информации б) хищение информации в) распространение вирусов г) согласованное копирование данных
12.	Как называется комплекс мероприятий, направленных на обеспечение информационной безопасности? а) защитой информации б) авторизацией в) информационной безопасностью г) безопасным состоянием
13.	Кто отвечает за защиту автоматизированной системы от несанкционированного доступа к информации? а) пользователь б) аутентификатор в) авторизатор г) администратор защиты

14.	Перехват данных является угрозой… а) доступности б) целостности в) конфиденциальности г) для администратора
15.	Сбор и накопление информации о событиях, происходящих в информационной системе, называется… а) протоколированием б) аудитом в) экранированием г) криптографией
16.	Что не относится к основополагающим документам в области информационной безопасности? а) концепция о криптостойкости систем б) Оранжевая книга в) Рекомендации Х.800 г) концепция защиты от несанкционированного доступа Гостехкомиссии при Президенте РФ
17.	Как называется набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию? а) эффективность защиты б) политика безопасности в) гарантированность г) гармонизированность безопасности
18.	Что не входит в аспекты информационной безопасности? а) доступность б) целостность в) стойкость г) конфиденциальность
19.	Сложность обеспечения информационной безопасности является следствием: а) злого умысла разработчиков информационных систем б) объективных проблем современной технологии программирования в) происков западных спецслужб, встраивающих «закладки» в аппаратуру и программы г) постоянные атаки хакеров

20.	В число принципов управления персоналом входит: а) разделяй и властвуй б) разделение обязанностей в) метод кнута и пряника г) разделение доступа
21.	Меры информационной безопасности направлены на защиту от: а) нанесения неприемлемого ущерба б) нанесения любого ущерба в) подглядывания в замочную скважину г) нанесения морального вреда
22.	На межсетевые экраны целесообразно возложить следующие функции: а) антивирусный контроль «на лету» б) антивирусный контроль компьютеров внутренней сети в) антивирусный контроль компьютеров внешней сети г) антивирусный контроль всех съемных носителей
23.	На современном этапе развития законодательного уровня информационной безопасности в России важнейшее значение имеют: а) меры ограниченной направленности б) меры направляющие и координирующие в) меры по обеспечению информационной независимости г) меры по поддержанию государственной безопасности
24.	Системы анализа защищенности помогают: а) оперативно пресечь известные атаки б) предотвратить известные атаки в) восстановить ход известных атак г) восстановить логические связи
25.	Сложность обеспечения информационной безопасности является следствием: а) невнимания широкой общественности к данной проблематике б) все большей зависимости общества от информационных систем в) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним г) обширной структуры предмета информационная безопасность
26.	Уровень безопасности С, согласно «Оранжевой книге», характеризуется: а) произвольным управлением доступом б) принудительным управлением доступом в) верифицируемой безопасностью г) комплексным управлением доступом

27.	Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что: а) с программно-технической точки зрения, информационная безопасность – ветвь информационных технологий и должна развиваться по тем же законам б) объектно-ориентированный подход популярен в академических кругах в) объектно-ориентированный подход поддержан обширным инструментарием г) объектно-ориентированный подход широко применяется в государственных структурах
28.	В число принципов физической защиты входят: а) беспощадный отпор б) непрерывность защиты в пространстве и времени в) минимизация защитных средств г) наличие охранника
29.	Что из перечисленного не относится к числу основных аспектов информационной безопасности: а) доступность б) конфиденциальность в) целостность г) масштабируемость
30.	Совместно с криптографическими сервисами туннелирование может применяться для достижения следующих целей: а) обеспечение гарантированной полосы пропускания б) обеспечение высокой доступности сетевых сервисов в) обеспечение конфиденциальности и целостности передаваемых данных г) обеспечение максимального уровня защищенности хранимых данных

Критерии оценивания выполнения тестирования

а) типовые задания к тесту

Формы тестовых заданий:

- выбор правильных ответов из перечисленных;
- установление правильной последовательности;
- установление соответствия.

б) критерии оценивания

Критерием оценивания теста является количество правильно выполненных тестовых заданий, свидетельствующих о полноте знаний теоретического материала в области технической защиты информации.

в) описание шкалы оценивания

5 «Отлично» – количество правильно выполненных заданий составляет от 80 до 100 %.

4 «Хорошо» – количество правильно выполненных заданий составляет от 60 до 79 %.

3 «Удовлетворительно» – количество правильно выполненных заданий составляет от 50 до 59 %.

2 «Неудовлетворительно» – количество правильно выполненных заданий составляет менее 50 %.

Промежуточная аттестация по дисциплине

Под промежуточной аттестацией понимается аттестация студентов по дисциплине, изученной в течение семестра. Аттестация – определение и оценка уровня знаний студента за определенный период обучения, а также отзыв о его способностях, деловых и иных качествах.

Таким образом, кроме оценки уровня знаний процедура аттестации предполагает на основе анализа текущей успеваемости и отношения к учебной работе оценку ряда личных качеств студента. Промежуточная аттестация предусматривает проведение зачетов и экзаменов, включенных в учебный план специальности, является обязательной формой аттестации и предназначена для проверки успеваемости студентов по дисциплине.

Аттестация также призвана обеспечить постоянную, систематическую и добросовестную работу над освоением учебных программ путем соблюдения установленных планов, графиков и расписаний; своевременное и с высоким качеством преодоление установленных порогов требовательности при текущем контроле знаний. Промежуточная аттестация студентов по дисциплине осуществляется в рамках завершения изучения дисциплины и позволяет определить качество усвоения изученного материала. Промежуточная аттестация осуществляется в конце семестра в период семестровых экзаменационных сессий. Формы проведения промежуточной аттестации определяются рабочим учебным планом специальности, являются едиными и обязательными для всех форм обучения.

Промежуточная (заключительная) аттестация по дисциплине предусматривает проведение зачета и экзамена (экзаменационного тестирования). Зачеты и экзамены проводятся по расписанию, согласно графику учебного процесса.

Изучение дисциплины в седьмом семестре завершается **зачетом** (в соответствии с учебным планом образовательной программы).

Цель – оценка качества усвоения учебного материала и сформированности компетенций в результате изучения дисциплины.

По итогам зачета выставляется «зачтено» или «не зачтено». Содержание представляет перечень примерных вопросов к зачету.

Зачет как форма промежуточного контроля и организации обучения служит приемом проверки степени усвоения учебного материала и лекционных занятий, качества усвоения обучающимися отдельных разделов учебной программы, сформированных умений и навыков.

Зачет проводится устно или письменно по решению преподавателя, в объеме учебной программы. Преподаватель вправе задать дополнительные вопросы, помогающие выяснить степень знаний обучающегося в пределах учебного материала, вынесенного на зачет.

По решению преподавателя зачет может быть выставлен без опроса – по результатам работы обучающегося на лекционных и (или) лабораторных занятиях.

В период подготовки к зачету обучающиеся вновь обращаются к пройденному учебному материалу. При этом они не только закрепляют полученные знания, но и получают новые.

Подготовка обучающегося к зачету включает в себя три этапа:

- самостоятельная работа в течение процесса обучения;

- непосредственная подготовка в дни, предшествующие зачету по темам курса.

Литература для подготовки к зачету рекомендуется преподавателем.

Зачет в письменной форме проводится по тестам, охватывающим весь пройденный по данной теме материал. По окончании ответа преподаватель может задать обучающемуся дополнительные и уточняющие вопросы.

Результаты зачета объявляются обучающемуся после проверки ответов.

Примерный перечень вопросов к самостоятельной проверке своих знаний по дисциплине:

1. Дайте определение информации, документированной информации. Каково отличие государственной тайны, конфиденциальной информации и открытой информации.

2. Классификация технической разведки. Эффективность добывания информации технической разведкой.

3. Государственная система защиты информации. Эффективность защиты информации.

4. Основные объекты защиты информации.

5. Дайте определение демаскирующих признаков. Для чего они используются. Приведите примеры.

6. Дайте определение терминам «Контролируемая зона», «Опасная зона», «Опасная зона 1», «Опасная зона 2».

7. Состав технического канала утечки информации.

8. Классификация технических каналов утечки информации.

9. Перечислите технические каналы утечки информации, обрабатываемой ОТСС. Приведите примеры.

10. Перечислите технические каналы утечки информации при передаче по каналам связи. Приведите примеры.

11. Перечислите каналы утечки речевой информации. Приведите примеры.

12. Перечислите каналы утечки видовой информации. Приведите примеры.

13. Каково влияние паразитных емкостных, индуктивных и резистивных связей в каналах связи.

14. Перечислите методы противодействия утечке информации по техническим каналам.

15. Способы скрытого видеонаблюдения. Характеристики оборудования для скрытого видеонаблюдения.

16. Способы скрытого прослушивания переговоров в помещении. Демаскирующие признаки радиозакладок. Демаскирующие признаки проводных закладок.

17. Способы прослушивания переговоров по телефонным линиям. Демаскирующие признаки акустических закладок типа «телефонное ухо».

18. Направленные микрофоны. Принцип действия.

19. Охранные системы. Назначение. Структура. Приведите примеры охранных систем объектов и помещений.

20. Датчики охранных систем. Принципы действия датчиков.

21. Охранное видеонаблюдение. Назначение. Структура. Основные характеристики.

22. Средства радиотехнической разведки. Состав. Характеристики.

23. Охрана объектов. Особенности охраны объектов различного класса. Задачи средств охраны объектов.

24. Периметровые средства охраны. Датчики периметровых систем охраны.

25. Охрана выделенных (защищаемых) помещений. Технические средства охраны помещений.

26. Экранирование электромагнитных волн.

27. Экранирование акустических сигналов.

28. Фильтрация опасных сигналов. Приведите примеры.

29. Маскировка опасных сигналов зашумлением. Приведите примеры.

30. Металлодетекторы. Сферы применения. Принцип действия.

31. Локаторы нелинейностей. Сферы применения. Принцип действия.

32. Аттестация объектов информатизации по требованиям безопасности. Назначение. Порядок проведения аттестации.

33. Специальная проверка. Специальное обследование. Специальное исследование.

34. Проведение измерений акустических и виброакустических характеристик. Приведите примеры.

35. Проведение измерений побочных электромагнитных излучений. Приведите примеры.

Ответ студента на зачете оценивается одной из следующих оценок: «зачтено» и «незачтено», которые выставляются по следующим критериям.

«Зачтено» – обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности.

Оценкой «зачтено» также оцениваются ответы студентов, показавших знание основного учебного материала в объеме, необходимом для дальнейшей учебы и в предстоящей работе по профессии, справляющихся с выполнением заданий, предусмотренных программой, но допустившим погрешности в ответе и при выполнении контрольных заданий, не носящие принципиального характера, когда установлено, что студент обладает необходимыми знаниями для последующего устранения указанных погрешностей под руководством преподавателя.

«Незачтено» выставляется студентам, обнаружившим пробелы в знаниях основного учебного материала, допускающим принципиальные ошибки в выполнении предусмотренных программой заданий. Такой оценки заслуживают ответы студентов, носящие несистематизированный, отрывочный, поверхностный характер, когда студент не понимает существа излагаемых им вопросов, что свидетельствует о том, что студент не может дальше продолжать обучение или приступать к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Изучение дисциплины в восьмом семестре завершается **экзаменом** (в соответствии с учебным планом образовательной программы).

К **экзамену** допускаются студенты:

- выполнившие и защитившие все предусмотренные лабораторные работы (получившие положительную оценку по результатам лабораторного практикума);

- выполнившие индивидуальные контрольные задания (получившие оценку «зачтено» по каждому индивидуальному заданию) – для студентов очной формы;

- выполнившие контрольную работу (получившие оценку «зачтено» по контрольной работе) – для студентов заочной формы.

Экзамен может проводится как в традиционной форме, так и в виде экзаменационного тестирования.

Экзаменационный билет содержит два экзаменационных вопроса.

Примерный перечень экзаменационных вопросов по дисциплине:

1. Классификация каналов связи.
2. Классификация электромагнитных излучений по диапазонам частот и длинам волн согласно номенклатуре международного Регламента радиосвязи.
3. Характеристика проводных электрических линий связи.
4. Параметры линий связи.
5. Помехи (наводки), возникающие в каналах связи.
6. Характеристика электромагнитных каналов утечки информации.
7. Характеристика спектральных составляющих ПЭМИН персонального компьютера.
8. Характеристика электрических каналов утечки информации.
9. Средства и способы съема информации по электрическим каналам информации.
10. Классификация демаскирующих признаков объектов.
11. Характеристика демаскирующих признаков объектов в видимом диапазоне электромагнитного спектра.
12. Характеристика демаскирующих признаков объектов в инфракрасном диапазоне электромагнитного спектра.
13. Основные характеристики радиосигналов демаскирующих признаков радиоэлектронных средств.
14. Классификация технических признаков радиоизлучений.
15. Классификация демаскирующих признаков акустических закладок.
16. Основные характеристики микрофонов.
17. Назначение, состав и принцип работы параболического микрофона.
18. Назначение, состав и принцип работы плоских фазированных решеток.
19. Назначение, состав и принцип работы трубчатого микрофона.
20. Назначение, состав и принцип работы градиентного микрофона.
24. Основные характеристики направленных микрофонов.
25. Назначение, решаемые задачи и составные части радиомикрофонов.
23. Основные тактико-технические характеристики сканирующих радиоприемников.

24. Назначение, решаемые задачи, ТТХ и принцип работы портативного измерителя частоты MFP-8000.

25. Основные способы контроля и прослушивания телефонных каналов связи.

26. Принцип реализации способа прослушивания помещений через микрофон телефонного аппарата (схема прослушивания способом высокочастотного навязывания).

27. Основные задачи охраны и принципы обеспечения безопасности объектов.

28. Сформулировать основные особенности построения периметровой системы охраны особо важных объектов.

29. Реализация периметровой охраны особо важных объектов путем создания функциональных зон.

30. Оптимизация построения системы охранной безопасности.

31. Организация контроля доступа к защищаемым помещениям.

32. Характеристика активных лучевых инфракрасных систем охраны.

33. Характеристика пассивных инфракрасных систем охраны.

34. Назначение и составные части оптоволоконных систем охраны.

35. Особенности реализации охраны периметров с помощью емкостных систем.

36. Назначение, принцип действия вибрационных систем с сенсорными кабелями.

37. Назначение, составные части и принцип работы вибрационно-сейсмических систем.

38. Назначение, устройство и принцип действия радиолучевых систем охраны объектов.

39. Назначение, принцип действия специальных систем наблюдения за территорией охраняемого объекта.

40. Особенности реализации защиты электронных устройств с помощью экранирования электромагнитных волн.

41. Классификация помехоподавляющих фильтров, их амплитудно-частотные характеристики.

42. Методика расчета параметров LC-фильтров.

43. Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании.

44. Назначение, характеристики и принцип работы нелинейного локатора.

45. Раскрыть особенности функционирования технических средств радиомониторинга и обнаружения закладных устройств.

46. Раскрыть содержание методики защиты от утечки за счет микрофонного эффекта.

47. Раскрыть содержание организационных мер защиты информации от утечки за счет электромагнитного излучения.

48. Раскрыть содержание методики защиты от утечки в волоконно-оптических линиях и системах связи.
49. Раскрыть содержание основных способов несанкционированного доступа к источникам конфиденциальной информации.
50. Раскрыть содержание основных способов коммуникации сигналов от закладных микрофонов.
51. Раскрыть содержание основных способов противодействия подслушиванию телефонных переговоров.
52. Организация выявления возможных точек расположения лазерного регистратора.
53. Организация технической защиты от лазерного подслушивания.
54. Раскрыть содержание способа несанкционированного получения информации за счет приема электромагнитных сигналов радиодиапазона на примере частной модели радиоперехвата.
55. Методика определения вероятности установления информационного контакта.
56. Классифицировать основные методы защиты от радиоперехвата.

Критерии оценивания экзамена

Критерии оценок на экзамене по дисциплине (отлично, хорошо, удовлетворительно, неудовлетворительно):

- **«ОТЛИЧНО»** выставляется в случае правильных, полных и четких ответов на теоретические вопросы, с их проецированием и интерпретацией на сегодняшнюю ситуацию. Допускаются непринципиальные погрешности или небольшая незавершенность ответов, диктуемых лимитом времени.

- **«ХОРОШО»** выставляется в случаях: правильных и четких ответов при незначительных замечаниях, неточностях.

- **«УДОВЛЕТВОРИТЕЛЬНО»** выставляется в случаях ответа на большую часть (не менее 50% основных положений); при правильном ответе на один вопрос или неполных ответах на два вопроса.

- **«НЕУДОВЛЕТВОРИТЕЛЬНО»** выставляется при ответах, не удовлетворяющих критериям, указанным в предыдущих пунктах.

5. ЗАКЛЮЧЕНИЕ

На лекциях излагаются основные теоретические положения, составляющие дисциплину, и разбираются примеры практических задач. Преподавателю, ведущему курс, рекомендуется на вводной лекции определить структуру курса, пояснить цели и задачи изучения дисциплины, сформулировать основные вопросы и требования к результатам освоения.

При рассмотрении темы важно выделить основные понятия и определения, желательна их визуализация. При подготовке и проведении занятий по данному курсу преподаватель должен руководствоваться как общими учебно-методическими принципами (научность, системность, доступность, последовательность, преемственность, наличие единой внутренней логики курса, его связь с другими предметами), так и специфическими особенностями дисциплины. В подборе материала к занятиям следует руководствоваться рабочей программой учебной дисциплины, обращая внимание на компетенции, указанные в федеральном государственном образовательном стандарте высшего образования.

На первом занятии преподаватель обязан довести до обучающихся порядок работы в аудитории и нацелить их на проведение самостоятельной работы с учетом количества часов, отведенных на нее учебным планом. Рекомендуя литературу для самостоятельного изучения, преподаватель должен максимально использовать возможности, предлагаемые библиотекой академии, в том числе ее электронными ресурсами.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления или процессов, научные выводы и практические рекомендации.

В конце лекции необходимо делать выводы и ставить задачи на самостоятельную работу. Лабораторные занятия направлены на закрепление лекционного материала.

Самостоятельная работа студентов заключается в подготовке к лабораторным и лекционным занятиям и выполнении заданий, выдаваемых преподавателем по каждому из разделов дисциплины. В целях лучшего понимания сути представления и обработки информации при защите рекомендуется использовать гипотетическую модель информации, что позволит использовать архитектурные особенности, свойственные конкретным моделям анализа. Примеры следует выбирать так, чтобы вычисления были не слишком громоздкими. Следует рассматривать задачи, возникающие в самых различных отраслях, и показать динамику решения задач: как подойти к решению конкретной проблемы, какие ограничения возникают в рамках данного решения и какие результаты получаются в конечном счете.

В самостоятельную работу входит выполнение индивидуальных заданий. Преподаватель принимает решение о допуске студента к лабораторной работе по результатам собеседования. Студенты знакомятся с общими сведениями, порядком выполнения работы, пишут необходимые пояснения в соответствии с

полученным вариантом задания. При защите работы студент отвечает преподавателю на контрольные вопросы, представляет теоретическую часть решения задачи, практический расчет.

6. ЛИТЕРАТУРА

1. Конституция РФ. – URL: http://constitutionrf.ru/.
2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646. – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.
3. ГОСТ РВ 50170-92. Противодействие ИТР. Термины и определения. – М.: Госстандарт России.
4. ГОСТ Р 50992-96. Защита информации. Термины и определения. М.: Госстандарт России.
5. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Гостехкомиссией России 25.11.1994). – М.: Гостехкомиссия РФ, 1994. – 11 с.
6. Кузнецов, А. В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В. А. Иванов, О. П. Пономарев, И. А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.
7. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В., 3-е изд. – М.: ИЦ РИОР, НИЦ ИНФРА. – М, 2016. – 322 с. – Режим доступа: http://znanium.com.
8. Зайцев, А. П. Техническая защита информации: учебник для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : Горячая линия-Телеком, 2009. – 616 с.
9. Бузов, Г. А., Защита от утечки информации по техническим каналам: учеб. пособие / С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия-Телеком, 2005. – 256 с.
10. Хорев А. А. Защита информации от утечки по техническим каналам. Ч. I. Технические каналы утечки информации : Учебное пособие. – М. : Гостехкомиссия России, 1998. – 320 с.
11. Сапожников М. А. Акустика: справочник. – М. : Радио и связь, 1989. – 336 с.
12. Покровский Н. Б. Расчет и измерение разборчивости речи. – Москва : Госиздат по вопросам связи и радио, 1962. – 392 с.
13. Быков С. Ф., Журавлев В. И., Шалимов И. А. Цифровая телефония : учеб. пособие. – М. : Радио и связь, 2003. – 144 с.
14. Дураковский, А. П. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации: учеб. пособие / А. П.

Дураковский, И. В. Куницын, Ю. Н. Лаврухин. – М.: НИЯУ МИФИ, 2015. − 152 с.

15. Палий, А. М. Радиоэлектронная борьба. – М.: Воениздат, 1989. – 350 с.

16. Парамонов, И. Б. Способ защиты информации от утечки по цепи вторичного электропитания / И. Б. Парамонов, А. В. Мазин, А. А. Филимонов. // Вопросы радиоэлектроники. – 2017. – № 11. – С. 52–55.

17. Егошин, Н. С. Формирование модели нарушителя / Н. С. Егошин, А. А. Конев, А. А. Шелупанов // Безопасность информационных технологий. – 2017. – № 4. – С. 21–29.

18. Козлачков, С. Б. Некоторые особенности формирования акустоэлектрического канала утечки речевой акустической информации / С. Б. Козлачков [и др.]. // Безопасность информационных технологий. – 2017. – № 4. – С. 64–76.

19. Панычев, С. Н. Защита акустической информации методом интермодуляционного зашумления с помощью нелинейных случайных антенн / С. Н. Панычев [и др.] // Радиотехника. – 2017. – № 6. – С. 136–140.

Локальный электронный методический материал

Александр Георгиевич Жестовский

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Редактор М. А. Дмитриева

Уч.-изд. л. 3,6. Печ. л. 4,4.

Издательство федерального государственного бюджетного образовательного
учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1