ПРИЛОЖЕНИЕ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Рязанский государственный радиотехнический университет имени В.Ф. Уткина»

КАФЕДРА «ЭЛЕКТРОННЫЕ ВЫЧИСЛИТЕЛЬНЫЕ МАШИНЫ»

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

«ПРОЕКТИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ»

Специальность

27.05.01 Специальные организационно-технические системы

Специализация

Информационные технологии и программное обеспечение в специальных организационно-технических системах

Квалификация (степень) выпускника — инженер-системотехник

Форма обучения — очная, очно-заочная

1. ПЛАНЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ И ЛАБОРАТОРНЫХ РАБОТ

а) Планы практических занятий

Тема 1 Введение

Современные средства обеспечения информационной безопасности компьютерных сетей

Цель – ознакомить обучающихся с современными средствами обеспечения информационной безопасности сетевых архитектур

Проблемы сетей специального назначения

Цель – дать представление обучающимся о структуре и проблематике сетей специального назначения.

Рекомендуемая литература:

1. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Лань, 2018. — 96 с. — ISBN 978-5-8114-3099-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110935 (дата обращения: 27.05.2020). — Режим доступа: для авториз. пользователей.

Тема 2 Основы законодательства РФ в области информационной безопасности компьютерных сетей

Стадии создания АСЗИ

Цель – изучение основных этапов создания АС в защищенном исполнении

Классификация АСЗИ

Цель – дать представление обучающимся о существующих подходах и стандартах классификации АС

Рекомендуемая литература:

1. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации
2. ГОСТ Р 51583-2014
3. ГОСТ 34.003-90
4. ГОСТ 34.601-90
5. РД 50-680-88
6. РД 50-34.680-90

Тема 3 Технологии построения локальных защищенных компьютерных сетей

МЭ. Классификация

Цель – ознакомить обучающихся с основами защиты сетей с использованием МЭ

Демилитаризованные зоны

Цель - ознакомить обучающихся с основами проектирования защищенных сетей

Рекомендуемая литература:

1. Руководящий документ Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации
2. Вишневский, В.М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский ; Ин-т пробл.передачи информ.РАН. - М.:Техносфера, 2003. - 506с.
3. Науманн, Ш. Компьютерная сеть. Проектирование, создание, обслуживание : Пер.с нем. / Ш. Науманн, Х. Вер. - М.:ДМК, 2000. - 332с.

Тема 4 Технологии построения распределенных защищенных компьютерных сетей

Единые IP пространства

Цель – ознакомить обучающихся с современными распределенными технологиями доступа к ресурсам сетей и способов их организации.

Оверлейные сети.

Цель – ознакомить обучающихся с современными промышленными сетями, оверлейными сетями и технологиями их функционирования

Рекомендуемая литература:

1. Вишневский, В.М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский ; Ин-т пробл.передачи информ.РАН. - М.:Техносфера, 2003. - 506с.
2. Науманн, Ш. Компьютерная сеть. Проектирование, создание, обслуживание : Пер.с нем. / Ш. Науманн, Х. Вер. - М.:ДМК, 2000. - 332с.

б) Перечень лабораторных работ

Лабораторная работа №1. VPN L2

Лабораторная работа №2. VPN L3

Лабораторная работа №3. МЭ

Лабораторная работа №4. Сети с DMZ

Рекомендуемая литература:

1. Компьютерные сети. Лабораторный практикум: Учебное пособие / Бабаев С.И., Никифоров М.Б. — М.: КУРС, 2018 — 160 с.
2. Лабораторный практикум по дисциплине Методы и средства защиты информации в компьютерных сетях [Электронный ресурс]/ — Электрон. текстовые данные.— Москва: Московский технический университет связи и информатики, 2015.— 58 с.— Режим доступа: http://www.iprbookshop.ru/61742.html.— ЭБС «IPRbooks»

в) Курсовой проект

В курсовом проекте рассматриваются основные разделы дисциплины, которые были рассмотрены на момент выполнения курсовой работы.

Тема курсового проекта: «Проектирование архитектуры сети специального назначения». Все варианты заданий связаны с разработкой макета сети специального назначения в одном из приложений-эмуляторов сетевого оборудования.

Разрабатываемая архитектура должна удовлетворять:

- требования безопасности, предъявляемым к сетям данного уровня;
- функциональным требованиям технического задания;
- эксплуатационным требованиям;
- требованиям надежности.

Типовые задания:

- Проектирование архитектуры сети паспортного стола
- Проектирование архитектуры сети филиала банка
- Проектирование архитектуры сети промышленного предприятия
- Проектирование архитектуры сети ВУЗа
- Проектирование архитектуры сети управления в сфере экономики
- Проектирование архитектуры сети управления в сфере ОПК

Темы могут быть дополнены актуальными вариантами заданий по темам данного курса.

2. ВОПРОСЫ К ЭКЗАМЕНУ И ЗАЧЕТУ ПО ДИСЦИПЛИНЕ

Вопросы зачета

1. Основы законодательства в области защиты компьютерных сетей
2. Защита КС на этапе их создания
3. АСЗИ классификация

4. Классы защищенности АСЗИ по РД ГРК России (сравнение)
5. Классы защищенности АСЗИ по РД ГРК России (3 группа)
6. Классы защищенности АСЗИ по РД ГРК России (2 группа)
7. Классы защищенности АСЗИ по РД ГРК России (1 группа)
8. СВТ. МЭ. Классификация
9. МЭ. Принципы функционирования
10. МЭ. Классификация
11. МЭ. Принципы применения
12. Основные этапы разработки политики безопасности.
13. Основные нормативные документы по разработке политики безопасности.
14. Назовите защитные механизмы. Как их можно классифицировать?
15. Охарактеризуйте динамический и статический анализ безопасности приложения. В чем их принципиальная разница?
16. Уязвимость информационных систем.
17. Классификация сетевых атак
18. Модели компьютерных систем.
19. Доступ и монитор безопасности.
20. Методологические принципы и организационные мероприятия, реализуемые в процессе защиты информации.
21. Компьютерная система (КС) как объект защиты информации.
22. Эволюция концептуальных основ реализации ее защиты.
23. Общая характеристика случайных и преднамеренных угроз в КС.
24. Состав комплекса стандартов по ЗИ для различных классов ОЗИ;
25. Классификация ОЗИ и группы требований по ЗИ;

Вопросы экзамена

1. Общая характеристика нормативных документов по стандартизации;
2. Правовое регулирование отношений по защите информации в информационных и телекоммуникационных сетях, а также в сети Интернет.
3. Классификация объектов информатизации.
4. Правовой порядок установления соответствия параметров объектов информатизации и средств защиты информации требованиям нормативных документов.
5. Классы безопасности.
6. Политики разграничения доступа.
7. Какова цель защиты корпоративной информационной системы?
8. Назовите защитные механизмы. Как их можно классифицировать?
9. Перечислите основные классификационные схемы уязвимостей. Каковы их основные достоинства и недостатки
10. Какие средства защиты информации применяются на компьютерах в ГИС любых уровней и классов, не подключенных к сетям общего пользования
11. Какие средства защиты информации применяются на компьютерах в ГИС любых уровней и классов подключенных к сетям общего пользования
12. Какие средства защиты информации применяются на компьютерах в ИСПДн любых уровней и классов, не подключенных к сетям общего пользования
13. Какие средства защиты информации применяются на компьютерах в ИСПДн любых уровней и классов, подключенных к сетям общего пользования
14. 2. В случае поступления запросов на получение информации из организаций, не обладающих соответствующими полномочиями что обязан сделать работодатель?
15. 3. Сколько существует уровней защищенности, которые необходимо обеспечить персональным данным в соответствии с постановлением Правительства №1119? Назовите их.
16. Что подлежит проверке при контроле состояния ТКЗИ в организации?
17. 2. Как происходит оценка вероятности(возможности) реализации угроз безопасности информации в степени возможного ущерба согласно ФСТЭК России?
18. 3. Как происходит определение актуальности угрозы безопасности информации согласно ФСТЭК России?
19. Технология VPN
20. VPN L2

21. VPN L3
22. Принципы проектирования сетей
23. Способы размещения сетевых сервисов
24. Демилитаризованные зоны
25. Сеть с DMZ1
26. Сеть с DMZ2
27. Сеть с DMZ3
28. Программные средства защиты КС
29. Пакетные фильтры
30. Оверлейные сети. Обзор
31. Безопасность IPv6
32. Трансляция адресов

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПОДГОТОВКЕ РЕФЕРАТОВ

Реферат представляет собой краткий доклад по определённой теме, в котором собрана информация из одного или нескольких источников. Данный вид работ направлен на более глубокое самостоятельное изучение студентами лекционного материала или рассмотрения вопросов для дополнительного изучения.

Типовые темы рефератов:

- Современные средства сетевой безопасности (аппаратные и программные)
- Высокоскоростные сети и их безопасность
- Современный рынок сетевого оборудования для защиты информации при ее передаче по сети
- Современные МЭ. Возможности. Технологии
- Беспроводные сети. Современные реалии безопасности
- Проектирование сетей. Подходы к обеспечению безопасности
- Промышленные сети.
- Оверлейные сети
- Многопротокольная маршрутизация и коммутация

Темы рефератов могут быть дополнены и изменены в рамках программы курса.

Основные требования к оформлению:

1. Общий объем работы 2- 2,5 п.л. (32-40 стр. стандартного машинописного текста) Реферат должен содержать введение, основную часть с анализом и выводам по рассматриваемому вопросу и обоснованное заключение. Список используемых источников, актуальных на момент написания реферата – не менее 15 наименований.

2. Оформление основного текста в соответствии с ГОСТ 7.32-2017 «Отчет о научно-исследовательской работе. Структура и правила оформления». Оформление библиографического списка в соответствии с ГОСТ 7.1-2003 «Библиографическая запись».

3. Дата отправки на проверку устанавливается преподавателем.