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 «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Для студентов специалитета по специальности 10.05.03 очной формы обучения

Ульяновск, 2020

Методические указания для самостоятельной работы студентов по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2020. 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 № 6/20 от 22.09.2020 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html.

2. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / 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

3. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201216.html.

4. Некоммерческая интернет-версия СПС "КонсультантПлюс":

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

4.2 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/

4.3 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/

4.4 Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/

5. 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. Режим доступа: http://gostexpert.ru/gost/gost-27002-2012

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

7. Андреев А. С. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная

безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" [Электронный ресурс] / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Электрон. текстовые дан. (1 файл : 14, 7 Мб). - Ульяновск : УлГУ, 2015. Режим доступа http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf

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

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

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

11. 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

12. Информационная безопасность открытых систем: учебник для вузов по спец. 075500 (090105) - "Комплексное обеспечение информ. безопасности автоматизир. систем": в 2 т. /Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В.. - М.: Горячая линия-Телеком, 2008. - 558 с.

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

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

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 1. ПРЕДМЕТ И ЗАДАЧИ ДИСЦИПЛИНЫ «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» (ПАСОИБ)

Основные вопросы:

1. Основные понятия и определения в создании «Программно-аппаратные средства информационной безопасности» (ПАСОИБ)
2. Предмет и задачи дисциплины ПАСОИБ
3. Нормативно-правовая база создания и использования ПАСОИБ

Рекомендации по изучению темы:

Вопрос 1 изложен в конспекте.

Для самостоятельного изучения вопроса 1 следует обратиться к [1] на с. 3-6.

Вопрос 2 изложен в учебном пособии [1] на с. 5-7.

Вопрос 3 изложен в учебном пособии [1] на с. 8-11.

Контрольные вопросы по теме 1:

1. Дать характеристику программно-аппаратных средств обеспечения информационной безопасности (ПАСОИБ)
2. Что относится к нормативно-правовой базе создания и использования ПАСОИБ?

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.

2.2. РАЗДЕЛ 1. ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 2. АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Понятие доступа, субъект и объект доступа
2. Классификация угроз информационной безопасности
3. Каналы утечки информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [9] на с. 57-60, 69-70.

Вопрос 2 изложен в учебном пособии [1] на с. 12-24.

Для самостоятельного изучения вопроса 2 следует обратиться к [8] на с. 23-33 и к [4.1-4.4].

Вопрос 3 изложен в учебном пособии [10] на с. 171-180.

Для самостоятельного изучения вопроса 3 следует обратиться к [11] на с. 9-17.

Контрольные вопросы по теме 2:

1. Охарактеризовать понятия доступа, субъекта и объекта доступа
2. Привести вариант классификации угроз информационной безопасности
3. Основные каналы утечки информации
4. Модель нарушителя. Для чего она нужна?

Тесты для самостоятельной работы:

1. Для защиты информации в каналах связи и узлах коммутации не используются:

а) процедуры аутентификации абонентов и сообщений
б) шифрование
в) средства контроля включения питания и загрузки программного обеспечения
г) специальные протоколы связи

2. 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

3. 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
программа, которая приводит к повреждению файлов или компьютеров.

2.3. РАЗДЕЛ 1. ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 3. МЕХАНИЗМЫ ЗАЩИТЫ. ПОЛИТИКА БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Основные вопросы:

1. Политика безопасности в компьютерных системах
2. Способы защиты конфиденциальности, целостности и доступности в КС
3. Основные механизмы защиты

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [12] на с. 227-240.

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

Вопрос 2 изложен в конспекте.

Для самостоятельного изучения вопроса 2 следует обратиться к [13] на с. 241-258.

Вопрос 3 изложен в конспекте.

Для самостоятельного изучения вопроса 3 следует обратиться к [2,3,6,7].

Контрольные вопросы по теме 3

1. Политика безопасности в компьютерных системах
2. Назвать основные механизмы защиты информации
3. Основные требования к защищенности информации
4. Что такое оценка защищенности информации?
5. Основные модели управления доступом
6. Основные способы защиты конфиденциальности, целостности и

доступности

7. Функции ядра безопасности

8. Привести вариант классификации функциональных требований по защите информации.

9. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления.

Тесты для самостоятельной работы:

1. Свойство верифицируемости монитора обращений говорит о том, что:

а) монитор обращений должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

д) необходимо предупредить возможность отслеживания работы монитора обращений.

б) монитор обращений должен вызываться при каждом обращении, не должно быть способов обойти его

2. Основными методами обеспечения целостности информации (данных) при хранении в автоматизированных системах являются:

а) обеспечение отказоустойчивости

б) обеспечение безопасного восстановления

в) оба ответа не верны

г) оба ответа верны

2.4. РАЗДЕЛ 1 ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 4. ОСНОВНЫЕ ПРИНЦИПЫ В СОЗДАНИИ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Классификация ПАСОИБ
2. Функциональные возможности ПАСОИБ
3. Принципы действия и технологические особенности ПАСОИБ

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 25-29.
Вопрос 2 изложен в учебном пособии [1] на с. 30-33.
Вопрос 3 изложен в учебном пособии [1] на с. 34-35.

Контрольные вопросы по теме 4:

1. Привести вариант классификации ПАСОИБ
2. Основные функциональные возможности ПАСОИБ

3. Охарактеризовать концепцию диспетчера доступа
4. Порядок проектирования ПАСОИБ
5. Модель системы защиты информации (СЗИ).

Тесты для самостоятельной работы:

1. На этапе планирования системы защиты:
а) определяются учитываемые воздействия на компоненты АС и риски, связанные с реализацией угроз безопасности.
б) формулируется система защиты как единая совокупность мер противодействия угрозам различной природы.
в) осуществляется выбор конкретных мер и средств обеспечения информационной безопасности
обеспечивается непрерывное функционирование системы защиты в жизненном цикле

2. К организационным принципам создания ПАСОИБ не относятся:
а) Принцип законности
б) Принцип персональной ответственности
в) Принцип ограничения полномочий по доступу к информации
Принцип минимального риска

2.5. РАЗДЕЛ 1. ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 5. ТИПОВАЯ СТРУКТУРА И ОСНОВНЫЕ ПРОГРАММНО–АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Структура ПАСОИБ. Компоненты и подсистемы.
2. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 41-44.
Вопрос 2 изложен в конспекте.

Контрольные вопросы по теме 5:

1. Структура типового ПАСОИБ. Компоненты и подсистемы
2. Основные функции ПАСОИБ
3. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ
4. Принципы действия и технологические особенности ПАСОИБ,

реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.

Тесты для самостоятельной работы:

1. Формальное описание структуры СЗИ не должно опираться на:

а) модель системы документооборота
б) модель информационной системы;
в) модель угроз информации и информационной системы;
г) модель угроз средств защиты информации.
д) все выше перечисленные

2. Механизмы защиты от угроз нарушения целостности включают:

а) механизмы восстановления
б) разграничение доступа,
в) аутентификацию
г) шифрование.

2.6. РАЗДЕЛ 1. ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 6. МЕТОДЫ РАЗГРАНИЧЕНИЯ ДОСТУПА И УПРАВЛЕНИЯ ДОСТУПОМ

Основные вопросы:

1. Методы ограничения доступа и управления доступом
2. Классы и виды НСД
3. Идентификация и аутентификация

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [9] на с. 57-60, 69-70.
Вопрос 2 изложен в учебном пособии [9] на с. 14-20.
Вопрос 3 изложен в учебном пособии [9] на с. 67-76.

Контрольные вопросы по теме 6:

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.

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

2.7. РАЗДЕЛ 1. ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 7. МЕТОДЫ РАЗГРАНИЧЕНИЯ ДОСТУПА И УПРАВЛЕНИЯ ДОСТУПОМ

Основные вопросы:

1. Понятие протокола идентификации и идентифицирующей информации
2. Способы хранения идентифицирующей информации
3. Контроль и управление доступом средствами операционной системы и программно-аппаратными техническими средствами

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [9] на с. 70-76.

Вопрос 2 изложен в учебном пособии [1] на с. 40-43.

Вопрос 3 изложен в учебном пособии [13] на с. 174-189.

Контрольные вопросы по теме 7:

1. В чём заключается задача идентификации пользователя
2. Дать понятие протокола идентификации
3. Локальная и удаленная идентификация
4. Понятие идентифицирующей информации
5. Способы хранения идентифицирующей информации
6. Симметричные и несимметричные методы аутентификации субъекта
7. Аутентификация объекта
8. Что такое авторизация

9. Контроль и управление доступом средствами операционной системы и программно-аппаратными техническими средствами

Тесты для самостоятельной работы:

1. Симметричным методом аутентификации является:

а) протокол Диффи-Хеллмана,
б) протокол Шнорра,
в) схема Kerberos
г) протокол Фиата-Шамира.

2. Основными атаками на протоколы аутентификации являются:

а) отражение передачи
б) повторная передача
в) маскарад
г) все ответы верны

2.8. РАЗДЕЛ 1. ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 8. МЕТОДЫ И СРЕДСТВА ХРАНЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Основные вопросы:

1. Информация, используемая для контроля доступа
2. Классификация средств хранения ключей и идентифицирующей информации
3. Типовые решения в организации ключевых систем

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 70-71.

Вопрос 2 изложен в учебном пособии [1] на с. 71-73.

Для самостоятельного изучения вопроса 2 следует обратиться к [14] на с. 363-368.

Вопрос 3 изложен в конспекте.

Для самостоятельного изучения вопроса 3 следует обратиться к [14] на с. 393-406.

Контрольные вопросы по теме 8:

1. Информация, используемая для контроля доступа: ключи и пароли
2. Привести вариант классификации средств хранения ключей и идентифицирующей информации
3. Организация хранения ключей
4. Типовые решения в организации ключевых систем
5. Открытое распределение ключей

6. Персональные средства аутентификации и защищенного хранения данных

Тесты для самостоятельной работы:

1. В иерархию ключей обычно входят:

а) 1 ключ
б) 2 ключа
в) 3 ключа
г) 4 ключа

2.Среди электронных ключей наиболее стойкими являются:

а) Ключи с памятью
б) Ключи с микропроцессором
в) Оба ответа не верны

2.9. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 9. ЗАЩИТА ОТ НЕЗАКОННОГО КОПИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ ПРОГРАММ

Основные вопросы:

1. Классификация аппаратных и программных компонентов защиты программ
2. Способы встраивания средств защиты в ПО
3. Привязка ПО к аппаратному окружению и физическим носителям как основное средство защиты от копирования ПО

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [14] на с. 112-123.

Вопрос 2 изложен в учебном пособии [1] на с. 98-100.

Для самостоятельного изучения вопроса 2 следует обратиться к [2] на с. 343-360

Вопрос 3 изложен в учебном пособии [1] на с. 107-112.

Контрольные вопросы по теме 9:

1. Привести вариант классификация аппаратных и программных компонентов защиты программ
2. Способы встраивания средств защиты в программное обеспечение (ПО)
3. Способы определения факта незаконного копирования и использования программ
4. Способы защиты от незаконного копирования и использования программ

5. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО

Тесты для самостоятельной работы:

1. Одним из способов создания ключей на жестких дисках является:

а) Логическое превышение объема дорожки.
б) Уменьшение межсекторных промежутков.
в) Привязка к архитектуре компьютера
г) Изменение контрольной суммы.

2. Какой способ встраивания защитных механизмов является основным для проектируемых и проверяемых СЗИ?

а) вставка фрагмента проверочного кода
б) вставкой проверочного механизма в исходный код на этапе разработки и отладки программного продукта
в) преобразованием исполняемого файла к неисполняемому виду (шифрование, архивация с неизвестным параметром и т.д.) и применением для загрузки некоторой программы, в теле которой и осуществляются необходимые проверки;
г) комбинированный

2.10. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 10. ЗАЩИТА ОТ РАЗРУШАЮЩИХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ И ИЗУЧЕНИЯ КОДА ПРОГРАММ

Основные вопросы:

1. Способы изучения кода программ
2. Обратное проектирование ПО
3. Защита от разрушающих программных воздействий

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 107-112.
Вопрос 2 изложен в конспекте.
Вопрос 3 изложен в учебном пособии [14] на с. 234-270.

Контрольные вопросы по теме 10:

1. Способы изучения кода программ
2. Обратное проектирование ПО
3. Способы защиты программ от изучения кода
4. Основные принципы обеспечения безопасности программ
5. Защита от разрушающих программных воздействий
6. Вирусы как особый класс разрушающих программных воздействий

7. Необходимые и достаточные условия недопущения разрушающего воздействия

8. Понятие изолированной программной среды

Тесты для самостоятельной работы:

1. Способ защиты от трассировки программ по заданному событию, представляющий собой замыкание цепочек обработки событий минуя программы трассировки.

а) Пассивная защита
б) Активная защита первого типа
в) Активная защита второго типа
г) Активная защита третьего типа

2. Использование аппаратных особенностей микропроцессора относится к следующему классу защиты ПО от исследования:

а) Влияние на работу отладочного средства через общие программные или аппаратные ресурсы
б) Влияние на работу отладочного средства путем использования особенностей его аппаратной или программной среды.
в) Влияние на работу отладчика через органы управления или/и устройства отображения информации.
г) Использование принципиальных особенностей работы управляемого человеком отладчика.

2.11. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 11. ОСНОВНЫЕ ПОДХОДЫ К ЗАЩИТЕ ДАННЫХ ОТ НСД

Основные вопросы:

1. Файл как объект доступа. Понятие атрибутов доступа
2. Организация доступа к файлам в различных ОС
3. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [11] на с. 171-173.
Вопрос 2 изложен в учебном пособии [14] на с. 174-179.
Вопрос 3 изложен в учебном пособии [1] на с. 120-123.

Контрольные вопросы по теме 11:

1. Файл как объект доступа
2. Оценка надежности систем ограничения доступа
3. Понятие атрибутов доступа

4. Организация доступа к файлам в различных ОС

5. Защита сетевого файлового ресурса

6. Вариант классификации программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ

Тесты для самостоятельной работы:

1. Защита от чтения на уровне системы может осуществляться

а) Введением атрибута Read Only для файлов;

б) Введением атрибута Hidden для файлов;

в) Введением запрета на чтение папки, в котором находится файл

г) Ни один вариант ответа не верен

2.12. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 12. 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 [11] на с. 171-173.

Вопрос 2 изложен в учебном пособии [14] на с. 174-179.

Вопрос 3 изложен в учебном пособии [1] на с. 120-123.

Контрольные вопросы по теме 12:

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:

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

2.13. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 13. ОСОБЕННОСТИ ЗАЩИТЫ ДАННЫХ ОТ ИЗМЕНЕНИЯ

Основные вопросы:

1. Защита массивов информации от изменения. Имитозащита
2. Подход на основе формирования хэш-функции, требования к построению и способы её реализации
3. Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаление программ и файлов.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [14] на с. 297-299.
Вопрос 2 изложен в учебном пособии [14] на с. 299-304.
Вопрос 3 изложен в документации на СЗИ «Dallas Lock».

Контрольные вопросы по теме 13:

1. Защита массивов информации от изменения
2. Что такое имитозащита?
3. Криптографическая постановка защиты от изменения данных
4. Подходы к решению задачи защиты данных от изменения
5. Подход на основе формирования имитоприставки
6. Подход на основе формирования хэш-функции
7. Формирование электронной подписи (ЭП)
8. Особенности защиты документов и исполняемых файлов
9. Проблема самоконтроля исполняемых модулей

Тесты для самостоятельной работы:

1. Какие программно-аппаратные средства предназначены для защиты от несанкционированного изменения, установки или удаление программ и файлов?

а) «Шипка»
б) VipNet
в) СЗИ «Dallas Lock»
г) СЗИ «Secret Disk»

2.14. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 14. МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Основные вопросы:

1. Классификация методов криптографического преобразования
2. Требования к программно-аппаратным комплексам шифрования
3. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [13] на с. 198-116.
Вопрос 2 изложен в учебном пособии [14] на с. 42-64.
Вопрос 3 изложен в конспекте.

Контрольные вопросы по теме 14:

1. Классификация методов криптографического преобразования
2. Нормативно-правовая база криптографического преобразования
3. Требования к программно-аппаратным комплексам шифрования
4. Необходимые и достаточные функции аппаратного средства криптозащиты
5. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования
6. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа

Тесты для самостоятельной работы:

1.Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

а) знание алгоритма шифрования не должно влиять на надежность защиты
б) структурные элементы алгоритма шифрования должны быть неизменными
в) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования
г) все вышеперечисленные

2.15. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 15. ПАСОИБ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Основные вопросы:

1. Классификация программно-аппаратных средств защиты информации в сетях передачи данных
2. Программно-аппаратные средства межсетевого экранирования
3. Основные принципы обнаружения сетевых атак

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 144-148.
Вопрос 2 изложен в учебном пособии [1] на с. 149-152.
Вопрос 3 изложен в учебном пособии [1] на с. 151-153.

Контрольные вопросы по теме 15:

1. Классификация программно-аппаратных средств защиты информации в сетях передачи данных
2. Принципы построения и функционирования межсетевых экранов в сетях передачи данных
3. Программно-аппаратные средства межсетевого экранирования
4. Основные принципы защиты информации при передаче по каналам связи
5. Программно-аппаратные средства защиты информации при передаче по каналам связи
6. Основные принципы обнаружения сетевых атак
7. Основные принципы защиты от сетевых атак
8. Обнаружение сетевых атак

Тесты для самостоятельной работы:

1.Примерами средств межсетевого экранирования не являются:

а) ПАК «Соболь»
б) СЗИ «Dallas Lock»
в) VipNet
г) Континент

2.16. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 16. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ СЕТИ

Основные вопросы:

1. Основные принципы управления безопасностью сети
2. Программно-аппаратные средства управления безопасностью сети

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 146-151.
Вопрос 2 изложен в учебном пособии [1] на с. 152-160.

Контрольные вопросы по теме 16:

1. Основные принципы управления безопасностью сети
2. Программно-аппаратные средства управления безопасностью сети
3. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи

Тесты для самостоятельной работы:

1. Агент безопасности, установленный на сервере приложений

а) Ориентирован на защиту индивидуального пользователя
б) ориентирован на обеспечение защиты серверных компонент распределенных приложений
в) обеспечивает раз вязку сегментов сети внутри предприятия или между предприятиями, решая задачи согласования политик безопасности разных сетей.

2. Независимая экспертиза отдельных областей функционирования предприятия.

а) Аудит
б) Аттестация
в) Сертификация
г) Аккредитация

2.17. РАЗДЕЛ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ТЕМА 17. СЕРТИФИКАЦИЯ СЗИ

Основные вопросы:

1. Система сертификации СЗИ. Нормативно-правовая база сертификации
2. Задачи сертификации ПАСОИБ на соответствие требованиям информационной безопасности

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 172-183.

Вопрос 2 изложен в учебном пособии [11] на с. 174-190.

Контрольные вопросы по теме 17:

1. Предназначение системы сертификации СЗИ
2. Задачи сертификации ПАСОИБ на соответствие требованиям информационной безопасности
3. Нормативно-правовая база сертификации ПАСОИБ на соответствие требованиям информационной безопасности
4. Технология сертификации ПАСОИБ на соответствие требованиям информационной безопасности

Тесты для самостоятельной работы:

1. Органы по сертификации средств защиты информации в пределах установленной области аккредитации:

а) утверждает нормативные документы, на соответствие требованиям которых проводится сертификация средств защиты информации в системе,
б) принимают решение о проведении повторной сертификации при изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации;
в) обеспечивают соответствие средств защиты информации требованиям нормативных документов по защите информации