Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Иванцов А.М.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения

Ульяновск, 2020

Методические указания для самостоятельной работы студентов по дисциплине «Техническая защита информации» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2020. Настоящие методические указания предназначены для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к лекциям, семинарам, лабораторным и курсовым работам и к экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 6/20 от 22.09.2020 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

основная

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html.

2. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204248.html

3. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html

4. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности / А.А. Торокин. М.: Гелиос АРВ, 2005, 960 с.

5. Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров - Правительства Российской Федерации от 15 сентября 1993 г. № 912-51

дополнительная

1. Сычев М.П., Лабораторный практикум по курсу "Акустика" [Электронный ресурс]: Учеб. пособие / М.П. Сычев, С.Б. Козлачков. - М.: Издательство МГТУ им. Н. Э. Баумана, 2011. - 76 с. - ISBN - Режим доступа: http://www.studentlibrary.ru/book/bauman_0568.html.

2. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201216.html.

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

3.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

3.3 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

3.4 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

учебно-методическая

1. Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» /А.С. Андреев, А.М. Иванцов, С.М. Рацеев. - Ульяновск: УлГУ, 2017. - 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

2. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", «Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", «Системный анализ и управление» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54 с.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 1. КОНЦЕПЦИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Основные вопросы:

1. Обобщённая структура государственной системы защиты информации. Основные документы по противодействию иностранным техническим разведкам
2. Концепция технической защиты информации
3. Основные положения системного подхода к технической защите информации
4. Модель системы защиты информации (СЗИ)

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [5].

Для самостоятельного изучения вопроса 2 следует обратиться к [5, 3.1-3.4].

Вопрос 2 изложен в учебном пособии [4] на с. 11-23.

Вопрос 3 изложен в учебном пособии [4] на с. 29-31.

Вопрос 4 изложен в учебном пособии [2] на с. 10-14.

Контрольные вопросы по теме 1:

1. Охарактеризовать основные элементы обобщённой структуры государственной системы защиты информации.
2. Перечислить основные документы по противодействию иностранным техническим разведкам.
3. Перечислить основные тезисы Положения о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам.
4. В чём заключается концепция технической защиты информации?
5. Назвать основные задачи технической защиты информации.
6. Назвать основные положения системного подхода к технической защите информации.
7. Описать сущность модели системы защиты информации.

Тесты для самостоятельной работы:

1. Какой документ, из перечисленных, не относится к сфере противодействия иностранным техническим разведкам?

а) Федеральный закон от 27 декабря 2002 г. № 184 - ФЗ «О техническом регулировании»

б) Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации»

в) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

г) Указ Президента Российской Федерации от 16 августа 2004 № 1085

«Вопросы Федеральной службы по техническому и экспортному контролю»

2. Какой подход предусматривает самый высокий уровень описания объекта исследования?
а) Структурный
б) Параметрический
в) Системный
г) Функциональный

3. Что такое системное мышление?
а) Форма мышления, характеризующая способность человека на бессознательном уровне решать задачи дедуктивным методом
б) Форма мышления, при котором человек ставит под сомнение любую информацию, и даже собственные убеждения
в) Форма мышления, при которой человек способен выделять в анализируемом объекте существенные детали, незаметные для поверхностного взгляда

2.2. РАЗДЕЛ 1. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 2. ФИЗИЧЕСКИЕ ОСНОВЫ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПОБОЧНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

Основные вопросы:
1. Опасные сигналы и их источники
2. Побочные электромагнитные излучения и наводки

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [4] на с. 92-98.
Вопрос 2 изложен в учебном пособии [4] на с. 129-166.

Контрольные вопросы по теме 2:
1. Пояснить сущность опасных сигналов и их источников.
2. В чём отличие функциональных сигналов от случайных?
3. Привести 3-4 примера функциональных и случайных сигналов.
4. Что такое побочные электромагнитные излучения и наводки (ПЭМИН)?
5. Пояснить физическую природу побочных преобразований акустических сигналов в электрические сигналы.
6. Пояснить физическую природу паразитных связей и наводок.
7. Пояснить физическую природу низкочастотных и высокочастотных излучений технических средств.
8. Что такое ВЧ-навязывание?

9. Пояснить физическую природу электромагнитных излучений сосредоточенных и распределённых источников.

10. Пояснить физическую природу утечки информации по цепям электропитания и заземления.

Тесты для самостоятельной работы:

1. К основным источникам функциональных сигналов относятся:

а) Излучатели акустических сигналов гидролокаторов и акустической связи

б) Электропроводящие коммуникации здания, проходящие через контролируемую зону

в) Средства мобильной телефонной и радиосвязи

2. Емкостная паразитная связь образуется в результате:

а) Воздействия магнитного поля

б) Воздействия электрического поля

в) Воздействия активного сопротивления

3. Низкочастотное излучение – это:

а) Электромагнитные поля, частота которых соответствует звуковому диапазону

б) Электромагнитные поля, излучаемые цепями радиоэлектронных средств

4. Что из перечисленного относится к случайным акустоэлектричесим преобразователям?

а) Металлические корпуса средств и приборов

б) Монтажные провода, соединительные кабели, токопроводы печатных плат

в) Ферромагнитные материалы в виде сердечников трансформаторов и дросселей

5. Что из перечисленного относится к случайным акустоэлектричесим преобразователям?

а) Металлические корпуса средств и приборов

б) Монтажные провода, соединительные кабели, токопроводы печатных плат

в) Ферромагнитные материалы в виде сердечников трансформаторов и дросселей

6. Основным распределенным источником магнитного, электрического и электромагнитного полей является:

а) Анизотропный излучатель

б) Симметричный/несимметричный кабель

в) Цепь звукоусилительной аппаратуры

г) Кабель внутренней АТС

7. Цепи заземления в общем случае создаются для выполнения следующих функций:
а) Создание электрического поля
б) Модуляция тока электропитания токами радиоэлектронного средства
в) Обеспечение путей для протекания возвратных (обратных) питающих и сигнальных токов

2.3. РАЗДЕЛ 1. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 3. ОСНОВНЫЕ НАПРАВЛЕНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Основные вопросы:

1. Основные факторы обеспечения защиты информации от угроз утечки информации

2. Классификация направлений и методов инженерно-технической защиты информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 280-282.

Вопрос 2 изложен в учебном пособии [1] на с. 287-300.

Для самостоятельного изучения вопроса 2 следует обратиться к [2] на с. 248-278.

Контрольные вопросы по теме 3

1. Перечислить основные факторы обеспечения защиты информации от угроз утечки информации.
2. Пояснить условия образования типового технического канала утечки информации.
3. Что необходимо сделать для предотвращения утечки информации по техническому каналу?
4. Перечислить основные направления технической защиты информации.
5. Перечислить и охарактеризовать основные методы технической защиты информации.
6. Что подразумевается под пространственным, структурным и временным скрытием.
7. Что такое компьютерная стеганография?

Тесты для самостоятельной работы:

1. Какой из нижеперечисленных факторов влияет на эффективность защиты информации от утечки?

а) Отношение сигнал/шум на входе приемника сигналов

б) Время и затраты на поиск канала утечки

в) Демаскирующие признаки носителя информации

2. Что необходимо сделать для предотвращения утечки информации по техническому каналу?

а) Увеличить мощность носителя

б) Нейтрализовать преднамеренные и случайные воздействия на источник информации

в) Уменьшить информативность признаковой структуры объектов защиты

3. К какому виду сокрытия информации относится стеганография?

а) Структурное скрытие

б) Временное скрытие

в) Энергетическое скрытие

г) Пространственное скрытие

2.4. РАЗДЕЛ 2. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

ТЕМА 4. ТИПОВАЯ СТРУКТУРА И ВИДЫ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Основные вопросы:

1. Типовая структура и виды технических каналов утечки информации.
2. Классификация технических каналов утечки информации
3. Основные показатели технических каналов утечки информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 171-180.

Для самостоятельного изучения вопроса 1 следует обратиться к [2] на с. 9-17.

Вопрос 2 изложен в учебном пособии [4] на с. 169-171.

Вопрос 3 изложен в учебном пособии [4] на с. 180-190.

Контрольные вопросы по теме 4:

1. Пояснить структуру образования канала утечки.
2. В чём заключается отличие ОТСС от ВТСС? Привести 4-5 примеров.
3. Раскрыть типовой канал утечки информации за счет возникновения паразитной генерации и самовозбуждения.
4. Раскрыть типовой канал утечки информации вследствие акусто-звуковых преобразований.

5. Раскрыть типовой канал утечки информации, образованный высокочастотным облучением и ВЧ-навязыванием.

6. Раскрыть типовой канал утечки информации по цепям электропитания и заземления.

7. Пояснить классификацию технических каналов утечки информации.

8. Основные показатели технических каналов утечки информации.

Тесты для самостоятельной работы:

1. Что является способом защиты от утечки, возникшей за счет высокочастотного облучения и ВЧ-навязывания?

а) Генерирование «розового» шума
в) Осуществление периодических проверок на увеличение тока потребления
г) Создание помех в диапазоне от 100 до 1000 мГц
д) Соблюдение размеров контролируемых зон

2. Что является важнейшим показателем технического канала утечки?

а) Пропускная способность
б) Информативность
в) Длина
г) Среда

3. Каким показателем характеризуется источник сигнала?

а) Мощность помех
б) Чувствительность
в) Диаграмма направленности излучения
г) Скорость распространения сигнала в среде

4. Каким из параметров обладает приемник сигналов?

а) Динамический диапазон сигнала
б) Параметр спектра сигнала
в) Пространственная селективность приемной антенны
г) Амплитудно-частотная характеристика

2.5. РАЗДЕЛ 2. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

ТЕМА 5. АКУСТИЧЕСКИЕ, ВИБРОАКУСТИЧЕСКИЕ И ОПТИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Основные вопросы:

1. Характеристика и противодействие акустическим и виброакустическим каналам утечки информации

2. Характеристика и противодействие оптическим каналам утечки информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 352-360.

Для самостоятельного изучения вопроса 1 следует обратиться к [2] на с. 14-25.

Вопрос 2 изложен в учебном пособии [4] на с. 312-320.

Для самостоятельного изучения вопроса 2 следует обратиться к [2] на с. 26-27.

Контрольные вопросы по теме 5:

1. Что такое преобразователи акустических и вибрационных колебаний? Привести 5-6 примеров.
2. Что такое автономные закладные устройства? Привести 3-4 примера.
3. Пояснить физическую природу виброакустического канала утечки.
4. Назвать пассивные и активные способы защиты речи от несанкционированного прослушивания.
5. Основные правила выбора ограждающих конструкций выделенных помещений в процессе проектирования.
6. Типовая аппаратура активной защиты помещений от утечки речевой информации.
7. Назвать характерные особенности постановки акустических помех.
8. Основные рекомендации по выбору систем виброакустической защиты.
9. Назвать основные технические каналы утечки видовой информации.
10. Основные средства противодействия наблюдению в оптическом диапазоне.

Тесты для самостоятельной работы:

1. К какому каналу утечки относятся трубы водоснабжения?

а) Параметрический
б) Вибрационный
в) Оптоэлектронный
г) Виброакустический

2. Что относится к активным способам защиты выделенных помещений?

а) Использование генераторов шума
б) Использование двойных дверей
в) Звукоизоляция помещений

3. Что из перечисленного относится к портативным подавителям диктофонов?

а) «ANG-2000»
б) «Шумотрон-3»
в) «Шорох»

4. Какой из перечисленных приборов является генератором шума?
а) «Порог-2М»
б) «Шторм»
в) «Штурм»
г) ST-031M «Пиранья»

5. Что из перечисленного относится к стационарным подавителям диктофонов?
а) VNG-006
б) «Буран-4»
в) «Шорох»

2.6. РАЗДЕЛ 2. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

ТЕМА 6. ЭЛЕКТРОМАГНИТНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАЗУЕМЫЕ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Основные вопросы:

1. Характеристика режимов обработки информации в ПЭВМ с точки зрения утечки информации
2. Потенциально информативные и неинформативные излучения
3. Электрические каналы утечки информации
4. Специально создаваемые технические каналы утечки информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 686-690.

Для самостоятельного изучения вопроса 1 следует обратиться к [2] на с. 27-29.

Вопрос 2 изложен в учебном пособии [4] на с. 423-454.

Вопрос 3 изложен в учебном пособии [4] на с. 690-696.

Вопрос 4 изложен в учебном пособии [4] на с. 654-658.

Контрольные вопросы по теме 6:

1. Перечислить 5-6 режимов обработки информации средствами вычислительной техники (СВТ), наиболее опасных с точки зрения утечки информации.
2. Дать характеристику режима вывода информации на экран монитора с точки зрения утечки информации.
3. Дать характеристику режима ввода данных с клавиатуры с точки зрения утечки информации.
4. Дать характеристику режима записи информации на накопители с точки зрения утечки информации.

5. Дать характеристику режима передачи данных в каналы связи с точки зрения утечки информации.

6. Дать характеристику потенциально информативных и неинформативных излучений.

7. Охарактеризовать наводки информативных сигналов в линиях электропитания ЭВМ.

8. Охарактеризовать наводки информативных сигналов в линиях электропитания и соединительных линиях ВТСС.

9. Охарактеризовать наводки информативных сигналов в цепях заземления ЭВМ и ВТСС

10. Охарактеризовать наводки информативных сигналов в посторонних проводниках (металлических трубах систем отопления, водоснабжения, металлоконструкциях и т.д.).

11. Специально создаваемые технические каналы утечки информации.

12. Дать вариант классификации аппаратных закладок.

13. Что такое программные закладки? Привести 2-3 примера.

Тесты для самостоятельной работы:

1. Какой из режимов обработки информации средствами ВТ является наиболее опасным с точки зрения утечки информации?

а) Чтение информации с накопителей
б) Передача данных в каналы связи
в) Вывод информации на экран монитора
г) Ввод данных с клавиатуры

2. Какие из перечисленных цепей не формируют потенциально-информативные ПЭМИН?

а) Цепи, формирующие шину данных системной шины компьютера
б) Внутренние цепи блока питания компьютера
в) Цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора
г) Цепи, формирующие шину данных системной шины компьютера

3. Какие из перечисленных цепей не формируют неинформативные ПЭМИ?

а) Цепи, передающие сигналы аппаратных прерываний
б) Цепи, формирующие шину управления и шину адреса системной шины
в) Цепи формирования и передачи сигналов синхронизации
г) Внутренние цепи блока питания компьютера
д) Цепи, формирующие шину данных внутри микропроцессора

4. Где не могут возникнуть наводки информативных сигналов?

а) В линиях электропитания ЭВМ
б) В цепях заземления ЭВМ и ВТСС

в) В полипропиленовых трубах систем отопления
г) В линиях электропитания и соединительных линиях ВТСС

5. Что необходимо для возникновения канала утечки?
а) Чтобы соединительные линии ВТСС, линии электропитания, посторонние проводники и т.д., выполняющие роль случайных антенн, выходили за пределы контролируемой зоны объекта
б) Чтобы расстояние от СВТ до случайной сосредоточенной антенны было более r1, и расстояние до случайной распределённой антенны было более r1
в) Чтобы была возможность непосредственного подключения к случайной антенне только в пределах контролируемой зоны объекта средств разведки ПЭМИН

6. Каких закладных устройств, внедряемых в СВТ, по виду перехватываемой информации не существует?
а) Аппаратные закладки для перехвата изображений, выводимых на экран монитора
б) Аппаратные закладки для перехвата информации, хранящейся в оперативной памяти
в) Аппаратные закладки для перехвата информации, записываемой на жёсткий диск ПЭВМ
г) Аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ

7. Каким путем нельзя осуществить перехват информации, обрабатываемой СВТ?
а) Перехватом побочных электромагнитных излучений, возникающих при работе СВТ
б) Перехватом наводок информативных сигналов с соединительных линий ВТСС и посторонних проводников
в) «Низкочастотного облучения» СВТ

2.7. РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

ТЕМА 7. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ В ЭЛЕКТРОМАГНИТНОМ КАНАЛЕ

Основные вопросы:

1. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале
2. Экранирование, зашумление и фильтрация опасных сигналов
3. Методы и средства измерения уровня защищённости от утечки по электромагнитному каналу

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 339-360, 686-690.

Вопрос 2 изложен в учебном пособии [4] на с. 364-366.

Вопрос 3 изложен в учебном пособии [4] на с. 266-273.

Контрольные вопросы по теме 7:

1. Перечислить основные задачи пассивных методов защиты информации.
2. Дать характеристику основным пассивным техническим средствам защиты.
3. Перечислить основные задачи активных методов защиты информации.
4. Пояснить понятия электростатического, магнитостатического и электромагнитного экранирования.
5. Что такое зашумление? Раскрыть понятия линейного и пространственного зашумления.
6. Показать физические основы фильтрации.
7. Раскрыть основные методы и средства измерения уровня защищённости от утечки по электромагнитному каналу.

Тесты для самостоятельной работы:

1. На что направлены пассивные методы защиты?

а) На создание маскирующих пространственных электромагнитных помех

б) На создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС

в) На ослабление побочных электромагнитных излучений

2. На что направлены активные методы защиты?
а) На ослабление наводок побочных электромагнитных излучений
б) На создание маскирующих пространственных электромагнитных помех
в) На исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания

3. За счет чего происходит ослабление побочных электромагнитных излучений ТСПИ и их наводок в посторонних проводниках?
а) Экранирование и заземление ТСПИ и их соединительных линий
б) Фильтрация информационных сигналов
в) Пространственное и линейное зашумление

4. В каких системах, средствах информатизации и связи не может осуществляться фильтрация?
а) В высокочастотных трактах передающих и приемных устройств
б) В различных сигнальных цепях технических средств
в) В цепях электропитания, управления, контроля, коммутации технических средств
г) В металлических проводящих конструкциях

2.8. РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

ТЕМА 8. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ В АКУСТИЧЕСКОМ (ВИБРОАКУСТИЧЕСКОМ) КАНАЛЕ

Основные вопросы:

1. Методы пассивной и активной защиты от утечки в акустическом (виброакустическом) канале
2. Технические средства обнаружения утечки информации по акустическому (виброакустическому) каналу
3. Средства противодействия перехвату «информации по акусто-вибрационному каналу

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 323-339.

Для самостоятельного изучения вопроса 1 следует обратиться к [2] на с. 278-300.

Вопрос 2 изложен в учебном пособии [4] на с. 339-358.

Для самостоятельного изучения вопроса 2 следует обратиться к [1] на с. 122-222.

Вопрос 3 изложен в учебном пособии [4] на с. 358-360.

Контрольные вопросы по теме 8:

1. Что такое закладные устройства в акустическом (виброакустическом) канале?
2. Привести вариант классификации закладных устройств.
3. Основные методы пассивной и активной защиты речевой информации.
4. Основные цели пассивных методов защиты речевой информации.
5. Основные цели активных методов защиты речевой информации.
6. Каким образом может осуществляться звукоизоляция помещений?
7. Привести 3-4 технических средства обнаружения утечки информации по акустическому (виброакустическому) каналу и назвать их основные технические характеристики.
8. Основные средства обнаружения и подавления диктофонов и акустических закладок.
9. Основные средства обнаружения и подавления диктофонов и акустических закладок
10. Назвать основные средства противодействия перехвату «информации по акустовибрационному каналу.

Тесты для самостоятельной работы:

1. На какие группы по способу регистрации можно разить закладные устройства?

а) С помощью проводных линий
б) С помощью оптического канала
в) С помощью микрофона

2. На какие группы по способу передачи можно разбить закладные устройства?

а) С помощью радиоканала
б) С помощью пьезокристаллического датчика
в) С помощью модуляции отраженного луча от светоотражающих поверхностей

3. На что направленны пассивные методы защиты акустической информации?

а) Создание маскирующих акустических и вибрационных помех
б) Создание маскирующих электромагнитных помех
в) Ультразвуковое подавление диктофонов в режиме записи
г) Обнаружение излучений акустических закладок

4. На что направленны активные методы защиты акустической информации?

а) Ослабление акустических (речевых) сигналов
б) Ослабление информационных электрических сигналов

в) Электромагнитное подавление диктофонов в режиме записи

5. Чем осуществляется ослабление информационных электрических сигналов?
а) Методами фильтрации сигналов
б) Путем звукоизоляции помещений
в) Путем использования генераторов помех

6. Какое устройство используется для локализации установленных закладных устройств?
а) «Рубеж»
б) «Дельта»
в) «Сова»

7. Какое устройство используется для обнаружения работающих в режиме записи диктофонов?
а) TRD-800
б) СМР-700
в) OSCOR OSC-500

8. Какое устройство используется для электромагнитного подавления диктофонов?
а) ST-031 «Пиранья»
б) NR-90EM
в) «Рубеж»

9. Какое устройство используется для электромагнитного подавления диктофонов?
а) ST-031 «Пиранья»
б) NR-90EM
в) «Рубеж»

10. Для чего предназначен генератор шума ANG-2000?
а) Для создания виброакустических помех с целью защиты от проводных и радиомикрофонов
б) Для защиты информации от утечки по акустическим и виброакустическим каналам
в) Для защиты объектов информатизации 1 категории и противодействия техническим средствам перехвата речевой информации

2.9. РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

ТЕМА 9. МЕРОПРИЯТИЯ ПО ВЫЯВЛЕНИЮ СРЕДСТВ ТЕХНИЧЕСКОЙ РАЗВЕДКИ. МЕТОДИКА ПОИСКА СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Основные вопросы:

1. Общая характеристика средств технической разведки
2. Основные мероприятия по выявлению средств технической разведки
3. Методика и средства поиска специальных технических средств

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 402-411.

Вопрос 2 изложен в учебном пособии [4] на с. 721-740.

Для самостоятельного изучения вопроса 2 следует обратиться к [2] на с. 343-360

Вопрос 3 изложен в учебном пособии [2] на с. 361-420.

Для самостоятельного изучения вопроса 3 следует обратиться к [1] на с. 223-248.

Контрольные вопросы по теме 9:

1. Дать общую характеристику основных средств технической разведки.
2. Привести вариант классификации средств технической разведки.
3. Перечислить основные мероприятия по выявлению средств технической разведки.
4. Основные мероприятия и средства радиообнаружения.
5. Последовательность осмотра помещения.
6. Порядок обследования электрических и электронных приборов.
7. Порядок проверки проводных коммуникаций.
8. Методика и средства поиска специальных технических средств

Тесты для самостоятельной работы:

1. Чем технические средства расширяют и дополняют возможности человека по добыванию информации?

а) Возможностью консервировать информацию на непродолжительное время

б) Съемом информации с носителей, которые недоступны органам чувств человека

в) Возможностью добычи информации за пределами контролируемой зоны

2. Что не должно входить в состав отчетных документов о проведении обследования помещения?
а) Протоколы изъятия средств съема информации
б) Рекомендации по устранению и нейтрализации технических каналов утечки
в) Методические рекомендации о степени защищенности объекта

3. Какое устройство, из перечисленных, подходит для проверки наличия и опасности НЧ-магнитных полей?
а) D-008
б) Трап-Н50
в) МТ-402
г) Цифровой мультимер

4. Какое устройство, из перечисленных, способно выявить специальные технические средства в выключенном состоянии?
а) ST-032 «Пиранья»
б) D-008
в) МТ-110
г) «Обь»

5. Какое устройство, из перечисленных, предназначено для проверки телефонных коммуникаций?
а) Цифровой мультиметр
б) OSC-5000
в) NR-900EM