

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

Иванцов А.М., Логинов А.А.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ
СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ТЕХНИЧЕСКИЕ СРЕДСТВА
ОБНАРУЖЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ»**

Для студентов специалитета по специальностям 10.05.03
очной формы обучения

Ульяновск, 2020

Методические указания для самостоятельной работы студентов по дисциплине «Технические средства обнаружения каналов утечки информации» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2020. Настоящие методические указания предназначены для студентов специалитета по специальностям 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.....	4
2. Методические указания.....	7
2.1. Раздел 1. Теоретические основы возникновения технических каналов утечки информации Тема 1. Классификация и основные характеристики технических каналов утечки информации.....	7
2.2. Раздел 1. Тема 2. Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации.....	8
2.3. Раздел 1. Тема 3. Каналы утечки акустической речевой информации.....	10
2.4. Раздел 1. Тема 4. Каналы утечки видовой информации.....	11
2.5. Раздел 2. Основные методы и средства обнаружения технических каналов утечки информации. Тема 5. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации. Часть 1.....	12
2.6. Раздел 2. Тема 6. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации. Часть 2.....	13
2.7. Раздел 2. Тема 7. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации. Часть 3.....	14
2.8. Раздел 2. Тема 8. Методы и средства выявления электромагнитных каналов утечки информации технических средств обработки и передачи информации.....	
2.9. Раздел 2. Тема 9. Методы и средства выявления электрических каналов утечки информации технических средств обработки и передачи информации.....	
2.10. Раздел 2. Тема 10. Методы и средства выявления каналов утечки акустической речевой информации.....	
2.11. Раздел 3. Основные мероприятия по выявлению технических каналов утечки информации Тема 11. Организация специальных обследований помещений и специальных проверок технических средств.....	
2.12. Раздел 3. Тема 12. Организация специальных исследований технических средств и помещений.....	

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

основная

1. «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282. ДСП

2. «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации». Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП

3. «Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации». Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП

4. «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам». Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП

5. «Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электро-акустических преобразований во вспомогательных технических средствах и системах». Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП

6. «Положение о системе сертификации средств защиты информации». Утверждено приказом ФСТЭК России от 03.04.2018 г. № 55. Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/119-polozheniya/1594-polozhenie-utverzhdeno-prikazom-fstek-rossii-ot-3-aprelya-2018-g-n-55>

7. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. - 320 с.

8. Бузов Г.А., Калинин С.В., Кондратьев А.В., Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.: ил.

9. 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>

10. 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>

11. Свиначев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / Свиначев 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>

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. Нет подписки

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 № 5485-1 «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/

3.5 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_147084/

учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" [Электронный ресурс] : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий, Каф. информ. безопасности и теории управления. - Электрон. текстовые дан. (1 файл : 352 КБ). - Ульяновск : УлГУ, 2017. URL: http://lib.ulsu.ru/MegaPro/Download/MObject/915/Andreev_2017.pdf

2. Андреев А. С. 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" [Электронный ресурс] / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Электрон. текстовые дан. (1 файл : 14, 7 Мб). - Ульяновск : УлГУ, 2015. URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf>

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. Раздел 1. Теоретические основы возникновения технических каналов утечки информации

Тема 1. Классификация и основные характеристики технических каналов утечки информации

Основные вопросы:

1. Классификация технических каналов утечки информации
2. Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации (ТС ОПИ)
3. Каналы утечки акустической речевой информации (АРИ)
4. Каналы утечки видовой информации.
5. Модель технического канала утечки информации и основные характеристики.

Рекомендации по изучению темы:

Вопрос 1 изложен на интернет ресурсе

https://ru.bmstu.wiki/index.php?title=Классификация_технических_каналов_утечки_информации&mobileaction=toggle_view_mobile

и национальном стандарте ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

Вопрос 2 изложен в учебном пособии [10] на с. 23-25.

Для самостоятельного изучения вопроса 2 следует обратиться к [7,8]

Вопрос 3 изложен в учебном пособии [10] на с. 15-22.

Для самостоятельного изучения вопроса 3 следует обратиться к [7,8]

Вопрос 4 изложен в учебном пособии [10] на с. 26-27.

Для самостоятельного изучения вопроса 4 следует обратиться к [7,8]

Вопрос 5 изложен в учебном пособии [10] на с. 10-14.

Для самостоятельного изучения вопроса 5 следует обратиться к интернет ресурсу https://studopedia.ru/18_70343_osnovnie-pokazateli-tehnicheskikh-kanalov-utechki-informatsii.html

Контрольные вопросы по теме 1:

1. Классификация технических каналов утечки информации по причинам возникновения и виду информации.
2. Перечислить каналы утечки информации, обрабатываемой ТС ОПИ, каналы утечки АРИ и каналы утечки видовой информации
3. Перечислить основные характеристики ТКУИ

Тесты для самостоятельной работы:

1. Чем отличается технический канал утечки информации от канала связи?

- а) средой распространения сигнала
- б) типом получателя информации
- в) видом помехи в канале
- г) все ответы верны

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. Что является важнейшим показателем технического канала утечки?

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

2.2. Раздел 1. Теоретические основы возникновения технических каналов утечки информации

Тема 2. Каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации.

Основные вопросы:

1. Электромагнитные каналы утечки информации ТС ОПИ
2. Электрические каналы утечки информации ТС ОПИ
3. Возможности технической разведки ПЭМИН.

Рекомендации по изучению темы:

Вопросы 1-2 изложены в учебном пособии [10] на с. 23-25.

Для самостоятельного изучения вопросов 1-2 следует обратиться к [7,8], национальному стандарту ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

Для самостоятельного изучения вопроса 3 следует обратиться к «Перечню контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности

по технической защите конфиденциальной информации», утвержденным директором ФСТЭК России 19.04.2017

Контрольные вопросы по теме 2:

1. Перечислить электромагнитные каналы утечки информации
2. Перечислить электрические каналы утечки информации
3. Перечислить технической разведки ПЭМИН (диапазоны частот приемников и антенн)

Тесты для самостоятельной работы:

1. К электромагнитным каналам утечки информации относится:

- а) Магнитные и электрические излучения
- б) Лазерные излучения
- в) Инфракрасные излучения
- г) Электромагнитные излучения

2. К электрическим каналам утечки информации относится:

- а) Наводки на линию телефонной связи
- б) Электрические излучения
- в) Наводки на линию электропитания и заземления
- г) Наводки на воздушную линию

3. Какими возможностями должна обладать аппаратура разведки побочных электромагнитных излучений и наводок:

- а) Широкой полосой пропускания приемника и антенны
- б) Минимальными массогабаритными показателями
- в) Чувствительностью приемника
- г) Минимальной стоимостью

2.3. Раздел 1. Теоретические основы возникновения технических каналов утечки информации

Тема 3. Каналы утечки акустической речевой информации

Основные вопросы:

1. Акустические, виброакустические (вибрационные) каналы и оптико-электронные (лазерные) утечки АРИ.
- 2 Акустоэлектрические, параметрические и акустооптические каналы утечки АРИ.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [10] на с. 16-17.

Вопрос 2 изложен в учебном пособии [10] на с. 17-22.

Для самостоятельного изучения вопросов 1-2 следует обратиться к [7,8]

Контрольные вопросы по теме 3:

1. Перечислить каналы утечки акустической речевой информации, характерные для выделенных помещений
2. Перечислить каналы утечки акустической речевой информации, характерные для технических средств, установленных в выделенных помещениях

Тесты для самостоятельной работы:

1. К каналам утечки акустической речевой информации относится:

- а) Магнитные и электрические излучения
- б) Акустические колебания
- в) Лазерные излучения
- г) Вибрационные колебания

2. К параметрическим каналам утечки акустической речевой информации относится:

- а) Высокочастотное навязывание
- б) Электрические сигналы
- в) Электромагнитные излучения
- г) Высокочастотное облучение

3. К акустоэлектрическим преобразователям относятся:

- а) Индуктивные преобразователи
- б) Электрические преобразователи
- в) Емкостные преобразователи
- г) Магнитные преобразователи

2.4. Раздел 1. Теоретические основы возникновения технических каналов утечки информации

Тема 4. Каналы утечки видовой информации

Основные вопросы:

1. Наблюдение за объектом. Съёмка объектов.
2. Электронные устройства негласного получения информации (аппаратные закладки, аудиозакладки и видеозакладки)
3. Возможности технической разведки ЭУНПИ

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [10] на с. 26-27.

Для самостоятельного изучения вопроса 1 следует обратиться к [7,8]

Вопросы 2-3 изложены в учебном пособии [10] на с. 50-102.

Для самостоятельного изучения вопросов 2,3 следует обратиться к [7,8]

Контрольные вопросы по теме 4:

1. Перечислить состав и характеристики аппаратных закладок
2. Перечислить состав и характеристики аудиозакладок и видеозакладок

Тесты для самостоятельной работы:

1. Вид входного преобразователя акустической закладки:

- а) Микрофон
- б) Электрическая антенна
- в) Вибропреобразователь
- г) Магнитная антенна

2. Вид преобразователя закладки на проводной линии:

- а) Вибропреобразователь
- б) Адаптер
- в) Микрофон
- г) Магнитная антенна

3. Основные свойства электронных устройств негласного получения информации:

- а) Миниатюризация
- б) Скрытное функционирование
- в) Скрытная установка
- г) Удешевление

2.5. Раздел 2. Основные методы и средства обнаружения технических каналов утечки информации

Тема 5. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации. Часть 1.

Основные вопросы:

1. Радиоконтроль (радиомониторинг) эфира и линий – методы выявления активных ЭУНПИ с передачей информации по радиоканалу (включая сотовые и беспроводные сети) и отходящим линиям.
2. Основные характеристики современных автоматизированных поисковых комплексов российских производителей.

Рекомендации по изучению темы:

Для самостоятельного изучения вопросов 1-2 следует обратиться к интернет ресурсам:

- <http://detektor.ru/prod/self/srch/radiomonitoring1/>
- <http://www.inspectorsoft.ru/soft.php>
- <https://nelk.ru/catalog/>
- <http://www.novocom.ru/ru/public-catalog>
- <https://www.tezasy.ru/>
- <http://radioservice.ru/>
- http://www.ircos.ru/ru/asrp_main.html

Контрольные вопросы по теме 5:

1. Перечислите основных российских производителей автоматизированных поисковых комплексов

Тесты для самостоятельной работы:

1. Какой из перечисленных приборов является аппаратурой радиоконтроля?

- а) «Аврора-3»
- б) «Сканер-ЦП»
- в) «Кассандра-СО»
- г) «Омега-М5»

2. Какой из перечисленных приборов выявляет ЭУНПИ, использующий WI-FI:

- а) «Саламандра»
- б) «Рубин»
- в) «Сканер-ЦП»
- г) «Сириус»

3. Основные параметры автоматизированных комплексов радиоконтроля:

- а) Чувствительность
- б) Точность
- в) Динамический диапазон
- г) Анализ гармоник

2.6. Раздел 2. Основные методы и средства обнаружения технических каналов утечки информации

Тема 6. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации. Часть 2.

Основные вопросы:

1. Активные методы выявления ЭУНПИ с дистанционным управлением и пассивных ЭУНПИ в эфире и отходящих линиях.
2. Основные характеристики современных автоматизированных поисковых комплексов российских производителей.

Рекомендации по изучению темы:

Для самостоятельного изучения вопросов 1-2 следует обратиться к интернет ресурсам:

- <http://detektor.ru/prod/self/audit/>
- <https://nelk.ru/catalog/>
- <http://www.novocom.ru/ru/public-catalog>
- <http://nera-s.com/catalog?cat=4>
- <https://answerpro.ru/services/hardware-development/krokus-kcp/#services>
- <http://www.saomega.ru/produkty-i-resheniya>

Контрольные вопросы по теме 6:

1. Перечислите основных российских производителей автоматизированных поисковых комплексов

Тесты для самостоятельной работы:

1. Какой из перечисленных приборов является аппаратурой высокочастотного облучения?

- а) «Сканер-ЦП»
- б) «Ревиз»
- в) «Парнас»
- г) «Омега-М5»

2. Основные параметры автоматизированных комплексов высокочастотного облучения и навязывания:

- а) Чувствительность
- б) Точность
- в) Динамический диапазон
- г) Коэффициент модуляции

3. Какой из перечисленных приборов является аппаратурой высокочастотного навязывания?

- а) «Сканер-ЦП»
- б) «Сириус»
- в) «Крона»
- г) «Омега-М5»

2.7. Раздел 2. Основные методы и средства обнаружения технических каналов утечки информации

Тема 7. Методы и средства обнаружения технических каналов утечки информации за счет электронных устройств негласного получения информации. Часть 3.

Основные вопросы

- 1. Методы неразрушающего контроля
- 2. Метод оптической локации.
- 3. Метод нелинейной локации.
- 4. Рефлектометрический метод.
- 5. Основные характеристики современной досмотровой техники.

Рекомендации по изучению темы:

Для самостоятельного изучения вопросов 1 и 5 (тепловой или инфракрасный контроль; вихретоковый контроль) следует обратиться к интернет ресурсам:

- <http://www.novocom.ru/ru/public-catalog>
- <https://nelk.ru/catalog/>
- http://signal-t.ru/catalog/signal_t/
- <http://spymarket.com/tovary>
- http://detektor.ru/prod/self/srch/selective_detectors/

Для самостоятельного изучения вопросов 2 и 5 следует обратиться к интернет ресурсам:

- <http://www.novocom.ru/ru/public-catalog>
- <https://www.analitika.info/catalog>
- <https://www.spektr-at.ru/catalogue/>
- <https://www.bugshunt.ru/info/news/obnaruzhitel-skrytykh-videokamer-vizir/>

- <https://suritel.ru/catalog/all/>

Для самостоятельного изучения вопросов 3 и 5 следует обратиться к интернет ресурсам:

- http://detektor.ru/prod/self/srch/nelinejnaya_lokaciya/
- <http://spymarket.com/catalog/folder/dosmotr.htm>
- <http://nera-s.com/catalog?cat=1>
- <http://www.elvira.ru/>
- <https://reicom.ru/information-protection/nonlinear-locators>

Для самостоятельного изучения вопросов 4 и 5 следует обратиться к интернет ресурсам:

- <https://reicom.ru/information-protection/analyzers-wireline>
- <http://www.novocom.ru/ru/public-catalog>
- <http://spymarket.com/tovary>

Контрольные вопросы по теме 7:

1. Перечислите основных российских производителей автоматизированных поисковых комплексов

Тесты для самостоятельной работы:

1. Основные параметры досмотрового оборудования, выявляющие инфракрасный канал:

- а) Диапазон частот
- б) Диапазон длин волн
- в) Расстояние
- г) Чувствительность

2. Основные параметры досмотрового оборудования, применяющие метод нелинейной локации:

- а) Точность
- б) Диапазон длин волн
- в) Расстояние
- г) Чувствительность

3. Основные параметры досмотрового оборудования, применяющие метод оптической локации:

- а) Дальность
- б) Диапазон длин волн
- в) Поле зрения
- г) Чувствительность

2.8. Раздел 2. Основные методы и средства обнаружения технических каналов утечки информации

Тема 8. Методы и средства выявления электромагнитных каналов утечки информации технических средств обработки и передачи информации

Основные вопросы

1. Методика оценки защищенности интерфейсов ТС ОПИ от утечки конфиденциальной информации за счет побочных электромагнитных излучений.
2. Предъявляемые требования к измерительной аппаратуре.
3. Предъявляемые требования к средствам активной защиты информации.

Рекомендации по изучению темы:

Вопрос 1 изложен в документе [2].

Вопрос 2 изложен в:

«Перечне контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.02.2012г. № 79», утвержденным директором ФСТЭК России 19.04.2017

<https://fstec.ru/normotvorcheskaya/litsenzirovanie/76-inye/438-perechen-utverzhdn-direktorom-fstek-rossii-3-aprelya-2012-g>

«Перечне контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.03.2012г. № 171», утвержденным директором ФСТЭК России 06.2018

<https://fstec.ru/normotvorcheskaya/litsenzirovanie/76-inye/1383-perechen-utverzhdn-direktorom-fstek-rossii-29-avgusta-2017-g>

Для самостоятельного изучения вопроса 3 следует обратиться к интернет ресурсам:

- <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>
- <http://npoanna.ru>
- <http://www.pps.ru>
- <https://www.rnt.ru/ru>
- <http://www.infopro.ru/>
- <http://forso.ru>
- <https://www.apsecurity.ru/catalog/ke-dr-p.html>
- <http://cstbi.ru/>

- <https://www.irsural.ru/szi/pemin/saz/>
- <https://suritel.ru>
- <https://voentelecom.ru/projects/razrabotka-novykh-obraztsov-tekhniki-svyazi/sazan/>
- <https://www.krypton-niiaa.ru>

Контрольные вопросы по теме 8:

1. Перечислите основные этапы методики оценки защищенности.
2. Перечислите требования, предъявляемые к аппаратуре измерения побочных электромагнитных излучений.
3. Перечислите основных российских производителей средств защиты информации

Тесты для самостоятельной работы:

1. Какой из режимов обработки информации средствами вычислительной техники является наиболее опасным с точки зрения утечки информации за счет побочных электромагнитных излучений:

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

2. На что направлены активные методы защиты:

- а) На ослабление наводок побочных электромагнитных излучений
- б) На создание маскирующих электромагнитных помех
- в) На исключение (ослабление) просачивания информативных сигналов в цепи электропитания

3. Предъявляемые требования к аппаратуре измерения побочных электромагнитных излучений

- а) Диапазон частот
- б) Чувствительность
- в) Погрешность
- г) Класс точности

2.9. Раздел 2. Основные методы и средства обнаружения технических каналов утечки информации

Тема 9. Методы и средства выявления электрических каналов утечки информации технических средств обработки и передачи информации.

Основные вопросы

1. Методика оценки защищенности интерфейсов ТС ОПИ от утечки конфиденциальной информации за счет наводок побочных электромагнитных излучений
2. Предъявляемые требования к измерительной аппаратуре.
3. Предъявляемые требования к пассивным средствам защиты информации

Рекомендации по изучению темы:

Вопрос 1 изложен в документе [3].

Вопрос 2 изложен в:

«Перечне контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.02.2012г. № 79», утвержденным директором ФСТЭК России 19.04.2017

<https://fstec.ru/normotvorcheskaya/litsenzirovanie/76-inye/438-perechen-utverzhdn-direktorom-fstek-rossii-3-aprelya-2012-g>

«Перечне контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.03.2012г. № 171», утвержденным директором ФСТЭК России 06.2018

<https://fstec.ru/normotvorcheskaya/litsenzirovanie/76-inye/1383-perechen-utverzhdn-direktorom-fstek-rossii-29-avgusta-2017-g>

Для самостоятельного изучения вопроса 3 следует обратиться к интернет ресурсам:

- <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>

- <http://filters-fspk.ru>

- <http://priborvbg.ru>

- <http://www.pps.ru>

- <http://npoanna.ru>

- <https://filtr-fp.ru>

Контрольные вопросы по теме 9:

1. Перечислите основные этапы методики оценки защищенности.
2. Перечислите требования, предъявляемые к аппаратуре измерения наводок побочных электромагнитных излучений.
3. Перечислите основных российских производителей средств защиты информации

Тесты для самостоятельной работы:

1. На что направлены пассивные методы защиты:

- а) На создание маскирующих электромагнитных помех
- б) На создание маскирующих электрических помех в посторонних проводниках и соединительных линиях
- в) На ослабление побочных электромагнитных излучений и наводок

2. Предъявляемые требования к аппаратуре измерения наводок побочных электромагнитных излучений:

- а) Диапазон частот
- б) Чувствительность
- в) Погрешность
- г) Класс точности

3. Предъявляемые требования к средствам пассивной защиты:

- а) Диапазон частот
- б) Чувствительность
- в) Неравномерность амплитудно-частотной характеристики
- г) Коэффициент затухания

2.10. Раздел 2. Основные методы и средства обнаружения технических каналов утечки информации

Тема 10. Методы и средства выявления каналов утечки акустической речевой информации.

Основные вопросы

1. Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.
2. Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам акустоэлектрических преобразований
3. Предъявляемые требования к измерительной аппаратуре.
4. Предъявляемые требования к средствам активной акустической и вибрационной защиты.

Рекомендации по изучению темы:

Вопрос 1 изложен в документе [4].

Вопрос 2 изложен в документе [5].

Вопрос 3 изложен в:

«Перечне контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.02.2012г. № 79», утвержденным директором ФСТЭК России 19.04.2017

<https://fstec.ru/normotvorcheskaya/litsenzirovanie/76-inye/438-perechen-utverzhdn-direktorom-fstek-rossii-3-aprelya-2012-g>

«Перечне контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.03.2012г. № 171», утвержденным директором ФСТЭК России 06.2018

<https://fstec.ru/normotvorcheskaya/litsenzirovanie/76-inye/1383-perechen-utverzhdn-direktorom-fstek-rossii-29-avgusta-2017-g>

Для самостоятельного изучения вопроса 4 следует обратиться к интернет ресурсам:

- <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>

- <http://npoanna.ru>

- <http://www.pps.ru>

- <http://kb-elaks.ru/vual.php>

- <https://suritel.ru>
- <http://tehzi.ru/musson.html>
- <http://shoroh5.ru/>
- <http://forso.ru>
- <https://nelk.ru>
- <http://www.infopro.ru/>
- [https://www.apsecurity.ru/catalog/кедр-a.html](https://www.apsecurity.ru/catalog/keдр-a.html)
- <https://nppgamma.ru/catalog>
- <http://cstbi.ru/>
- <https://www.zaonet.ru/kamerton5.html>

Контрольные вопросы по теме 10:

1. Перечислите основные этапы методик оценки защищенности.
2. Перечислите требования, предъявляемые к аппаратуре измерения.
3. Перечислите основных российских производителей средств защиты информации

Тесты для самостоятельной работы:

1. Что относится к активным способам защиты выделенных помещений:

- а) Использование виброгенераторов на стеклах
- б) Использование акустических излучателей
- в) Двойные двери
- г) Звукоизоляция стен

2. Предъявляемые требования к аппаратуре измерения акустических и вибрационных сигналов:

- а) Чувствительность
- б) Неравномерность амплитудно-частотной характеристики
- в) Погрешность
- г) Точность

3. Что относится к пассивным способам защиты выделенных помещений:

- а) Использование виброгенераторов на стеклах
- б) Двойные двери
- в) Использование акустических излучателей
- г) Звукоизоляция стен

2.11. Раздел 3. Основные мероприятия по выявлению технических каналов утечки информации

Тема 11. Организация специальных обследований помещений и специальных проверок технических средств.

Основные вопросы

1. Порядок проведения специальной проверки технических средств.
2. Алгоритм проведения специального обследования помещения.
3. Документальное оформление результатов работ.

Рекомендации по изучению темы:

Для самостоятельного изучения вопросов 1-3 следует обратиться к интернет ресурсам:

- <https://allrefrs.ru/1-37950.html>
- <https://studfile.net/preview/7005592/page:59/>
- <https://infopedia.su/17x8d60.html>
-

https://nelk.ru/catalog/osnashchenie_uchebnykh_laboratoriy_tekhnicheskoy_zashchity_informatsii/laboratoriya_spetsialnykh_proverok_tekhnicheskikh_sredstv_i_spetsialnogo_obsledovaniya_pomeshcheniy/

Контрольные вопросы по теме 11:

1. Перечислите основные этапы специальных проверок технических средств.
2. Перечислите основные этапы специального обследования помещения.

Тесты для самостоятельной работы:

1. Выставить этапы проведение специальных проверок (СП) в правильной последовательности:

- а) проведение СП
- б) анализ результатов и оформление отчетных документов
- в) разработка программы проведения СП
- г) прием-передача ТС, формирование исходных данных

2. Выставить этапы проведение специальных обследований (СО) в правильной последовательности:

- а) инструментальное обследование помещения
- б) обследование ограждающих конструкций помещения, предметов интерьера и ТС
- в) анализ результатов и оформление отчетных документов
- г) обследование здания и прилегающих территорий

3. Основной метод при проведении СП и СО:

- а) радиомониторинг

- б) нелинейная локация
- в) визуальный
- г) ВЧ-облучение и ВЧ-навязывание

2.12. Раздел 3. Основные мероприятия по выявлению технических каналов утечки информации

Тема 12. Организация специальных исследований технических средств и помещений.

Основные вопросы

1. Порядок проведения специальных исследований средств вычислительной техники.
2. Алгоритм проведения специальных исследований помещений.
3. Документальное оформление результатов работ.

Рекомендации по изучению темы:

Вопросы 1 и 3 изложен в документах [2,3].

Вопрос 2 и 3 изложен в документах [4,5].

Контрольные вопросы по теме 12:

1. Перечислите основные этапы специальных исследований средств вычислительной техники.
2. Перечислите основные этапы специальных исследований помещений.

Тесты для самостоятельной работы:

1. Выставить этапы проведение специальных исследований средств вычислительной техники в правильной последовательности:

- а) инструментальные измерения
- б) определение перечня используемых интерфейсов
- в) прием-передача ТС, формирование исходных данных
- г) расчёты и оформление отчетных документов

2. Выставить этапы проведение специальных исследований помещений в правильной последовательности:

- а) инструментальное измерения
- б) обследование ограждающих конструкций помещения
- в) расчёты и оформление отчетных документов
- г) обследование территории, прилегающей к помещению

3. Основной метод при проведении специальных исследований:

- а) радиомониторинг
- б) нелинейная локация
- в) инструментальный
- г) Высокочастотное облучение и высокочастотное навязывание