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. МЕТОДЫ И СРЕДСТВА ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА»

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. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа» / 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. Некоммерческая интернет-версия СПС "КонсультантПлюс":

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

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

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

2. Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 103 с.

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

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

5. 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.

6. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

7. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

8. Программно-аппаратная защита информации: учеб. Пособие / П.Б. Хорев. – М.: Форум, 2012. – 352 с.

9. 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

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

11. Основы программно-аппаратной защиты информации: Учебное пособие. Издание 4-е, перераб. и доп.- М.: ЛЕНАНД. – 416 с.

12. Основы программно-аппаратной защиты информации: Учебное пособие. Издание 4-е, перераб. и доп.- М.: ЛЕНАНД. – 416 с.

13. 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.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННЫЕ С НСД

ТЕМА 1. ПОНЯТИЕ И ОБЩАЯ КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННЫХ С НСД

Основные вопросы:

1. Основные термины и определения в области НСД.
2. Источники угроз безопасности информации.
3. Модели угроз безопасности информации, связанных с НСД.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 9-15, в учебном пособии [8] на с. 8-13.

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

Вопрос 2 изложен в учебном пособии [3] на с. 29-33

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

Контрольные вопросы по теме 1:

1. Перечислить основные документы ГТК при Президенте РФ и ФСТЭК России о НСД к информации
2. Что такое НСД к информации?
3. Какие подсистемы входят в систему защиты информации от НСД?
4. Перечислить основные угрозы безопасности информации
5. Охарактеризовать основные источники угроз безопасности информации
6. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации
7. Что такое «Модель угроз безопасности информации»

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

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

2.2. РАЗДЕЛ 1. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННЫЕ С НСД

ТЕМА 2. МЕТОДЫ ВЫЯВЛЕНИЯ И АНАЛИЗА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО В АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМАХ

Основные вопросы:
1. Методы выявления уязвимостей информационных систем
2. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [3] на с. 29-34.

Вопрос 2 изложен в учебном пособии [6].

Для самостоятельного изучения вопроса 2 следует обратиться к [7].

Контрольные вопросы по теме 2

1. Перечислить основные методы выявления уязвимостей информационных систем
2. Какие факторы опасности (причины возникновения угроз) Вы знаете?
3. Пояснить классификацию естественных и искусственных угроз.
4. Привести 5 примеров основных непреднамеренных искусственных угроз.
5. Привести 5 примеров основных преднамеренных искусственных угроз.
6. Что такое уязвимости информационных систем
7. Назвать основные потенциальные каналы доступа к информации.
8. Назвать основные потенциальные каналы утечки информации.

Тесты для самостоятельной работы:

1. К происшествиям, связанным с ненамеренными действиями людей, относятся:

а) неправильное обращение с гибкими дисками или другими магнитными носителями при их использовании или хранении

б) ложное объявление себя другим пользователем (маскировка) для нарушения адресации сообщений или возникновения отказа в законном обслуживании

в) нарушения в сети электропитания: перенапряжения или импульсные выбросы, аварийное отключение электропитания;

г) блокировка канала связи собственными сообщениями, вызывающая отказ в обслуживании легальных пользователей

2. Программная закладка – это?

а) специализированная программа анализирует проходящий по сети трафик и декодирует его

б) программа, которая сохраняют вводимую с клавиатуры информацию (в том числе и пароли) в некоторой зарезервированной для этого области.

в) программа, которая захватывает (монополизирует) отдельные ресурсы вычислительной системы, не давая другим программам возможности его использовать

г) программа, которая приводит к повреждению файлов или компьютеров.

2.3. РАЗДЕЛ 1. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННЫЕ С НСД

ТЕМА 3. БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ВКЛЮЧАЮЩИХ БАЗУ ДАННЫХ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО В АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМАХ

Основные вопросы:

1. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.
2. Методы выявления уязвимостей информационных систем. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем, в том числе средств защиты информации информационных систем

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [8].

Для самостоятельного изучения вопроса 1 следует обратиться к [6, 7]

Вопрос 2 изложен в учебном пособии [4].

Контрольные вопросы по теме 3:

1. Общая характеристика Банка данных угроз безопасности информации
2. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах
3. Основные методы выявления уязвимостей информационных систем.
4. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем, в том числе средств защиты информации информационных систем
5. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE.
6. Общая система оценки уязвимостей (стандарт CVSS).

Тесты для самостоятельной работы:

1. 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

2. 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 2. МЕРЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

ТЕМА 4. ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ МЕР И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

Основные вопросы:
1. Методы ограничения доступа и управления доступом
2. Классы и виды НСД

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [2] на с. 57-60, 69-70.
Вопрос 2 изложен в учебном пособии [2] на с. 14-20.
Для самостоятельного изучения вопроса 2 следует обратиться к [13]

Контрольные вопросы по теме 4:
1. Методы ограничения доступа и управления доступом
2. Понятие несанкционированного доступа (НСД).
3. Классы и виды НСД
4. Идентификация и аутентификация
5. Дискреционное управление доступом
6. Мандатное управление доступом
7. Ролевое управление доступом

Тесты для самостоятельной работы:
1. Аутентификация – это
а) процедура проверки подлинности
б) присвоение субъектам и объектам идентификатора или сравнение идентификатора с перечнем присвоенных идентификаторов.
в) предоставление определённому лицу или группе лиц прав на выполнение определённых действий

2. Разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности)
а) мандатное

б) дискреционное
в) ролевое

2.5. РАЗДЕЛ 2. МЕРЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

ТЕМА 5. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

Основные вопросы:

1. Межсетевые экраны, требования к ним и способы применения.
2. Системы обнаружения вторжений, требования к ним и способы применения.
3. Криптографические средства защиты информации.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 70-87.
Вопрос 2 изложен в учебном пособии [9] главы 2-3.
Вопрос 3 изложен в учебном пособии [2] на с. 47-57.

Контрольные вопросы по теме 5:

1. Что понимается под технологией межсетевого экранирования?
2. Классификация межсетевых экранов.
3. Основные функции межсетевых экранов.
4. Охарактеризовать элементы, входящие в обобщённую систему обнаружения вторжений (СОВ).
5. Каким образом оценивается эффективность СОВ.
6. Какие отличия интеллектуальной СОВ от поведенческой.
7. Пояснить классификацию СОВ.
8. Обобщенная схема асимметричной криптосистемы шифрования.
9. Процесс передачи зашифрованной информации в асимметричной криптосистеме.
10. Назвать характерные особенности асимметричных криптосистем.
11. Требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы.
12. Привести пример однонаправленной функции.
13. Преимущества и недостатки асимметричных криптосистем.
14. Функция хэширования и её свойства.
15. Что такое дайджест сообщения?
16. Электронная подпись.
17. От каких видов злоумышленных действий позволяет защитить использование ЭП?
18. Процедуры формирования и проверки ЭП.

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

3. 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

4. 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

5. В чём основное преимущество систем обнаружения аномалий (СОА)?

а) обнаружение неизвестных атак
б) скорость работы
в) Большое число ложных срабатываний (выдачи ложных сигналов тревоги)

6. 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

7. 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

2.6. РАЗДЕЛ 2. МЕРЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

ТЕМА 6. ОБЩИЙ ПОРЯДОК СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

Основные вопросы:
1. Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации
2. Порядок проведения сертификационных испытаний на соответствие классам защищенности СВТ.
3. Отчетность по результатам испытаний.

Рекомендации по изучению темы:
Вопрос 1 изложен в РД СВТ. Защита от НСД к информации. Показатели защищенности от НСД.
Вопрос 2 изложен в РД СВТ. Защита от НСД к информации. Показатели защищенности от НСД.
Вопрос 3 изложен в [1.1-1.3].
Для самостоятельного изучения вопроса 3 следует обратиться к [13].

Контрольные вопросы по теме 6:
1. Основные показатели защищенности СВТ от НСД.
2. Требования к показателям защищенности.
3. Порядок проведения тестирования программного обеспечения
4. Дискреционный принцип контроля доступа
5. Мандатный принцип контроля доступа
6. Содержание руководства пользователя
7. Порядок формирования отчета

Тесты для самостоятельной работы:
1. Какие показатели защищенности отсутствуют в перечне показателей?
а) Очистка памяти
б) Изоляция модулей потребления
в) Очистка свободного места
г) Маркировка документов

2. Какие документы разрабатываются при проведении сертификационных испытаний?
а) Заявка на проведение сертификации
б) Решение о проведении сертификации
в) Акт отбора образца
г) Интегральная оценка уязвимостей кода
д) Методика испытаний

3. Что является объектом сертификационных испытаний?
а) Программно-аппаратные компоненты
б) Эксплуатационная документация
в) Техническая документация
г) Технологическая документация

4. Что не подлежит отбору испытательной лабораторией?
а) Дистрибутив программного обеспечения
б) Аппаратные компоненты СВТ
в) Тестовое программное обеспечение
г) Документация на СВТ

2.7. РАЗДЕЛ 2. МЕРЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

ТЕМА 7. ОПРЕДЕЛЕНИЕ ФАКТА ДОСТУПА К ФАЙЛАМ. ДОСТУП К ДАННЫМ СО СТОРОНЫ ПРОЦЕССА

Основные вопросы:
1. Способы определения факта доступа
2. Журналы доступа. Критерии информативности журналов доступа
3. Механизмы контроля аппаратной конфигурации ПЭВМ

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [10] на с. 171-173.
Вопрос 2 изложен в учебном пособии [11] на с. 174-179.
Вопрос 3 изложен в учебном пособии [12] на с. 120-123.

Контрольные вопросы по теме 7:
1. Основные способы определения факта доступа
2. Журналы доступа
3. Критерии информативности журналов доступа
4. Выявление следов несанкционированного доступа к файлам
5. Что такое метод инициированного НСД?
6. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя
7. Понятие и примеры скрытого доступа

8. Надежность систем ограничения доступа
9. Понятие электронного замка
10. Принципы построения и функционирования электронных замков
11. Механизмы контроля аппаратной конфигурации ПЭВМ

Тесты для самостоятельной работы:
1.Файлы, созданные процессом: 18
а) Наследуют идентификатор процесса и могут быть запущены только данным процессом
б) Наследуют идентификатор пользователя, запустившего процесс
в) Могут быть использованы только администратором

2.Функциями ПАК Соболь не являются:
а) Идентификация пользователей по электронным идентификаторам;
б) Проверка целостности программной среды и запрет загрузки с внешних носителей;
в) Контроль целостности аппаратной среды
г) Защищенная передача данных

2.8. РАЗДЕЛ 2. МЕРЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

ТЕМА 8. МЕРОПРИЯТИЯ ПО ФИЗИЧЕСКОЙ ЗАЩИТЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ И ОТДЕЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ, ИСКЛЮЧАЮЩИХ НСД К ТЕХНИЧЕСКИМ СРЕДСТВАМ, ИХ ХИЩЕНИЕ И НАРУШЕНИЕ РАБОТОСПОСОБНОСТИ

Основные вопросы:
1. Задачи, методы и средства физической защиты информации
2. Концепция инженерной защиты и технической охраны объекта

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [5] на с. 184-197.
Вопрос 2 изложен в учебном пособии [5] на с. 198-207.

Контрольные вопросы по теме 8:
1. Что можно отнести к средствам физической защиты информации
2. Для решения каких задач применяются физические средства защиты информации
3. На какие категории можно разделить физические средства защиты объектов?
4. Привести вариант классификации датчиков охранных систем
5. Что такое концепция инженерно-технической защиты объекта
6. Привести вариант классификации систем видеонаблюдения

7. Что можно отнести к средствам защиты ПЭВМ
8. Что относится к атрибутным и персональным методам опознавания
9. Что такое категорирование охраняемых зон по уровню доступа
10. Привести примеры систем пожарно-охранной сигнализации
11. Что относится к специальным средствам защиты

Тесты для самостоятельной работы:

1. К атрибутным методам опознавания относятся (отметить 3 позиции):

а) Отпечаток пальца
б) Особенности строения руки
в) Удостоверение личности
г) Карта с магнитным идентификатором
д) Паспорт

2. Какой из датчиков ориентирован на защиту по площади и объёму?

а) Инфракрасный датчик
б) Механический датчик
в) Коврики давления

3. Какой метод опознавания имеет более высокую степень защиты?

а) Идентификация по паролю
б) Идентификация по пропускной карте
в) Биометрическая идентификация