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 «ПРОФЕССИОНАЛЬНЫЙ ЭЛЕКТИВ. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ»

Для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения

Ульяновск, 2022

Методические указания для самостоятельной работы студентов по дисциплине «Профессиональный электив. Организационно-правовые основы технической защиты конфиденциальной информации» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2022. 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, курсовым работам и к зачёту по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол №3/22 от 19.04.2022 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991205252.html.

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

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 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/

3.2 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/

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

3.4. Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации". Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

3.5 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

3.6 Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

3.7 Приказ ФСТЭК № 21 от 18 февраля 2013 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.8 Методический документ ФСТЭК «Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн».

3.9Постановление Правительства РФ от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

3.10 Постановление Правительства РФ от 26 июня 1995 г. N 608 «О сертификации средств защиты информации».

3.11 Положение о системе сертификации средств защиты информации (Приказ ФСТЭК от 03.04.2018 № 55).

3.12 Положение о сертификации СЗИ по требованиям безопасности информации (Приказ Председателя Гостехкомиссии № 199).

4. ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

5. Основы информационной безопасности. Курс лекций. Часть 1 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 63 с.

6. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск: УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). URL: http://edu.ulsu.ru/cources/750/interface/.

7. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»; ИНФРА-М, 2014. – 416 с. ил.

8. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. - 392с.

9. Дронов В.Ю., Международные и отечественные стандарты по информационной безопасности [Электронный ресурс]: Дронов В.Ю. - Новосибирск: Изд-во НГТУ, 2016. - 34 с. - ISBN 978-5-7782-3112-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778231122.html.

10. Домарев В.В. Безопасность информационных технологий. Системный подход: К.: ООО «ТИД «ДС», 2004. – 992 с.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ЦЕЛИ И ЗАДАЧИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ТЕМА 1. ВВЕДЕНИЕ В ДИСЦИПЛИНУ. МЕСТО ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Основные вопросы:

1. Информация как объект защиты. Основные термины и определения в области ТЗИ.
2. Цели и задачи ТЗКИ. Перечень сведений конфиденциального характера, подлежащих защите

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] на с. 9-15, в учебном пособии [8] на с. 8-13.

Для самостоятельного изучения вопроса 1 следует обратиться к [1] на с. 3-10 и к [3.1-3.2].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к [8] на с. 62-71.

Контрольные вопросы по теме 1:

1. Перечислить основные объекты обеспечения информационной безопасности Российской Федерации
2. Перечислить основные субъекты обеспечения информационной безопасности Российской Федерации
3. Что входит в государственную систему защиты информации Российской Федерации?
4. Охарактеризовать основные предметные области информационной сферы
5. Охарактеризовать понятие «информация»
6. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации
7. Цели и задачи ТЗКИ
8. Перечень сведений конфиденциального характера, подлежащих защите

Тесты для самостоятельной работы:

1. В каком нормативно-правовом акте, из перечисленных, даётся трактовка понятия «информация»?

а) Конституции РФ

б) № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

в) № 152-ФЗ «О персональных данных»

г) Закон РФ N 5485-1 «О государственной тайне»

д) № 98-ФЗ "О коммерческой тайне"

2. Какой документ определяет национальные интересы РФ в информационной сфере?

а) Доктрина информационной безопасности

б) Конституция РФ

в) № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

г) Закон РФ N 5485-1 «О государственной тайне»

3. В каком документе содержатся правовые основы защиты служебной тайны?

а) Постановление Правительства РФ от 3 ноября 1994г. № 1233

б) Конституция РФ

в) Закон РФ N 5485-1 «О государственной тайне»

4. 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»

2.2. РАЗДЕЛ 1. ЦЕЛИ И ЗАДАЧИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ТЕМА 2. УГРОЗЫ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Основные вопросы:

1. Проблемы обеспечения информационной безопасности
2. Потенциальные угрозы информации
3. Классификация угроз и каналов утечки информации
4. Неформальная модель нарушителя

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [5] на с. 20-21.
Для самостоятельного изучения вопроса 1 следует обратиться к [3.1-3.2]
Вопрос 2 изложен в учебном пособии [5] на с. 21-23.
Вопрос 3 изложен в учебном пособии [5] на с. 22-26.
Вопрос 4 изложен в учебном пособии [5] на с. 26-29.
Для самостоятельного изучения вопроса 2 следует обратиться к [3.1- 3.2].

Контрольные вопросы по теме 2

1. Характеристика проблем обеспечения информационной безопасности.
2. Основные условия решения острых проблем в области ИБ.
3. Угрозы безопасности информации. Привести примеры характерных угроз.
4. Пояснить на примерах основные свойства информации при ее обработке техническими средствами: конфиденциальность, целостность и доступность.
5. Какие факторы опасности (причины возникновения угроз) Вы знаете?
6. Пояснить классификацию естественных и искусственных угроз.
7. Привести 5 примеров основных непреднамеренных искусственных угроз.
8. Привести 5 примеров основных преднамеренных искусственных угроз.
9. Назвать основные потенциальные каналы доступа к информации.
10. Назвать основные потенциальные каналы утечки информации.
11. Дать характеристику неформальной модели нарушителя.
12. Раскрыть основное предназначение неформальной модели нарушителя. Дать примеры внешних и внутренних нарушителей.

Тесты для самостоятельной работы:

1. Что, из нижеперечисленного, является угрозой целостности информации?

а) Незаконное уничтожение или модификация информации
б) Утрата контроля над системой защиты;
в) Каналы утечки информации

2. Основной непреднамеренной искусственной угрозой не является:
а) Неправомерное отключение оборудования или изменение режимов работы устройств и программ
б) Отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.)
в) Неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной
г) Неумышленная порча носителей информации

3. **Что, из перечисленного, не относится к основным преднамеренные искусственным угрозам?**
а) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи
б) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др.)
в) применение подслушивающих устройств, дистанционная фото и видеосъемка
г) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность)

4. Что, из перечисленного, следует к внешним факторам возникновения угрозы информационной безопасности?
а) уровень развития информационной инфраструктуры
б) глобальный процесс информатизации
в) нормативно-правовое регулирование информационной сферы

5. Что, из нижеперечисленного, является угрозой целостности информации?
а) Незаконное уничтожение или модификация информации
б) Утрата контроля над системой защиты;
в) Каналы утечки информации

2.3. РАЗДЕЛ 1. ЦЕЛИ И ЗАДАЧИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ТЕМА 3. МЕТОДЫ ВЫЯВЛЕНИЯ И ОЦЕНКИ ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

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
4. Методы пассивной и активной защиты от утечки в акустическом (виброакустическом) канале

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 339-360, 686-690.

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

Вопрос 3 изложен в учебном пособии [2] на с. 266-273.

Вопрос 4 изложен в учебном пособии [2] на с. 323-339.

Контрольные вопросы по теме 3:

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.
8. Основные методы пассивной и активной защиты речевой информации.
9. Основные цели пассивных методов защиты речевой информации.
10. Основные цели активных методов защиты речевой информации.
11. Каким образом может осуществляться звукоизоляция помещений?

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

5. 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

6. На что направленны активные методы защиты акустической информации?

а) Ослабление акустических (речевых) сигналов

б) Ослабление информационных электрических сигналов

2.4. РАЗДЕЛ 2. ОСНОВЫ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ТЗКИ

ТЕМА 4. СИСТЕМА СТАНДАРТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Основные вопросы:

1. Роль стандартов информационной безопасности
2. Международные стандарты информационной безопасности
3. Отечественные стандарты безопасности информационных технологий

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] на с. 76-78.
Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [9] на с. 3-5.
Вопрос 2 изложен в учебном пособии [10] на с. 78-88.
Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [9] на с. 10-26.
Вопрос 3 изложен в учебном пособии [10] на с. 92-97.
Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [9] на с. 27-29.

Контрольные вопросы по теме 4:

1. В чём заключается главная задача стандартов ИБ
2. Какие уровни безопасности были определены в оранжевой книге Министерства обороны США?
3. Какие задачи предполагает обеспечение ИБ в любой компании?
4. Какие основные стандарты рассматривают актуальные вопросы обеспечения ИБ организаций и предприятий?
5. Особенности Германского стандарта BSI
6. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»
7. Стандарты для беспроводных сетей
8. Стандарты информационной безопасности в сети Интернет
9. Отечественные стандарты безопасности информационных технологий

Тесты для самостоятельной работы:

1. Сколько уровней безопасности содержится в "Оранжевой книге"?

а) 4
б) 3
в) 8
г) 6
д) 9

2. Стандарт ISO 15408 рассматривает информационную безопасность как:

а) обеспечение конфиденциальности информации
б) совокупность конфиденциальности и целостности информации
в) совокупность конфиденциальности и доступности информации
г) совокупность доступности и целостности информации

3. Какой стандарт определяет протоколы, необходимые для организации беспроводных локальных сетей?

а) SSL
б) IEEE 802.11
в) SET
г) ISO 5408

4. Какой стандарт, из перечисленных, в настоящий момент отменён?

а) ГОСТ Р ИСО/МЭК 17799-06
б) ГОСТ Р ИСО/МЭК 27002-2012
в) ГОСТ Р 34.11-2012

2.5. РАЗДЕЛ 2. ОСНОВЫ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ТЗКИ

ТЕМА 5. ОСНОВЫ ЛИЦЕНЗИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПО ТЗКИ. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Основные вопросы:

1. Основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации
2. Виды деятельности, подлежащие лицензированию, и порядок получения лицензий
3. Лицензирование деятельности по технической защите конфиденциальной информации

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим законам, стандартам и Постановлениям Правительства [3.3, 3.9-3.11].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к соответствующим законам, стандартам и Постановлениям Правительства [3.3, 3.9].

Вопрос 3 изложен в лекции.

Для самостоятельного изучения вопроса 3 следует обратиться к соответствующим законам, стандартам и Постановлениям Правительства [3.3, 3.10].

Контрольные вопросы по теме 5:

1. Дать определения лицензирования в области защиты информации
2. Для чего выдаётся лицензия
3. Порядок сертификации средств защиты информации
4. Перечислить лицензировнные виды деятельности
5. Основные документы для лицензирования и сертификации
6. Порядок получения лицензии
7. Лицензирование деятельности по технической защите конфиденциальной информации

Тесты для самостоятельной работы:

1. Какие органы, из перечисленных, уполномочены на ведение лицензионной деятельности? Отметить 2 позиции.

а) ФСТЭК
б) СВР РФ
в) МВК
г) ФСБ РФ

2. Организация подает документы на получение лицензии. В течение какого времени орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии?

а) В течение 7 дней
б) В течение 30 дней
в) В течение 15 дней

3. В течение какого времени организация должна подать заявление о переоформлении лицензии, если изменились условия ведения лицензируемого вида деятельности?

а) В течение 7 дней
б) В течение 30 дней
в) В течение 15 дней

4. Какая организация занимается лицензированием деятельности по ТЗИ конфиденциальной информации?

а) ФСТЭК
б) МВК
в) ФСБ

2.6. РАЗДЕЛ 2. ОСНОВЫ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ТЗКИ

ТЕМА 6. СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ. ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Основные вопросы:

1. Сертификация средств защиты информации
2. Назначение сертификации по требованиям защиты информации.
3. Законодательно-правовые основы сертификации.
4. Обязательность сертификации.

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим законам, стандартам и Постановлениям Правительства [3.3, 3.5].

Вопрос 2 изложен в [3.10-3.11].

Вопрос 3 изложен в [3.11].

Вопрос 4 изложен в [3.11-3.12].

Контрольные вопросы по теме 6:

1. Дать определения сертификации в области защиты информации
2. Порядок сертификации средств защиты информации
3. Сертификация средств защиты информации
4. Основные виды сертификации.
5. Основные системы сертификации по требованиям безопасности информации.
6. Основные нормативные документы по сертификации.
7. Для кого сертификация является обязательной?
8. Ответственность разработчиков средств защиты информации ограниченного распространения.

Тесты для самостоятельной работы:

1. На кого возлагается организация сертификации средств ЗИ? Выбрать 3 позиции.

а) ФСТЭК
б) МВК по ЗГТ
в) ФСБ
г) Аттестационная комиссия
д) МО РФ

2. Какая организация занимается координацией работ по организации сертификации?
а) ФСТЭК
б) МВК по ЗГТ
в) ФСБ

3. Что относится к деятельности изготовителей СЗИ?
а) Приостановление действий выданных сертификатов
б) Принятие решения о повторной сертификации при изменении технологии изготовления изделия
в) Маркировка сертифицированного изделия знаком соответствия

2.7. РАЗДЕЛ 2. ОСНОВЫ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ТЗКИ

ТЕМА 7. ТРЕБОВАНИЯ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ (ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ, ОТ НСД И СПЕЦИАЛЬНЫХ ВОЗДЕЙСТВИЙ

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 [2] на с. 686-690.

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

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

Вопрос 3 изложен в учебном пособии [2] на с. 690-696.

Вопрос 4 изложен в учебном пособии [2] на с. 654-658.

Контрольные вопросы по теме 7:

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

2.8. РАЗДЕЛ 2. ОСНОВЫ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ТЗКИ

ТЕМА 8. ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ВОПРОСАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основные вопросы:

1. Первоочередные мероприятия по созданию системы защиты персональных данных на предприятии (7 шагов).
2. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных.

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [6] на с. 3-11 и к [3.5].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [6] на с. 30-38 и к [3.6-3.8].

Контрольные вопросы по теме 8:

1. Перечислить основные мероприятия по созданию системы защиты персональных данных на предприятии

2. Что включено в отчёт об обследовании информационных систем персональных данных организации?

3. Разработка и применение документов под названиями: «Согласие на обработку персональных данных» и «Отзыв согласия на обработку ПДн»

4. Перечислить основные технические средства защиты персональных данных

5. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных

6. Что включается в акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных «наименование ИСПДн»?

7. Модель угроз безопасности ПДн при их обработке в ИСПДн

8. Что содержит технический паспорт ИСПДн?

9. Что включается в руководство пользователю ИСПДн?

10. «Уведомления об обработке ПДн»

Тесты для самостоятельной работы:

1. На какие документы, из перечисленных, следует опираться при создании системы защиты ПДн на предприятии? Выбрать 2 позиции.

а) № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

б) ПП РФ N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
в) Конституция РФ
г) N 152-ФЗ «О персональных данных»

2. Какой организации следует отправлять Уведомление о намерении осуществлять обработку ПДн, если организация является оператором по обработке ПДн?
а) Роскомнадзор
б) ФСТЭК
в) Налоговая служба
г) ФСБ

1.9. РАЗДЕЛ 2. ОСНОВЫ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ТЗКИ

ТЕМА 9. ТРЕБОВАНИЯ МЕЖДУНАРОДНЫХ И НАЦИОНАЛЬНЫХ СТАНДАРТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Основные вопросы:
1. Роль стандартов информационной безопасности
2. Международные стандарты информационной безопасности

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [7] на с. 76-78.
Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [9] на с. 3-5.
Вопрос 2 изложен в учебном пособии [10] на с. 78-88.
Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [9] на с. 10-26.
Вопрос 3 изложен в учебном пособии [10] на с. 92-97.
Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [9] на с. 27-29.

Контрольные вопросы по теме 9:
1. В чём заключается главная задача стандартов ИБ
2. Какие уровни безопасности были определены в оранжевой книге Министерства обороны США?
3. Особенности Германского стандарта BSI
4. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»
5. Стандарты для беспроводных сетей
6. Стандарты информационной безопасности в сети Интернет

Тесты для самостоятельной работы:

1. Сколько уровней безопасности содержится в "Оранжевой книге"?

а) 4
б) 3
в) 8
г) 6
д) 9

2. Какой стандарт определяет протоколы, необходимые для организации беспроводных локальных сетей?

а) SSL
б) IEEE 802.11
в) SET
г) ISO 5408