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 «ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ПРИЛОЖЕНИЙ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

Для студентов специалитета по специальности 10.05.03
очной формы обучения

Ульяновск, 2021

Методические указания для самостоятельной работы студентов по дисциплине «Технология построения защищённых приложений открытых информационных систем» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2021. Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса, 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 зачёту и экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 2/21 от 16 марта 2021 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Методологические основы построения защищенных автоматизированных систем: учеб. пособие / А. В. Душкин, О. В. Ланкин, С. В. Потехецкий, А. П. Данилкин, А. А. Малышев - Воронеж: ВГУИТ, 2013. - 263 с. - ISBN 978-5-89448-981-0. - Текст: электронный https://www.iprbookshop.ru/47427.html

2. Барабанов, А. В. Семь безопасных информационных технологий / Барабанов А. В. , Дорофеев А. В. , Марков А. С. , Цирлов В. Л. - Москва: ДМК Пресс, 2017. - 224 с. - ISBN 978-5-97060-494-6. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785970604946.html

3. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О.В. Казарин, А.С. Забабурин. – Москва: Издательство Юрайт, 2021. – 312 с. – (Высшее образование). – Текст: непосредственный

4. Проектирование информационных систем: учебник и практикум для вузов / под общей редакцией Д. В. Чистова. — Москва: Издательство Юрайт, 2021. — 258 с. — (Высшее образование). — ISBN 978-5-534-00492-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469199

5. 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.

6. Грекул, В. И. Проектирование информационных систем: учебник и практикум для вузов / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — Москва: Издательство Юрайт, 2021. — 385 с. — (Высшее образование). — ISBN 978-5-9916-8764-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469757

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

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 1. ОБЩИЕ СВЕДЕНИЯ ОБ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Основные вопросы:

История развития открытых информационных систем (ОИС). Понятийный аппарат ОИС. Этапы развития ОИС. Основные принципы системного подхода при создании ОИС. Классификация ОИС.

Рекомендации по изучению темы:

Вопросы темы 1 изложены в учебном пособии [1] на с. 4-24.

Для самостоятельного изучения темы следует обратиться к учебному пособию [4] на с. 12-31.

Контрольные вопросы по теме 1:

1. Что такое «Открытая информационная система (ОИС)»
2. Что такое «Защищённая ОИС»?
3. Назвать этапы развития информационных систем
4. Перечислить основные черты современных ОИС
5. Привести вариант классификации ОИС
6. Назвать основные принципы системного подхода при создании сложных информационных систем

2.2. РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 2. ЖИЗНЕННЫЙ ЦИКЛ ИНФОРМАЦИОННЫХ СИСТЕМ

Основные вопросы:

Основные требования к защищённым ОИС. Принципы построения защищённых ОИС. Технология функционирования защищённых ОИС. Построение систем безопасности защищённых ОИС. Методические вопросы оценки эффективности защищённых ОИС. Показатели и критерии эффективности.

Рекомендации по изучению темы:

Вопросы темы 2 изложен в учебном пособии [1] на с. 25-52.

Для самостоятельного изучения темы следует обратиться к учебному пособию [4] на с. 5-16.

Контрольные вопросы по теме 2:

1. Назвать основные принципы построения защищённых ОИС
2. Перечислить основные требования к системам защиты информации в ИС
3. Дать характеристику технологии функционирования защищённой ОИС
4. Назвать основные задачи, необходимые для осуществления функций обеспечения защиты информации в ОИС
5. Что понимается под эффективностью оценки сложных систем?
6. Назвать основные показатели и критерии эффективности
7. Перечислить основные методы оценки эффективности ОИС
8. Пояснить алгоритм вероятностной оценки эффективности ОИС

2.3. РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 3. СТАНДАРТЫ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Основные вопросы:

Содержание угроз безопасности ОИС. Классификация угроз безопасности ОИС. Оценка угроз безопасности ОИС. Методы и модели угроз безопасности ОИС.

Рекомендации по изучению темы:

Вопросы темы 3 изложены в учебном пособии [1] на с. 59-93.

Для самостоятельного изучения вопросов темы следует обратиться к учебному пособию [4] на с. 58-98.

Контрольные вопросы по теме 3:

1. Что понимается под угрозой безопасности ОИС?
2. Перечислить основные угрозы безопасности ОИС
3. Назвать основные уязвимости ОИС (м.б. ЛР2 от Клочкова)
4. Что понимается под методологией выявления угроз безопасности информации?
5. Перечислить основные методы и модели анализа угроз безопасности ОИС

2.4. РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Основные вопросы:

Политика безопасности защищённых открытых информационных систем. Основные компоненты системы безопасности. Методы и системы защиты информации.

Рекомендации по изучению темы:

Вопросы темы 4 изложены в учебном пособии [1] на с. 94-127.

Для самостоятельного изучения темы следует обратиться в учебном пособии [5] на с. 227-240.

Контрольные вопросы по теме 4:

1. Привести примеры политик безопасности ОИС для типового предприятия
2. Что входит в структуру типовой политики безопасности?
3. Что относится к основным компонентам системы безопасности ОИС?
4. Для чего предназначен программный комплекс КОНДОР?
5. Каким образом осуществляется оценка рисков в программном комплексе КОНДОР?
6. Дать характеристику интерфейсу программы КОНДОР
7. Дать характеристику системы автоматизации разработки политики безопасности Toolbox
8. Возможно ли использовать Toolbox при формализации политики безопасности?

2.5. РАЗДЕЛ 2. ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ПРИЛОЖЕНИЙ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 5. МЕТОДОЛОГИЯ ПРОЕКТИРОВАНИЯ ЗАЩИЩЁННЫХ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Основные вопросы:

Общие задачи и этапы проектирования защищённых открытых информационных систем. Содержание этапов проектирования защищённых ОИС. Основные методы проектирования защищённых ОИС. Классификация объектов проектирования. Организация работ по проектированию защищённых ОИС.

Рекомендации по изучению темы:

Вопросы темы изложены в учебном пособии [1] на с. 128-153.

Для самостоятельного изучения темы следует обратиться к учебном пособии [6] на с. 38-82.

Контрольные вопросы по теме 5:

1. Назвать основные этапы проектирования защищённых ОИС
2. Что понимается под методологией проектирования защищённых ОИС
3. Что включается в техническое задание на проектируемую ОИС?
4. Что входит в организацию работ по проектированию ОИС?
5. Назвать основной функционал заказчиков и разработчиков
6. Исходные данные для проектирования защищённых ОИС
7. Жизненный цикл (ЖЦ) защищённых ОИС
8. Основные модели ЖЦ защищённых ОИС

2.6. РАЗДЕЛ 2. ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ПРИЛОЖЕНИЙ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 6. СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Основные вопросы:

Этапы развития и классификация CASE-средств. Основные характеристики CASE-средств.

Рекомендации по изучению темы:

Вопросы темы изложены в учебном пособии [1] на с. 154-171.

Для самостоятельного изучения темы следует обратиться к учебному пособию [4] на с. 158-171.

Контрольные вопросы по теме 6:

1. Что такое CASE-средства?
2. Что понимается под CASE-технологиями?
3. Перечислить этапы развития и классификацию CASE-средств
4. Преимущества разработки защищённых ОИС с использованием CASE-технологий
5. Перечислить основные типы CASE-средств
6. Дать предназначение Upper CASE
7. Дать предназначение Middle CASE
8. Дать предназначение ПО Lower

2.7. РАЗДЕЛ 2. ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ПРИЛОЖЕНИЙ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 7. МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗАЩИЩЁННЫХ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Основные вопросы:

Практические методы реализации моделей безопасности защищённых открытых информационных систем. Методология создания комплексной системы защиты информации открытых информационных систем. Математические модели обеспечения безопасности информации в защищённых открытых информационных системах. Технологический цикл реализации защищённой открытой информационной системы.

Рекомендации по изучению темы:

Вопросы темы изложен в учебном пособии [1] на с. 172-219.

Для самостоятельного изучения вопросов темы следует обратиться к учебному пособию [7] на с. 19-24.

Контрольные вопросы по теме 7:

1. Перечислить основные способы и средства защиты информации в информационных системах
2. Назвать условия, способствующие повышению эффективности защиты информации в ОИС
3. Что понимается под методологией комплексной системы защиты информации в ИС?
4. Требования, предъявляемые нормативными документами к ИС различных классов
5. Требования, предъявляемые нормативными документами к различным классам средств вычислительной техники
6. Перечислить основные математические модели обеспечения безопасности в информационных системах
7. В чём различие дискреционного и мандатного контроля доступа?

2.8. РАЗДЕЛ 2. ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ПРИЛОЖЕНИЙ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 8. РАСПРЕДЕЛЁННЫЕ ЗАЩИЩЁННЫЕ ОТКРЫТЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Основные вопросы:

Концепция построения и использования распределённых открытых информационных систем. Архитектура защищённых открытых информационных систем. Требования к распределённым защищённым открытым информационным системам. Основные методы защиты распределённых открытых информационных систем.

Рекомендации по изучению темы:

Вопросы темы изложен в учебном пособии [1] на с. 222-242.

Контрольные вопросы по теме 8:

1. Перечислить основные принципы построения защищённых ОИС
2. Что такое распределённые ОИС?
3. Перечислить основные принципы функционирования распределённых защищённых ОИС
4. Пояснить суть архитектуры «Клиент-сервер»
5. Требования, предъявляемые к системам защиты информации распределённых защищённых ОИС
6. Состав и структура распределённых защищённых ОИС
7. Основные методы защиты, применяемые в распределённых защищённых ОИС
8. Классификация программных средств защиты в распределённых защищённых ОИС

2.9. РАЗДЕЛ 2. ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ПРИЛОЖЕНИЙ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 9. РАЗРАБОТКА БЕЗОПАСНЫХ ПРОГРАММ ДЛЯ ЗАЩИЩЁННЫХ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Основные вопросы:

Жизненный цикл (ЖЦ) программ. Обзор мер безопасной разработки программ. Анализ требований по безопасности. Безопасное проектирование. Тестирование безопасности.

Рекомендации по изучению темы:

Вопросы темы изложен в учебном пособии [2] на с. 131-157.

Для самостоятельного изучения вопросов темы следует обратиться к учебному пособию [4] на с. 5-16.

Контрольные вопросы по теме 9:

1. Перечислить основные модели ЖЦ программного обеспечения (ПО)
2. Назвать положительные и отрицательные стороны каскадной модели
3. Дать характеристику спиральной модели ЖЦ ПО
4. Гибкая модель разработки ПО
5. Что такое безопасный ЖЦ ПО?
6. Дать классификацию уязвимостей ПО
7. Перечислить основные меры разработки безопасного ПО
8. Охарактеризовать основные процессы ЖЦ ПО
9. Требования по безопасности, предъявляемые к разрабатываемому ПО
10. Принципы создания проекта архитектуры ПО
11. Меры по тестированию разрабатываемого ПО

2.10. РАЗДЕЛ 2. ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ПРИЛОЖЕНИЙ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 10. МОДЕЛИРОВАНИЕ И ОЦЕНКА СООТВЕТСТВИЯ

Основные вопросы:

Понятие безопасной архитектуры. Концептуальные модели разграничения доступа. Принципы безопасной архитектуры защищённой ОИС. Скрытые каналы передачи информации. Критерии оценки информационной безопасности.

Рекомендации по изучению темы:

Вопросы темы изложен в учебном пособии [2] на с. 158-186.

Контрольные вопросы по теме 10:

1. Какие базовые понятия определяют безопасную архитектуру защищённых ОИС?
2. Что такое доверенная среда вычислений?
3. Назвать основные концептуальные модели информационной безопасности
4. В чём отличия мандатной политики доступа от ролевой?
5. Дать характеристику модели Белла-ЛаПадулы
6. Дать характеристику модели Биба
7. Назвать основные принципы безопасной архитектуры ОИС
8. Что такое скрытые каналы передачи информации?
9. Назвать типы скрытых каналов передачи информации
10. Назвать критерии оценки соответствия защищённых ОИС
11. Для чего нужен стандарт «Общие критерии»?
12. Что такое «профиль защиты»?

2.11. РАЗДЕЛ 2. ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ ПРИЛОЖЕНИЙ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ТЕМА 11. ИССЛЕДОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ПРЕДМЕТ ОТСУТСТВИЯ НЕДЕКЛАРИРОВАННЫХ

Сертификация средств защиты информации по требованиям безопасности информации. Проверка соответствия реальных и декларируемых функциональных возможностей. Методы проведения испытаний. Контроль исходного состояния программного комплекса посредством утилиты» ФИКС». Статический и динамический анализ исходных текстов и исполняемых модулей ПО.

Рекомендации по изучению темы:

Вопросы темы изложен в учебном пособии [3] на с. 159-180.

Контрольные вопросы по теме 11:

1. Кто занимается сертификацией средств защиты информации по требованиям безопасности?
2. Какие методы проверок применяются при проведении испытаний ПО?
3. Что должно входить в состав документации для испытаний ПО?
4. Для чего используется утилита ФИКС?
5. Что такое статический анализ исходных текстов и исполняемых модулей ПО?
6. С помощью каких средств проводится синтаксический контроль наличия заданных конструкций?
7. Каким образом проводится динамический анализ исходных текстов программ?
8. Укажите порядок действий при контроле и фиксации исходного состояния ПО программой ФИКС
9. На каких стадиях статического анализа исходных текстов используется утилита АИСТ?
10. Какова методика использования утилиты АИСТ для динамического анализа исходных текстов?