ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.В.03 Безопасность вычислительных сетей

Направление подготовки 10.03.01 Информационная безопасность

Профиль подготовки Безопасность автоматизированных систем

Квалификация выпускника бакалавр

Форма обучения очная

СОДЕРЖАНИЕ

1. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1.1. Организационно-методические данные дисциплины

№ п.п.	Наименование темы	Общий объем часов по видам самостоятельной работы				
		подготовка курсового проекта (работы)	подготовка реферата/эссе	индивидуальные домашние задания (ИДЗ)	самостоятельное изучение вопросов (СИВ)	подготовка к занятиям (ПкЗ)
1	2	3	4	5	6	7
2	Основы вычислительных сетей. Сетевая архитектура.	-	-	-	15	5
3	Технологии обеспечения безопасности в сетях Типовые угрозы сетевой безопасности.	-	-	-	7	3
4	Построение защищенных сетей на базе сетевых операционных систем: Сетевые операционные системы (ОС) NetWare, Windows, UNIX.	-	-	-	8	2
5	Глобальная сеть Интернет.	-	-	-	6	2
6	Безопасности сети Интернет.	-	-	-	3	2
7	Комплексная защита подключения к Интернет.	-	-	-	3	-

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1 Основы вычислительных сетей. Сетевая архитектура.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Разделение кода и данных между процессами. Экспорт и импорт функций.

2.2 Технологии обеспечения безопасности в сетях Типовые угрозы сетевой безопасности

При изучении вопроса необходимо обратить внимание на следующие особенности.

Угрозы безопасности ВС. Классификация угроз безопасности ВС. Наиболее распространенные угрозы.

2.3 Построение защищенных сетей на базе сетевых операционных систем: Сетевые операционные системы (ОС) NetWare, Windows, UNIX

При изучении вопроса необходимо обратить внимание на следующие особенности.

Требования к защите ВС. Понятие защищенной ВС. Подходы к организации защиты.

2.4 Глобальная сеть Интернет.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Анализ атаки «Переполнение буфера системного приложения» и способов защиты от неё.

2.5 Безопасности сети Интернет.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Взлом паролей и защита от взлома.

2.6 Комплексная защита подключения к Интернет.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Взлом паролей UNIX и защита от взлома

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 Основы вычислительных сетей. Сетевая архитектура.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Разделение кода и данных между процессами. Экспорт и импорт функций.

3.2 Технологии обеспечения безопасности в сетях Типовые угрозы сетевой безопасности

При изучении вопроса необходимо обратить внимание на следующие особенности.

Угрозы безопасности ВС. Классификация угроз безопасности ВС. Наиболее распространенные угрозы.

3.3 Построение защищенных сетей на базе сетевых операционных систем: Сетевые операционные системы (ОС) NetWare, Windows, UNIX

При изучении вопроса необходимо обратить внимание на следующие особенности.

Требования к защите ВС. Понятие защищенной ВС. Подходы к организации защиты.

3.4 Глобальная сеть Интернет.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Анализ атаки «Переполнение буфера системного приложения» и способов защиты от неё.

3.5 Безопасности сети Интернет.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Взлом паролей и защита от взлома.

4.Темы курсовых работ (проектов)

1. Анализ системы безопасности вычислительных сетей класса Windows, стратегий ее использования.
2. Анализ системы безопасности вычислительных сетей клона Unix и стратегий ее

использования.

3. Для систем клона Unix предполагается решение следующих практических задач: настройка защищенной конфигурации web-портала с использованием средств разграничения прав доступа;
4. Редактирование регистрационных записей и настройка пользователей;
5. Разработка программы определяющей сетевое имя и ip-адрес компьютера (рабочей станции).
6. Настройка комплексной защиты сервера с использованием расширенных атрибутов;
7. Организация разделения дискового пространства между пользователями с использованием механизма квот;
8. Настройка ограничения ресурсов, используемых в процессе работы, для заданной группы пользователей;
9. Настройка межсетевого экрана с заданными требованиями к безопасности;
10. Безопасная настройка сервиса SSH с учетом уязвимостей в версии SSH 1.0.