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 «РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ»

Для студентов специалитета по специальности 10.05.03 очной формы обучения

Ульяновск, 2021

Методические указания для самостоятельной работы студентов по дисциплине «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2021. Настоящие методические указания предназначены для студентов специалитета по специальности 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 № 2/21 от 16 марта 2021 г.).

Содержание

1. Литература для изучения дисциплины…….…….....…….. 4
2. Методические указания ……..…….....…6
2.1. Раздел 1. Понятия и сущность защищённых автоматизированных систем (АС). Тема 1. Основные понятия и классификация защищенных автоматизированных систем ….……..…….…....6
2.2. Раздел 1. Тема 2. Основы защиты информации в защищенных автоматизированных системах …….……...……..7
2.3. Раздел 1. Тема 3. Угрозы безопасности информации в защищенных автоматизированных системах..…..……...…….…8
2.4. Раздел 1. Тема 4. Программно-технический уровень защиты автоматизированных систем ……..……10
2.5. Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем. Тема 5. Основы организации разработки защищенных АС ……..……..11
2.6. Раздел 2. Тема 6. Общие принципы проектирования защищенных АС ...12
2.7. Раздел 2. Тема 7. Основы эксплуатации защищенных АС …..……..13
2.8. Раздел 2. Тема 8. Криптографические протоколы обеспечения безопасности ……..……..…….16
2.9. Раздел 2. Тема 9. Основы администрирования АС ….……...17

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

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

2. Новиков В.К., Информационное оружие - оружие современных и будущих войн [Электронный ресурс] / Новиков В.К. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2013. - 262 с. - ISBN 978-5-9912-0166-7 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201667.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/

4. Малюк А.А., Введение в информационную безопасность [Электронный ресурс]: Учебное пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.. Под ред. В.С. Горбатова. - М.: Горячая линия - Телеком, 2011. - 288 с. - ISBN 978-5-9912-0160-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201605.html.

5. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск: УлГУ, 2016. URL: http://edu.ulsu.ru/cources/750/interface/.

6. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ - Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

7. Мартемьянов, Ю. Ф. Операционные системы. Концепции построения и обеспечения безопасности: учебное пособие для вузов / Мартемьянов Ю. Ф. , Яковлев Ал. В., Яковлев Ан. В. - Москва: Горячая линия - Телеком, 2010. - 332 с. - ISBN 978-5-9912-0128-5. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785991201285.html

8. Шаньгин, В. Ф. Информационная безопасность и защита информации / Шаньгин В. Ф. - Москва : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Текст: электронный // ЭБС "Консультант студента" : [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785940747680.html

9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2014. — 944 с.

10. Бирюков А.А. Информационная безопасность: защита и нападение / Бирюков А. А. - Москва: ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785970604359.html

11. «Положение по аттестации объектов информатизации по требованиям безопасности информации»

12. Национальный стандарт ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»

13. Национальный стандарт ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

14. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев - Москва : Издательство МГТУ им. Н. Э. Баумана, 2018. - 250 с. - ISBN 978-5-7038-4899-9. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785703848999.html

15. Милёхина, О. В. Информационные системы: теоретические предпосылки к построению: учеб. пособие / Милёхина О. В. - Новосибирск: Изд-во НГТУ, 2013. - 282 с. - ISBN 978-5-7782-2220-5. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785778222205.html

16. Беленькая, М. Н. Администрирование в информационных системах: учебное пособие для вузов / Беленькая М. Н., Малиновский С. Т. , Яковенко Н. В. - Москва: Горячая линия - Телеком, 2011. - 400 с. - ISBN 978-5-9912-0164-3. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785991201643.html

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

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ПОНЯТИЯ И СУЩНОСТЬ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 1. ОСНОВНЫЕ ПОНЯТИЯ И КЛАССИФИКАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Основные вопросы:

1. Классификация автоматизированных систем
2. Основные угрозы безопасности информации в автоматизированных системах

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [14] на с. 4-14.

Для самостоятельного изучения вопроса 1 следует обратиться к [3.1- 3.3] и к учебному пособию [15] на с. 100-112.

Вопрос 2 изложен в учебном пособии [8] на с. 22-70.

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [1] на стр. 23-40 и к учебному пособию [14] на с. 20-32.

Контрольные вопросы по теме 1:

1. Актуальность защиты АС
2. Защита АС как процесс управления рисками
3. Классификация АС
4. Жизненный цикл АС
5. Основные понятия информационной безопасности и защиты информации в автоматизированной системе (АС)
6. Доступность, целостность и конфиденциальность
7. Основные правила разграничения доступа к ресурсам
8. Охарактеризовать понятие «Объект информатизации»
9. Атака на АС
10. Что такое эффективность защиты информации?
11. Понятие НСД
12. Основные угрозы АС. Классификация угроз и противодействие им
13. Фишинг и защита от него
14. Фарминг и защита от него
15. Ботненты

Тесты для самостоятельной работы:

1. Выберите 3 правильных метода защиты от типовой атаки на интрасети «Анализ сетевого трафика»

а) Использование системы Kerberos

б) Установка средств для мониторинга всех процессов в сети

в) выявление разрушающих воздействий в BIOS (ПЗУ)

г) Сегментация сетей

2. С помощью установки какого защитного средства осуществляется разделение интрасети на сегменты?
а) Система обнаружения/предотвращения вторжений втор-жений
б) Межсетевой экран
в) Сетевая операционная система
г) Браузер

2.2. РАЗДЕЛ 1. ПОНЯТИЯ И СУЩНОСТЬ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 2. ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Основные вопросы:

1. Базовые понятия и определения информационной безопасности
2. Основные принципы организации защиты информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 6-11.

Для самостоятельного изучения вопроса 1 следует обратиться к [3.1-3.3].

Вопрос 2 изложен в учебном пособии [1] на с. 12-15.

Для самостоятельного изучения вопроса 2 следует обратиться к [2] на стр. 25-34, к учебному пособию [14] на с. 33-38, к учебному пособию [17] на с. 109-113.

Контрольные вопросы по теме 2:

1. Основные составляющие информационной безопасности (ИБ).
2. Перечень оснований для ограничения информационных прав.
3. Раскрыть понятие ИБ.
4. Перечень видов информации с ограниченным доступом.
5. Предметы рассмотрения дисциплины.
6. Основные базовые свойства защищаемой информации.
7. Основные цели защиты информации (ЗИ).
8. Основная терминология по ИБ и ЗИ.
9. Основные принципы организации ЗИ.

Тесты для самостоятельной работы:

1. Коммерческую тайну не могут составлять следующие виды информации:
а) Техническая
б) информация о спросе и предложении,
в) информация о состоянии окружающей среды
информация о конкурентах

2. К внешним субъектам, способствующим обеспечению информационной безопасности, относятся

а) конкуренты
б) функциональные и отраслевые министерства и ведомства
в) сотрудники специализированных организаций, оказывающих услуги по договору;
г) служба внутреннего аудита в целом и ее сотрудники и т.д.

2.3. РАЗДЕЛ 1. ПОНЯТИЯ И СУЩНОСТЬ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 3. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Основные вопросы:

1. Угрозы информационной безопасности и их проявления
2. Классификация источников угроз информационной безопасности
3. Модель действий нарушителя

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 21-23.

Для самостоятельного изучения вопроса 1 следует обратиться к [17] на с. 94-100.

Вопрос 2 изложен в учебном пособии [1] на с. 22-26.

Вопрос 3 изложен в учебном пособии [4] на с. 26-29.

Для самостоятельного изучения вопроса 3 следует обратиться к [3.1-3.3].

Контрольные вопросы по теме 3:

1. Раскрыть понятия угрозы, уязвимостей и последствий реализации угроз.

2. Назвать 3 примера уязвимостей информационной системы.

3. Привести вариант классификации источников угроз информационной безопасности.

4. Назвать 3 примера техногенных источников угроз.

5. Привести 3 примера актуальных стихийных источников угроз.

6. Назвать 3 примера антропогенных источников угроз.

7. Пояснить необходимость разработки модели действий нарушителя.

8. Внутренние и внешние нарушители.

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)
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. Источниками угроз информационной безопасности не являются:
а) социальные источники
б) антропогенные источники
в) техногенные источники
г) стихийные источники

5. Что, из нижеперечисленного, относится к объективным уязвимостям?
а) Аппаратные закладки
б) Ошибки при эксплуатации технических средств
в) Нарушение режима конфиденциальности
г) Сбои электроснабжения
д) Повреждения жизнеобеспечивающих коммуникаций

6. Что, из нижеперечисленного, относится к субъективным уязвимостям?
а) Сбои электроснабжения
б) Повреждения жизнеобеспечивающих коммуникаций
в) Ошибки при эксплуатации технических средств
г) Аппаратные закладки
д) Нарушение режима конфиденциальности

2.4. РАЗДЕЛ 1. ПОНЯТИЯ И СУЩНОСТЬ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 4. ПРОГРАММНО-ТЕХНИЧЕСКИЙ УРОВЕНЬ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Основные вопросы:

1. Политика информационной безопасности
2. План защиты
3. План обеспечения непрерывной работы и восстановления работоспособности

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [5] на с. 40-48.

Для самостоятельного изучения вопроса 1 следует обратиться к [6] на с. 5-6 и [7] на с. 233-238.

Вопрос 2 изложен в учебном пособии [17] на с. 233-235.

Вопрос 3 изложен в лекции и в учебном пособии [5] на с. 54-63.

Для самостоятельного изучения вопроса 3 следует обратиться к [6] на с. 22-28.

Контрольные вопросы по теме 4:

1. Основные разделы политики информационной безопасности (ПИБ) предприятия
2. Привести примеры типовых целей ПИБ
3. Варианты стратегий ответных действий на нарушение безопасности
4. Уровни ответственности пользователей и администраторов
5. Дать характеристику плану защиты (ПЗ)
6. Основные разделы ПЗ
7. Предназначение Плана обеспечения непрерывной работы и восстановления работоспособности
8. Дать характеристику основных мер реагирования на нарушения безопасности
9. Перечислить основные восстановительные работы

Тесты для самостоятельной работы:

1. Политика информационной безопасности (ПИБ) - это:

а) Совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса

б) Совокупность документированных технических решений, направленных на обеспечение безопасности информационного ресурса

в) Совокупность документированных процедурных решений, направленных на обеспечение безопасности инф. ресурса

2. Какая стратегия ответных действий на нарушение безопасности наиболее характерна для правоохранительных органов?
а) «Выследить и осудить»
б) «Защититься и продолжить»
в) «Выследить и отпустить после проведения профилактической работы»

3. Какие частные политики являются обязательными в типовой организации? Выбрать 3 варианта
а) Организации режима секретности
б) Использования Интернета
в) Разработки и лицензирования ПО
г) Обращения с информацией ограниченного доступа
д) Транспортировки носителей информации
е) Резервировании информации
ж) Проведения внешних и внутренних аудитов ИБ

4. Какие наиболее характерные угрозы ИС предприятия учитываются при составлении плана защиты? Выбрать 3 варианта
а) Точки доступа
б) Нелицензированные программные средства
в) Неправильно сконфигурированные системы
г) Отсутствие достаточных средств на счетах предприятия
д) Внутренние враги

5. В каком документе, из перечисленных, описывается схема оповещения конкретных лиц об инцидентах ИБ?
а) Политика информационной безопасности
б) План обеспечения непрерывной работы и восстановления работоспособности
в) План защиты

2.5. РАЗДЕЛ 2. ОБЩИЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ И РАЗРАБОТКИ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 5. ОСНОВЫ ОРГАНИЗАЦИИ РАЗРАБОТКИ ЗАЩИЩЕННЫХ АС

Основные вопросы:
1. Типовые модели разработки АС
2. Основные этапы проектирования и разработки АС
3. Современные методологии проектирования АС

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [15] на с. 103-112.
Вопрос 2 изложен в учебном пособии [15] на с. 100-102.

Для самостоятельного изучения вопроса 2 следует обратиться к [14] на с. 33-39 и к учебному пособию [17] на с. 730-744.

Вопрос 3 изложен в учебном пособии [15] на с. 131-159.

Контрольные вопросы по теме 5:

1. Этапы разработки, эксплуатации и сопровождения АС
2. Каскадная модель разработки АС
3. Итерационная модель разработки АС
4. Спиральная модель разработки АС
5. Информационные потоки АС
6. Основные технологии проектирования АС
7. CASE-технологии
8. CASE-средства
9. Функциональные (IDEFO) и информационные (IDEF1X) модели
10. Методология DFD
11. Методы и средства обеспечения отказоустойчивости автоматизированных систем
12. Критерии оценки защищенности АС
13. Методы обеспечения информационной безопасности АС
14. Организация коллективной разработки программного обеспечения АС

Тесты для самостоятельной работы:

1. Какая, из перечисленных моделей разработки АС, позволяет переходить на следующий этап проектирования, не завершив полностью работы на текущем этапе?

а) Каскадная модель разработки АС
б) Итерационная модель разработки АС
в) Спиральная модель разработки АС

2.6. РАЗДЕЛ 2. ОБЩИЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ И РАЗРАБОТКИ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 6. ОБЩИЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ АС

Основные вопросы:

1. Меры и основные принципы обеспечения безопасности в ходе проектирования АС

2. Основы ведения конструкторской документации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [14] на с. 33-50.

Для самостоятельного изучения вопроса 1 следует обратиться к [15] на с. 135-150.

Вопрос 2 изложен в учебном пособии [14] на с. 121-127.

Для самостоятельного изучения вопроса 2 следует обратиться к [17] на с. 700-702.

Контрольные вопросы по теме 6:

1. Меры противодействия угрозам безопасности
2. Достоинства и недостатки различных видов мер защиты
3. Принципы обеспечения безопасности
4. Содержание этапов проектирования
5. Основы ведения конструкторской документации
6. Структура и содержание технического задания
7. Построение комплексной защиты АС
8. Основы проектирования комплексной защиты информационной безопасности от НСД
9. Средства обеспечения надежности защищенных АС
10. Организация хранения информации в защищенных АС

Тесты для самостоятельной работы:

1. 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

2.7. РАЗДЕЛ 2. ОБЩИЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ И РАЗРАБОТКИ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 7. ОСНОВЫ ЭКСПЛУАТАЦИИ ЗАЩИЩЕННЫХ АС

Основные вопросы:

1. Общие положения аттестации объектов информатизации.
2. Основные этапы создания и ввода в эксплуатацию объектов информатизации.

Рекомендации по изучению темы:

Для изучения вопроса 1 следует обратиться к [11,12].

Для самостоятельного изучения вопроса [1] следует обратиться к [13]. а также к соответствующим разделам документов

Для изучения вопроса 2 следует обратиться к [17] на с. 738-744.

Контрольные вопросы по теме 7:

1. Назовите основные положения в области аттестации объектов информатизации
2. Перечислите основные этапы создания объектов информатизации

(информационных систем, автоматизированных систем управления, значимых объектов критической информационной инфраструктуры)

3. Перечислите основные документы на объекты информатизации (информационные системы, автоматизированные системы управления, значимые объекты критической информационной инфраструктуры).

4. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС

5. Порядок обеспечения защиты информации при эксплуатации АС

6. Аппаратно-программные средства диагностики АС

7. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков

Тесты для самостоятельной работы:

1. Назвать основные организации, составляющие систему аттестации объектов информатизации:

а) ФСТЭК России

б) органы по аттестации

в) головное подразделение отрасли по защите информации

г) владельцы объектов информатизации

д) представитель заказчика

2. Какой их перечисленных видов работ не относится к аттестации объектов информатизации?

а) анализ исходных данных и предварительное ознакомление

б) обследования объекта информатизации и анализ разработанной документации по защите информации

в) поставка, монтаж и настройка средств защиты информации

г) проведение комплексных аттестационных испытаний объекта информатизации

д) утверждение заключения по результатам аттестации

3. Кто оплачивает расходы по проведению всех работ и услуг по обязательной аттестации объектов информатизации?

а) заявители

б) вышестоящие организации, в подчинении которых находятся аттестуемые организации

в) органы государственного управления, на территории которого находятся аттестуемые организации

4. В какой срок орган по аттестации обязан рассмотреть заявку на проведение аттестации?

а) 15 дней

б) 2 недели

в) 1 месяц

5. Расставить в правильном порядке проверки при аттестационных испытаниях автоматизированной системы

а) Проверка уровня подготовки специалистов и распределения ответственности должностных лиц

б) Проверка правильности категорирования

в) Проверка достаточности представленных документов и соответствия их содержания

г) Проверка наличия сертификатов соответствия требованиям безопасности информации

д) Проверка соответствия состава и структуры программно-технических средств автоматизированной системы

е) Проверка правильности классификации

6. Расставить в правильном порядке проверки при аттестационных испытаниях автоматизированной системы на соответствие требованиям по защите информации от утечки по техническим каналам

а) Экспертиза протоколов измерения и предписаний на эксплуатацию

б) Проверка выполнений требований к электропитанию и заземления

в) Проверка средств защиты информации

г) Проверка взаимного размещения технических средств

д) Проверка соответствия фактических размеров контролируемой зоны

е) Проверка соответствия размеров контролируемой зоны требованиям предписаний на эксплуатацию

7. Расставить в правильном порядке проверки при аттестационных испытаниях автоматизированной системы на соответствие требованиям по защите информации от несанкционированного доступа

а) Проверка подсистемы обеспечения целостности

б) Проверка подсистемы управления доступом

в) Проверка соответствия описания технологического процесса обработки, хранения и передачи защищаемой информации реальному технологическому процессу обработки

г) Проверка подсистемы регистрации и учета

8. В течение какого времени действует аттестат соответствия на автоматизированную систему?

а) 5 лет

б) 3 года

в) бессрочно

9. 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

10. 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

11. Предъявляемые требования к аппаратуре измерения побочных электромагнитных излучений

а) Диапазон частот

б) Чувствительность

в) Погрешность

г) Класс точности

2.8. РАЗДЕЛ 2. ОБЩИЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ И РАЗРАБОТКИ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 8. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основные вопросы:

1. Протоколы аутентификации на прикладном и транспортном уровнях
2. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [8] на с. 293-307.

Для самостоятельного изучения вопроса 2 следует обратиться к [9] на с. 860-869.

Вопрос 2 изложен в учебном пособии [10] на с. 368-390.

Контрольные вопросы по теме 5:

1. Протоколы аутентификации на прикладном уровне
2. Протокол Kerberos
3. Протоколы аутентификации на транспортном уровне
4. Протокол SSL/TLS
5. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI

Тесты для самостоятельной работы:

1. Какой подход обеспечения безопасности открытых систем, из перечисленных, наиболее распространён в VPN?

а) передача ключа через доверенный канал

б) прямой доступ в доверенную базу данных
в) использование криптосистем, основанных на идентификаторах
г) использование криптосистем с неявно сертифицированными открытыми ключами
д) использование метода сертификации открытых ключей

2. Сертификат открытого ключа – это?
а) специальная структура данных, состоящая из поля подписи
б) специальная структура данных, состоящая из полей данных и поля подписи
в) специальная структура данных, состоящая из полей данных

3. Какой из перечисленных стандартов относится к административным протоколам?
а) RFC 2585
б) RFC 2560
в) RFC 2511

4. Как генерируются данные для шифрования трафика?
а) Задаются вручную
б) С помощью специальных алгоритмов и библиотек
в) Берутся из открытой баз

2.9. РАЗДЕЛ 2. ОБЩИЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ И РАЗРАБОТКИ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 9. ОСНОВЫ АДМИНИСТРИРОВАНИЯ АС

Основные вопросы:

1. Сущность администрирования АС
2. Объекты администрирования и модели управления
3. Администрирование обеспечения информационной безопасности

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [16] на с. 8-23.
Вопрос 2 изложен в учебном пособии [16] на с. 24-59.
Вопрос 3 изложен в учебном пособии [16] на с. 250-285.

Контрольные вопросы по теме 9:
1. Что такое администрирование АС?
2. Функционал администратора АС
3. Состав служб администратора АС
4. Требования к администраторам АС
5. Функциональный состав АС
6. Объекты администрирования

7. Модель сетевого управления ISO OSI
8. Модель управления ITIL
9. Администрирование сетевых систем
10. Удаленное администрирование компонентов АС
11. Установка и настройка работы информационных сервисов АС

Тесты для самостоятельной работы:

1. Какая, из перечисленных служб прикладного уровня модели OSI, отвечает за установление соединений между приложениями различных систем?

а) ASCE
б) RTSE
в) RJSE