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 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Основы информационной безопасности» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2019. 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 практическим занятиям и к зачёту по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 2/19 от 19.03.2019 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Основы информационной безопасности. Курс лекций. Часть 1 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2019 – 63 с.

2. Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2019 – 103 с.

3. Защита информации: основы теории: учебник для бакалавриата и магистратуры / Щеглов А. Ю., Щеглов К. А. – М.: Издательство Юрайт, 2019. – 309 с. https://biblio-online.ru/viewer/zaschita-informacii-osnovy-teorii-433715.

4. 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

5. Долозов Н.Л., Программные средства защиты информации: конспект лекций [Электронный ресурс] / Долозов Н.Л. - Новосибирск: Изд-во НГТУ, 2015. - 63 с. - ISBN 978-5-7782-2753-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778227538.html

6. 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.

7. Шелухин О.И., Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов / Под ред. профессора О.И. Шелухина. - М.: Горячая линия - Телеком, 2013. - 220 с. - ISBN 978-5-9912-0323-4 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785991203234.html

8. Расторгуев С.П. Информационная война. - М: Радио и связь, 1999. - 416 с.

9. Некоммерческая интернет-версия СПС "КонсультантПлюс":

9.1 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/

9.2 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/

9.3 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/

9.4 Закон РФ 2010 года N 390-ФЗ «О безопасности» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

9.5 Федеральный закон от 27.07.2006 N152-ФЗ "О персональных данных" Режим доступа:

http://www.consultant.ru/document/cons_doc_LAW_61801/

9.6 Федеральный закон от 29.07.2004 N98-ФЗ "О коммерческой тайне" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

10. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: 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.

11. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:

11.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента;

11.2 ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

12. Андрианов В.В., Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. - 2-е изд., перераб. и доп. - М.: ЦИПСиР, 2011. - 373 с. - ISBN 978-5-9614-1364-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785961413649.html.

13. Туманов С.А., Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" [Электронный ресурс]: / Туманов С.А. - Новосибирск: Изд-во НГТУ, 2016. - 56 с. - ISBN 978-5-7782-2826-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778228269.html.

учебно-методическая

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

15. Лабораторный практикум по математическим методам защиты информации: учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев; УлГУ, ФМИиАТ. - Ульяновск: УлГУ, 2016. 54 с. URL: ftp://10.2.96.134/Text/Amiranov_2016.pdf

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕМА 1. ПОНЯТИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Сущность и содержание национальной безопасности
2. Основные понятия и общеметодологические принципы информационной безопасности

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 6-10.

Для самостоятельного изучения вопроса 1 следует обратиться к [9.1-9.6]

Вопрос 2 изложен в учебном пособии [1] на с. 11-14.

Для самостоятельного изучения вопроса 2 следует обратиться к [9.1-9.3].

Контрольные вопросы по теме 1:

1. В чём заключается сущность национальной безопасности РФ?
2. Какие документы определяют национальную безопасность РФ?
3. Кратко охарактеризовать основные виды национальной безопасности по сферам жизнедеятельности.
4. Пояснить основные общеметодологические принципы ИБ.
5. Перечислить основания для ограничения информационных прав.
6. Назвать примеры информации с ограниченным доступом.

Тесты для самостоятельной работы:

1. Какой из перечисленных документов является действующим?

а) Концепция национальной безопасности РФ

б) Стратегия национальной безопасности РФ до 2020 года

в) Стратегии нац. безопасности РФ

2. Что понимается под информационной безопасностью?

а) Соблюдение Конституции РФ, законодательства РФ

б) Состояние защищенности личности, общества и государства от внутренних и внешних угроз в информационной сфере

в) Программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

3. Что не выступает основным элементом национальной безопасности?

а) Безопасность личности

б) Общественная безопасность

в) Государственная безопасность

г) Безопасность бизнеса

2.2. РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕМА 2. НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ РОССИИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Основные вопросы:

1. Место и роль России в глобальном информационном пространстве
2. Национальные интересы РФ в информационной сфере и их обеспечение

Рекомендации по изучению темы:

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

Для самостоятельного изучения вопроса 1 следует обратиться к [9.1-9.2].

Вопрос 2 изложен в учебном пособии [1] на с. 15-20.

Контрольные вопросы по теме 2:

1. Какова значимость информационного обеспечения для государства?
2. Роль России в глобальном информационном пространстве.
3. Интересы личности, общества и государства в информационной сфере.
4. Составляющие национальных интересов РФ в информационной сфере.
5. Пояснить что такое единое информационное пространство как результат глобальной информатизации общества.
6. Перечислить первоочередные шаги РФ в области ИБ для формирования устойчивости к вызовам информационного пространства.

Тесты для самостоятельной работы:

1. Интересы личности в информационной сфере заключаются:

а) в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность

б) в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России

в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества

2. 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

2.3. РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕМА 3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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 [1] на с. 20-21.

Для самостоятельного изучения вопроса 1 следует обратиться к [9.1-9.2]

Вопрос 2 изложен в учебном пособии [1] на с. 21-23.

Вопрос 3 изложен в учебном пособии [1] на с. 22-26.

Вопрос 4 изложен в учебном пособии [1] на с. 26-29.

Для самостоятельного изучения вопроса 2 следует обратиться к [9.1-9.2].

Контрольные вопросы по теме 3

2. Характеристика проблем обеспечения информационной безопасности.
3. Основные условия решения острых проблем в области ИБ.
4. Угрозы безопасности информации. Привести примеры характерных угроз.
5. Пояснить на примерах основные свойства информации при ее обработке техническими средствами: конфиденциальность, целостность и доступность.
6. Какие факторы опасности (причины возникновения угроз) Вы знаете?
7. Пояснить классификацию естественных и искусственных угроз.
8. Привести 5 примеров основных непреднамеренных искусственных угроз.
9. Привести 5 примеров основных преднамеренных искусственных угроз.
10. Назвать основные потенциальные каналы доступа к информации.
11. Назвать основные потенциальные каналы утечки информации.
12. Дать характеристику неформальной модели нарушителя.
13. 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)

2.4. РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕМА 4. ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Основные вопросы:

Источники угроз информационной безопасности РФ

2. Классификация источников угроз информационной безопасности

3. Классификация уязвимостей информационных систем

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 29-31.

Вопрос 2 изложен в учебном пособии [1] на с. 31-32.

Вопрос 3 изложен в учебном пособии [1] на с. 32-34.

Контрольные вопросы по теме 4:

1. Пояснить на 2-3 примерах логическую цепочку угроз и их проявлений.
2. Дать определения угрозы, источника угроз, уязвимости и последствий реализации угроз.
3. Дать характеристику источникам внутренних и внешних угроз информационной безопасности РФ.
4. Пояснить выбранный вариант классификации источников угроз информационной безопасности.
5. Охарактеризовать антропогенные источники угроз и основные меры по их нейтрализации.
6. Охарактеризовать техногенные источники угроз и основные меры по их нейтрализации.
7. Охарактеризовать стихийные источники угроз и основные меры по их нейтрализации.
8. Привести примеры уязвимостей, присущих информационным системам.
9. Пояснить выбранный вариант классификации уязвимостей информационной системы.

Тесты для самостоятельной работы:

1. Источниками угроз информационной безопасности не являются:

а) социальные источники
б) антропогенные источники
в) техногенные источники
г) стихийные источники

2. 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

3. 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

2.5. РАЗДЕЛ 2 ИНФОРМАЦИОННАЯ ВОЙНА, МЕТОДЫ И СРЕДСТВА ЕЁ ВЕДЕНИЯ

ТЕМА 5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО

Основные вопросы:

1. Проблемы информационной войны

2. Субъекты информационного противоборства

3. Составные части и методы информационного противоборства

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 35-38.

Для самостоятельного изучения вопроса 1 следует обратиться к [6] главы 6-7. [4] глава 1.

Вопрос 2 изложен в учебном пособии [1] на с. 38-40.

Вопрос 3 изложен в учебном пособии [1] на с. 40-43.

Контрольные вопросы по теме 5:

1. Определение информационно-психологического воздействия. Примеры.
2. Раскрыть сущность понятия «информационная война».
3. Пояснить суть составляющих психологической войны.
4. Назвать основные средства Хакерской войны.
5. Основные субъекты информационного противоборства.
6. Назвать основные сферы ведения информационного противоборства.
7. Составные части информационного противоборства в политической сфере.
8. Пояснить сущность уровней ведения информационного противоборства.
9. Что понимается под информационно-психологическим воздействием.
10. Информационное оружие и основные методы его применения.

Тесты для самостоятельной работы:

1. Что, из нижеперечисленного, не относится к информационной войне?

а) Электронная война

б) Психологическая война

в) Хакерская война

г) Террористические акты

2. Объектом воздействия информационного оружия является:

а) Системы ПВО

б) Психика человека

в) Социальная инфраструктура

2.6. РАЗДЕЛ 2 ИНФОРМАЦИОННАЯ ВОЙНА, МЕТОДЫ И СРЕДСТВА ЕЁ ВЕДЕНИЯ

ТЕМА 6. ПРИЕМЫ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ В ИНФОРМАЦИОННОЙ ВОЙНЕ

Основные вопросы:

1. Информационная война как целенаправленное информационное воздействие информационных систем
2. Способы перепрограммирования информационных систем
3. Проблема начала информационной войны

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 43-46.

Для самостоятельного изучения вопроса 1 следует обратиться к [4] глава 5.

Вопрос 2 изложен в учебном пособии [1] на с. 46-50.

Для самостоятельного изучения вопроса 1 следует обратиться к [8] глава 10.

Вопрос 3 изложен в учебном пособии [1] на с. 50-52.

Для самостоятельного изучения вопроса 1 следует обратиться к [8] глава 11.

Контрольные вопросы по теме 6:

1. Привести примеры информационных воздействий.
2. Раскрыть понятие перепрограммирования информационных систем.
3. Привести примеры открытых и скрытых целенаправленных информационные воздействий систем друг на друга.
4. Примеры перепрограммирования людей в мире ПО.
5. Сущность формальных определений информационных обучающихся систем.
6. Каким образом можно перепрограммировать информационную систему?
7. Способы перепрограммирования ИС с использованием СМИ.
8. Способы защиты от перепрограммирования информационной системы.
9. Алгоритм защиты от перепрограммирования информационной системы.
10. Зачем нужно знать время начала информационной войны?

Тесты для самостоятельной работы:

1. Какое из перечисленных утверждений ошибочно?

а) Нарушение защитных барьеров во взаимодействии элементов сложной системы друг с другом приводит к перепрограммированию этих элементов и/или их уничтожению

б) Основными средствами корректировки протоколов информационно-логического взаимодействия для социального пространства сегодня стали СМИ

в) Протокол информационно-логического взаимодействия для элементов

социального пространства нашел свое воплощение в языках программирования

2. Какой вид воздействия на информационную систему наиболее эффективен?
а) входные данные — «сухие» факты
б) входные данные — эмоционально окрашенные утверждения
в) входные данные — логически обоснованные выводы

2.7. РАЗДЕЛ 2 ИНФОРМАЦИОННАЯ ВОЙНА, МЕТОДЫ И СРЕДСТВА ЕЁ ВЕДЕНИЯ

ТЕМА 7. ТИПОВАЯ СТРАТЕГИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ

Основные вопросы:

1. Обобщенный алгоритм информационной войны
2. Основные аспекты информационной войны
3. Последствия информационной войны

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 52-54.

Вопрос 2 изложен в учебном пособии [1] на с. 54-58.

Для самостоятельного изучения вопроса 1 следует обратиться к [8] Глава 12.

Вопрос 3 изложен в учебном пособии [1] на с. 58-62.

Для самостоятельного изучения вопроса 1 следует обратиться к [8] Глава 13.

Контрольные вопросы по теме 7:

1. Пояснить на примере зависимость устойчивости системы к целенаправленному информационному воздействию от мощности базовых элементов.
2. Дать характеристику алгоритма информационной войны.
3. Применение «Протоколов собраний Сионских мудрецов».
4. Проблемы защиты от информации и продвижение своего видения мира.
5. Чем характеризуется система, проигравшая в информационной войне?
6. Охарактеризовать победителя и побеждённого в информационной войне.
7. Роль ситуационного моделирования для ведения информационной войны.
8. СМИ как классическое информационное оружие.

Тесты для самостоятельной работы:

1. Как на западе называлась наука, придуманная для изучения индивидуальных особенностей и потенциальных возможностей «базовых элементов» СССР?

а) Коммунистициология
б) Кремлинология
в) Союзология

2. Чем прежде всего является информационное оружие?

а) Совокупностью методов
б) Технологией
в) Алгоритмом

3. Какое из утверждений верно?

а) Исходными данными систем, функционирующих в социальном пространстве, являются общегосударственные и частные банки данных на граждан, предприятия, услуги, товары
б) Результатом информационной войны становится рациональное поведение поверженных систем
в) СМИ не являются информационным оружием, принадлежащим правящей верхушке.

2.8. РАЗДЕЛ 3. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

ТЕМА 8. КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Основные вопросы:

1. Концепция защиты автоматизированных систем и средств вычислительной техники
2. Классификация автоматизированных систем по уровню их защищённости
3. Требования к автоматизированным системам по обеспечению безопасности информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 7-8.
Вопрос 2 изложен в учебном пособии [2] на с. 8-10.
Вопрос 3 изложен в учебном пособии [2] на с. 10-12.

Контрольные вопросы по теме 8:

1. Назвать и охарактеризовать пять руководящих документов ГТК России, посвященных вопросам защиты информации в АС в процессе ее обработки.
2. В чём суть Концепции защиты автоматизированных систем и средств вычислительной техники.
3. Классификация АС по уровню их защищённости.
4. Дать характеристику основных этапов классификации АС.
5. Классификация СВТ по уровню защищенности.
6. Привести основные требования к АС по обеспечению безопасности информации.

Тесты для самостоятельной работы:

1. Необходимыми исходными данными для проведения классификации конкретной ИС не является:

а) Перечень защищаемых информационных ресурсов и их уровень конфиденциальности

б) Перечень лиц, имеющих доступ к штатным средствам ИС с указанием их уровня полномочий.

в) Матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам ИС.

г) Перечень основных признаков ИС, необходимых для классификации

2. К числу определяющих признаков, по которым производится группировка ИС в различные классы, не относится:

а) Отсутствие в ИС информации различного уровня конфиденциальности

б) Уровень полномочий субъектов доступа ИС на доступ к конфиденциальной информации

в) Режим обработки данных в ИС – коллективный или индивидуальный

3. Сколько существует классов защищенности ИС от НСД к информации?

а) 10

б) 9

в) 12

г) 5

4. Что, из перечисленного, включает в себя ИС первой группы обработки информации?

а) ИС, в которых работает один пользователь

б) ИС, в которых пользователи имеют одинаковые права доступа

в) Многопользовательские ИС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности

2.9. РАЗДЕЛ 3. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

ТЕМА 9. СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. НАЗНАЧЕНИЕ И ФУНКЦИИ ЭЛЕМЕНТОВ

Основные вопросы:

1. Принципы защиты информации от НСД

2. Структура системы защиты информации, назначение и функции элементов

3. Типовая структура комплексной системы защиты информации от НСД

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 13-14.

Вопрос 2 изложен в учебном пособии [2] на с. 14-18.

Вопрос 3 изложен в учебном пособии [2] на с. 18-19.

Контрольные вопросы по теме 9:

1. Дать определение несанкционированного доступа и перечислить основные способы НСД.
2. Основные принципы защиты от НСД.
3. Характеристика основным подсистем СЗИ.
4. Раскрыть функционал подсистемы управления СЗИ.
5. Обобщённый алгоритм функционирования СЗИ.
6. Основные этапы развития СЗИ.
7. Состав типовой комплексной СЗИ предприятия.

Тесты для самостоятельной работы:

1. К основным способам НСД не относится:

а) Непосредственное обращение к объектам доступа

б) Резервирование технических средств, дублирование массивов и носителей информации

в) Создание программных и технических средств

г) Модификация средств защиты

2. К принципам защиты от НСД не относится:

а) Защита СВТ обеспечивается комплексом программно-технических средств

б) Защита СВТ и АС основывается на положениях и требованиях соответствующих законов, стандартов и нормативно-методических документов по защите от НСД к информации

в) Защита АС обеспечивается отдельными сотрудниками, ответственными за защиту информации

г) Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер

3. К основным способам НСД не относится:
а) Непосредственное обращение к объектам доступа
б) Резервирование технических средств, дублирование массивов и носителей информации
в) Создание программных и технических средств
г) Модификация средств защиты

4. К принципам защиты от НСД не относится:
а) Защита СВТ обеспечивается комплексом программно-технических средств
б) Защита СВТ и АС основывается на положениях и требованиях соответствующих законов, стандартов и нормативно-методических документов по защите от НСД к информации
в) Защита АС обеспечивается отдельными сотрудниками, ответственными за защиту информации
г) Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер

2.10. РАЗДЕЛ 3. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

ТЕМА 10. МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ

Основные вопросы:
1. Дискреционная политика
2. Мандатная политика (MLS)

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [2] на с. 19-24.
Вопрос 2 изложен в учебном пособии [2] на с. 24-30.

Контрольные вопросы по теме 10:
1. Что такое «Управление доступом (Разграничение доступа)»?
2. Основные классы моделей управления доступом.
1. Дать характеристику дискреционного управления доступом.
2. Свойства дискреционного управления доступом и варианты задания матрицы доступа.
3. Основные проблемы дискреционной политики.
4. Мандатное управление доступом.
5. Основные свойства и правила модели Белла-Лападулы.
6. Сравнительный анализ мандатного и дискреционного управления доступом.

Тесты для самостоятельной работы:

1. Какое из утверждений относится к мандатным моделям управления доступом?

а) Модель, в которой владелец ресурса сам задает права доступа к нему

б) Модель, копирующая иерархическую структуру организации и позволяющая упростить администрирование

в) Модель, в которой режим доступа субъектов к объектам определяется установленным режимом конфиденциальности

г) Модель являющаяся наиболее универсальной и позволяющая контролировать доступ с учетом произвольных параметров среды, субъектов и объектов доступа

2. Какое из утверждений относится к мандатным моделям управления доступом?

а) Модель, в которой владелец ресурса сам задает права доступа к нему

б) Модель, копирующая иерархическую структуру организации и позволяющая упростить администрирование

в) Модель, в которой режим доступа субъектов к объектам определяется установленным режимом конфиденциальности

г) Модель являющаяся наиболее универсальной и позволяющая контролировать доступ с учетом произвольных параметров среды, субъектов и объектов доступа

3. Какое из утверждений относится к дискреционным моделям управления доступом?

а) Модель, в которой владелец ресурса сам задает права доступа к нему

б) Модель, копирующая иерархическую структуру организации и позволяющая упростить администрирование

в) Модель, в которой режим доступа субъектов к объектам определяется установленным режимом конфиденциальности

г) Модель, являющаяся наиболее универсальной и позволяющая контролировать доступ с учетом произвольных параметров среды, субъектов и объектов доступа

2.11. РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 11. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Основные вопросы:

1. Основные понятия криптографии
2. История криптографии
3. Пример простейшего шифра

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 30-35.
Вопрос 2 изложен в учебном пособии [2] на с. 35-37.
Вопрос 3 изложен в учебном пособии [2] на с. 37-38.

Контрольные вопросы по теме 11:

1. Основные способы защиты информации.
2. Сферы применения криптографии в современном обществе.
3. Назвать основные понятия криптографии.
4. Криптосистемы: симметричные и с открытым ключом.
5. Что такое электронная подпись?
6. Основные требования к криптографическим системам.
7. Методы шифрования с симметричными ключами.
8. История развития криптографии.
9. Шифр Юлия Цезаря.
10. Способы усовершенствования Шифра Юлия Цезаря.

Тесты для самостоятельной работы:

1. Что, из перечисленного, не является сферой применения криптографии?

а) Обслуживание банковских пластиковых карт
б) Хранение и обработка паролей пользователей в сети
в) Сдача бухгалтерских и иных отчетов через удаленные каналы связи
г) Использование цифровых водяных знаков

2. Дешифрование это:

а) процесс расшифрования без знания ключа
б) процесс, обратный шифрованию

2.12. РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 12. СИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

Основные вопросы:

1. Обобщенная схема симметричной криптосистемы
2. Алгоритм шифрования DES
3. ГОСТ Р 34.12-2015 «Магма»
4. Особенности применения алгоритмов симметричного шифрования

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 38-43.
Вопрос 2 изложен в учебном пособии [2] на с. 43-44.

Вопрос 3 изложен в учебном пособии [2] на с. 44-46.
Вопрос 4 изложен в учебном пособии [2] на с. 46-47.

Контрольные вопросы по теме 12:

1. Обобщенная схема симметричной криптосистемы.
2. От чего зависит конфиденциальность передачи информации с помощью симметричной криптосистемы?
3. Каким образом обеспечивается целостность данных?
4. Как осуществляется распределения ключей между пользователями.
5. Общая характеристика алгоритма шифрования DES.
6. Общая характеристика ГОСТ Р 34.12-2015 («Магма»).
7. Особенности применения алгоритмов симметричного шифрования.

Тесты для самостоятельной работы:

1. Какой принцип, из перечисленных, не используется для получения стойких блочных шифров?

а) рассеивание
б) расслоение
в) перемешивание

2. Какой стандарт шифрования, из перечисленных, вошёл в современный ГОСТ Р 34.12-2015?

а) DES
б) ГОСТ 28147- 89
в) RSA

3. Какая проблема является наиболее актуальной для симметричных криптосистем?

а) проблема безопасного распределения симметричных секретных ключей
б) проблема использования ресурсоемких операций
в) проблема реализации аппаратного шифратора

2.13. РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 13. АСИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

Основные вопросы:

1. Обобщенная схема асимметричной криптосистемы шифрования
2. Функция хэширования
3. Электронная подпись

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 47-52.
Вопрос 2 изложен в учебном пособии [2] на с. 52-54.
Вопрос 3 изложен в учебном пособии [2] на с. 54-57.

Контрольные вопросы по теме 13:

1. Обобщенная схема асимметричной криптосистемы шифрования.
2. Процесс передачи зашифрованной информации в асимметричной криптосистеме.
3. Назвать характерные особенности асимметричных криптосистем.
4. Требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы.
5. Привести пример однонаправленной функции.
6. Преимущества и недостатки асимметричных криптосистем.
7. Функция хэширования и её свойства.
8. Что такое дайджест сообщения?
9. Электронная подпись.
10. От каких видов злоумышленных действий позволяет защитить использование ЭП?
11. Процедуры формирования и проверки ЭП.

Тесты для самостоятельной работы:

1. Какое требование, из перечисленных, не характерно для асимметричной криптосистемы?

а) вычисление пары ключей (Kb и кb) получателем B (на основе начального условия) должно быть достаточно сложным

б) отправитель A, зная открытый ключ Kb и сообщение M, может легко вычислить криптограмму C=EKb(M)

в) получатель B, используя секретный ключ кb и криптограмму C, может легко восстановить исходное сообщение M=Dкb(C)

г) противник, зная открытый ключ Kb, при попытке вычислить секретный, ключ кb, (наталкивается на непреодолимую вычислительную проблему

2. Какой тип преобразований, из перечисленных, не используется в криптосистемах с открытым ключом?

а) разложение больших чисел на простые множители

б) решение дифференциальных уравнений

в) вычисление логарифма в конечном поле

г) вычисление корней алгебраических уравнений

2.14. РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 14. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Основные вопросы:

1. Основы идентификации и аутентификации
2. Классификация протоколов аутентификации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 57-60.
Вопрос 2 изложен в учебном пособии [2] на с. 60-64.

Контрольные вопросы по теме 14:

1. Пояснить сущность процедур идентификации и аутентификации.
2. Процесс идентификации и аутентификации.
3. Что такое авторизация и администрирование.
4. Категории процесса аутентификации в зависимости от предъявляемых субъектом сущностей.
5. Типы процессов аутентификации.
6. Основные характеристики протоколов аутентификации.
7. Классификация основных протоколов аутентификации.

Тесты для самостоятельной работы:

1. Что из перечисленного относится к администрированию?

а) Регистрация действий пользователя в сети, включая его попытки доступа к ресурсам
б) Процедура проверки подлинности заявленного пользователя, процесса или устройства
в) Процедура распознавания пользователя по его имени

2. Что, из перечисленного, обычно не используется в качестве биометрических признаков при аутентификации потенциального пользователя

а) Отпечатки пальцев
б) Форма и размеры лица
в) Отпечаток стопы
г) Особенности голоса

2.15. РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 15. РАЗГРАНИЧЕНИЕ И КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ

Основные вопросы:

1. Ограничение доступа
2. Контроль доступа к аппаратуре
3. Разграничение и контроль доступа к информации ИС
4. Разграничение привилегий на доступ

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 65-66.
Вопрос 2 изложен в учебном пособии [2] на с. 66-67.
Вопрос 3 изложен в учебном пособии [2] на с. 68-69.
Вопрос 4 изложен в учебном пособии [2] на с. 69-70.

Контрольные вопросы по теме 15:

1. В чём заключается ограничение доступа к комплексам средств автоматизации?
2. Цели ограничения доступа и способы их реализации.
3. Контроль доступа к аппаратуре.
4. Основные принципы контроля доступа к аппаратуре.
5. Разделение привилегий на доступ.

Тесты для самостоятельной работы:

1. Задачей средств ограничения доступа является:

а) Исключить случайный и преднамеренный доступ посторонних лиц на территорию размещения КСА и непосредственно к аппаратуре

б) Создать некоторые преграды вокруг объекта защиты

в) Использовать цепи сигнализации и индикации в комплексе с различными датчиками

2.16. РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 16. ТЕХНОЛОГИИ МЕЖСЕТЕВЫХ ЭКРАНОВ

Основные вопросы:

1. Основные понятия технологии межсетевых экранов
2. Функции межсетевых экранов
3. Ориентация МЭ на уровни эталонной модели

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 70-72.
Вопрос 2 изложен в учебном пособии [2] на с. 72-76.
Вопрос 3 изложен в учебном пособии [2] на с. 76-87.

Контрольные вопросы по теме 16:

1. Что понимается под технологией межсетевого экранирования?
2. Классификация межсетевых экранов.
3. Основные функции межсетевых экранов.
4. Структура межсетевого экрана.
5. Функции посредничества межсетевых экранов.
6. Эталонная сетевая модель OSI.
7. Типы межсетевых экранов, функционирующих на различных уровнях модели OSI.

Тесты для самостоятельной работы:

1. Какие 2 протокола, из перечисленных, относятся к транспортному уровню модели OSI?

а) UDP
б) SMTP
в) FTP
г) TCP

2. Какие 2 протокола, из перечисленных, относятся к физическому уровню модели OSI?

а) UDP
б) IRDA
в) FTP
г) Bluetooth

2.17. РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 17. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN)

Основные вопросы:

1. Основные понятия и функции виртуальных сетей
2. Специфика построения VPN
3. Туннелирование в виртуальных частных сетях
4. Схема виртуальной частной сети
5. Политики безопасности в виртуальных частных сетях
6. Цифровые сертификаты
7. Примеры отечественного построения VPN

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 87-90.
Вопрос 2 изложен в учебном пособии [2] на с. 90-91.
Вопрос 3 изложен в учебном пособии [2] на с. 91-94.
Вопрос 4 изложен в учебном пособии [2] на с. 94-96.
Вопрос 5 изложен в учебном пособии [2] на с. 96-98.
Вопрос 6 изложен в учебном пособии [2] на с. 98-99.
Вопрос 7 изложен в учебном пособии [2] на с. 99-100.

Контрольные вопросы по теме 17:

1. Что понимается под технологией защищенных виртуальных частных сетей?
2. Пример частной сети с собственными территориальными каналами.
3. Специфика построения VPN. Что такое VPN-агент?
4. Механизм туннелирования (инкапсуляции).
5. Политики безопасности в виртуальных частных сетях.
6. Основные варианты построения VPN.
7. Примеры отечественных VPN.

Тесты для самостоятельной работы:

1. Суть туннелирования VPN состоит в том, что:

а) при туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня

б) при туннелировании пакет протокола более высокого уровня помещается в поле данных пакета протокола более низкого уровня

2. Как называют протокол IPX, переносящий данные в интрасеть филиалов предприятия?

а) протокол-пассажир

б) несущий протокол
в) протокол туннелирования

2.18. РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 18. МЕТОДЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ (АТАК)

Основные вопросы:

1. Классификация систем обнаружения вторжений
2. Интеллектуальное и поведенческое обнаружение вторжений

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] главы 2-3.
Вопрос 2 изложен в учебном пособии [7] главы 5-7.

Контрольные вопросы по теме 18:

1. Охарактеризовать элементы, входящие в обобщённую систему обнаружения вторжений (СОВ).
2. Каким образом оценивается эффективность СОВ.
3. Какие отличия интеллектуальной СОВ от поведенческой.
4. Пояснить классификацию СОВ.
5. Привести примеры СОВ системного и сетевого уровней.
6. Роль хоста-бастиона при обнаружении вторжений.

Тесты для самостоятельной работы:

1. Система обнаружения вторжений (СОВ) называется поведенческой, если она:
а) работает с информацией о вторжениях (атаках)
б) использует информацию о нормальном поведении контролируемой системы
в) только выдает предупреждения

2. Система обнаружения вторжений (СОВ) называется интеллектуальной, если она:
а) работает с информацией о вторжениях (атаках)
б) использует информацию о нормальном поведении контролируемой системы
в) только выдает предупреждения

3. В чём основное преимущество систем обнаружения аномалий (СОА)?
а) обнаружение неизвестных атак
б) скорость работы
в) Большое число ложных срабатываний (выдачи ложных сигналов тревоги)

2.19. РАЗДЕЛ 5. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 19. ПЕРСОНАЛЬНЫЕ СРЕДСТВА АУТЕНТИФИКАЦИИ И ЗАЩИЩЁННОГО ХРАНЕНИЯ ДАННЫХ - USB-КЛЮЧИ И СМАРТ-КАРТЫ ETOKEN

Порядок выполнения лабораторной работы:

Методика выполнения лабораторной работы включает в себя следующие положения:

1. Ознакомление с теоретической частью eToken.
2. Установка программного обеспечения приложения eToken PKI Client (набор драйверов и дополнительных утилит, обеспечивающий работу с электронными ключами eToken в операционной системе Microsoft Windows).
3. Установка eToken Network Logon.
4. Подключение USB-ключа к порту USB рабочей станции.
5. Инициализация eToken.
6. Смена пароля eToken.
7. Работа пользователя с eToken.

Подробные сведения по установке и настройке работе ПО eToken содержатся в комплекте документации (Руководство администратора, Руководство пользователя и Правила эксплуатации USB-ключей, смарт-карт и брелоков eToken), который поставляется совместно с комплексом. Кроме того, данная информация доступна на сайте компании http://www.aladdin.ru.

Рекомендации по изучению темы:

Вопрос изложен в учебном пособии [14] на с. 11-13.

Контрольные вопросы по теме 19:

1. Назначение персональных средств аутентификации данных.
2. Что входит в линейку продуктов eToken?
3. Основные этапы установки ПО eToken.
4. Администрирование. Основные настройки eToken.
5. Основные возможности eToken Network Logon.
6. Способы разблокирования eToken.
7. Меры при утере электронного ключа eToken.
8. Изменение пароля доступа к домену/компьютеру.

2.20. РАЗДЕЛ 5. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 20. ПЕРСОНАЛЬНОЕ СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ШИПКА»

Порядок выполнения лабораторной работы:

Методика выполнения лабораторной работы включает в себя следующие положения:

1. Установка и настройка ПСКЗИ «ШИПКА».

1.1 Инсталляция специального программного обеспечения (software).

1.2 Подключение аппаратной части изделия - USB-устройства «ШИПКА» (подключение USB-устройства «ШИПКА» осуществляется стандартным образом, т. е. установкой в свободный USB разъем системного блока ПЭВМ).

1.3 Подготовка к инициализации устройства ШИПКА (начальное форматирование и установка PIN-кода).

1.4 Начальное форматирование устройства ШИПКА.

1.5 Установка PIN-кода устройства ШИПКА.

1.6 Разблокирование устройства ШИПКА.

2. Использование ПСКЗИ «ШИПКА».

2.1 Шифрование и подпись файлов на жестком диске.

2.2 Получение цифровых сертификатов.

2.3 Импорт сертификатов в хранилища сертификатов и в физическое хранилище ПСКЗИ «ШИПКА».

2.4 Использование устройства ШИПКА в системах шифрования/подписи с открытым ключом (на примере защиты сообщений электронной почты).

2.5 Вход в домен Windows с использованием ПСКЗИ «ШИПКА» в качестве смарт-карты.

2.6 Защищенный вход на локальную рабочую станцию.

2.7 Использование ПСКЗИ для хранения и защиты персональной ключевой информации.

Подробные сведения по установке и настройке работе ПСКЗИ «ШИПКА» содержатся в комплекте документации (Руководство по эксплуатации, Руководство администратора, Руководство пользователя и Описание применения), который поставляется совместно с комплексом. Кроме того, данная информация доступна на сайте компании ОКБ САПР http://www.shipka.ru/.

Рекомендации по изучению темы:

Вопрос изложен в учебном пособии [14] на с. 13-16.

Контрольные вопросы по теме 20:

1. Назначение ПСКЗИ «ШИПКА».
2. В чём заключается начальное форматирование устройства ШИПКА.
3. Как производится установка PIN-кода устройства ШИПКА.
4. Как производится разблокирование устройства ШИПКА.
5. Последовательность шифрования и подписи файлов на жестком диске.
6. Получение цифровых сертификатов.
7. Как осуществляется импорт сертификатов в хранилища сертификатов и в физическое хранилище ПСКЗИ «ШИПКА».
8. Использование устройства ШИПКА в системах шифрования/подписи с открытым ключом (на примере защиты сообщений электронной почты).
9. Использование ПСКЗИ для хранения и защиты персональной ключевой информации.

2.21. РАЗДЕЛ 5. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 21. ЭЛЕКТРОННЫЙ ЗАМОК "СОБОЛЬ"

Порядок выполнения лабораторной работы:

Методика выполнения лабораторной работы включает в себя следующие положения:

1. Ознакомление с теоретической частью электронного замка "Соболь".
2. Установка программного обеспечения комплекса "Соболь".
3. Подготовка комплекса к инициализации.
4. Инициализация электронного замка "Соболь".
5. Подготовка электронного замка к эксплуатации.
6. Настройка и эксплуатация комплекса "Соболь".
7. Удаление программного обеспечения электронного замка "Соболь".

Подробные сведения об установке, удалении, настройке и эксплуатации электронного замка «Соболь» содержатся в документе "Программно-аппаратный комплекс (ПАК) "Соболь". Руководство администратора», который поставляется совместно с комплексом «Соболь». Кроме того, данная информация доступна на сайте компании "Информзащита" (http://www.infosec.ru/).

Рекомендации по изучению темы:

Вопрос изложен в учебном пособии [14] на с. 6-8.

Контрольные вопросы по теме 21:

1. Назначение электронного замка "Соболь".
2. Состав электронного замка "Соболь" и основные функции по защите информации от НСД.
3. Принцип работы механизма контроля целостности комплекса.
4. Принцип работы механизма сторожевого таймера комплекса.
5. Варианты применения электронного замка "Соболь".
6. В чем заключается инициализация электронного замка?
7. В чем заключается настройка и эксплуатация электронного замка?
8. Пояснить порядок смены паролей администратора и пользователей.
9. Работа с журналом регистрации событий.

2.22. РАЗДЕЛ 5. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 22. СИСТЕМА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ «SECRET DISK»

Порядок выполнения лабораторной работы:

Методика выполнения лабораторной работы включает в себя следующие положения:

1. Установить драйвер eToken, например, с web-сайта компании Аладдин Р.Д. www.aladdin-rd.ru/support/download/.
2. Установить программное обеспечение Secret Disk.
3. Подключить к компьютеру eToken с лицензией Secret Disk, зарегистрировать одного или нескольких пользователей Secret Disk, выбрать для них сертификаты открытого ключа, либо создать сертификаты открытого ключа с соответствующим закрытым ключом.
4. При выборе готовых сертификатов необходимо удостовериться в наличии резервных копий сертификатов и закрытых ключей. Если готовых сертификатов нет, их можно создать в памяти eToken средствами Secret Disk, сохраняя при создании резервные копии.
5. Создать зашифрованные диски.
6. Сохранить резервные копии мастер-ключей зашифрованных дисков.
7. При работе с мастер-ключами зашифрованных дисков следует руководствоваться инструкциями раздела Операции с мастер-ключами защищённых дисков.
8. Перенести необходимую конфиденциальную информацию с обычных дисков на зашифрованные, выбрав за основу сценарий (сценарии) использования Secret Disk на предприятии.
9. Предоставить (при необходимости) другим пользователям доступ к зашифрованным дискам.
10. Подключить зашифрованные диски.

11. Создать и удалить зашифрованный виртуальный диск.

12. Типовые сценарии использования Secret Disk на предприятии.

13. Отказ от использования Secret Disk и удаление его компонентов.

Подробные сведения по установке и настройке Secret Disk содержатся в комплекте документации (Справочное руководство, Дополнительные алгоритмы шифрования Secret Disk (Руководство пользователя), который поставляется совместно с системой защиты. Кроме того, данная информация доступна на сайте компании Аладдин http://www.aladdin.ru/.

Рекомендации по изучению темы:

Вопрос изложен в учебном пособии [14] на с. 17-19.

Контрольные вопросы по теме 22:

1. Назначение Secret Disk.
2. Пояснить, что такое сертификаты открытого ключа.
3. Порядок установки, настройки и использования Secret Disk.
3. Порядок создания/удаления зашифрованных дисков.
4. Типовые сценарии использования Secret Disk на предприятии.
5. Как отказаться от использования Secret Disk и удалить его компоненты?

2.23. РАЗДЕЛ 5. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 23. ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД «АККОРД–АМДЗ»

Порядок выполнения лабораторной работы:

Методика выполнения лабораторной работы включает в себя следующие положения:

1. Ознакомление с теоретической частью СЗИ НСД «Аккорд- АМДЗ».

2. Установка платы контроллера и программного обеспечения комплекса, включающая три основных этапа:

- установка платы контроллера в свободный слот ПЭВМ и регистрацию администратора безопасности информации (БИ) (супервизора), в том числе, настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ;

- регистрация пользователей, назначение пользователям личных ТМ-идентификаторов, паролей и времени доступа;

- назначение списка дисков, файлов, разделов реестра, контролируемых на целостность.

3. Инициализация СЗИ НСД «Аккорд- АМДЗ»:

- регистрация супервизора (администратора безопасности информации);

- регистрация нового пользователя.

4. Эксплуатация комплекса «Аккорд- АМДЗ».
5. Снятие средств защиты комплекса «Аккорд- АМДЗ».

Подробные сведения об установке, удалении, настройке и эксплуатации СЗИ НСД «Аккорд - АМДЗ» содержатся в комплекте документации на "Программно-аппаратный комплекс средств защиты информации от НСД для ПЭВМ “Аккорд–АМДЗ” (Описание применения, Руководство по установке, Руководство администратора, и Руководство пользователя), который поставляется совместно с комплексом «Аккорд - АМДЗ». Кроме того, данная информация доступна на сайте компании http://www.accord.ru.

Рекомендации по изучению темы:

Вопрос изложен в учебном пособии [14] на с. 8-11.

Контрольные вопросы по теме 23:

1. Назначение СЗИ НСД «Аккорд- АМДЗ».
2. Состав СЗИ НСД «Аккорд- АМДЗ» и основные функции по защите информации от НСД.
3. Основные этапы установки и настройки комплекса.
4. Порядок регистрации администратора БИ.
5. Порядок регистрации и удаления пользователя.
6. Назначение персонального идентификатора.
7. Порядок редактирования основных параметров администратора и пользователей.
8. Порядок контроля аппаратуры, целостности служебных областей жестких дисков и файлов.
9. Порядок работы с системным журналом СЗИ НСД «Аккорд- АМДЗ».