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

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1. Б.2. 05 Обеспечение информационной безопасности на критически важных объектах

Направление подготовки (специальность) 10.05.03 Информационная безопасность автоматизированных систем

Профиль образовательной программы Информационная безопасность автоматизированных систем критически важных объектов

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
1	**Тема 1** Основные сведения о КВО и КВИС как об объектах защиты					2
2	**Тема 2** Нормативная правовая база РФ в области обеспечения безопасности КВО					2
3	**Тема 3** Архитектура сети критически важного объекта и ее уязвимости					2
4	**Тема 4** Модель угроз критически важного объект					2
5	**Тема 5** Специальные средства защиты ИТ-инфраструктур КВО					2
6	**Тема 6** Комплексная защита критически важных объектов					2
7	**Тема 7** Средства защиты информации, использующиеся на критически важных объектах и в автоматизированных системах критически важных объектов					2
8	**Тема 8** Разработка и реализация планов реагирования и восстановления после инцидентов безопасности критически важного объекта					2
9	**Тема 9** Построение системы защиты информации на критически важном объекте.					2
	Итого:					18

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 Лабораторная работа 1 «Изучение «Доктрины информационной безопасности».»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Общие положения Доктрины
2. Основные информационные угрозы и состояние информационной безопасности
3. Организационные основы обеспечения информационной безопасности

3.2 Лабораторная работа 2-3 «Изучение руководящих документов ФСТЭКРФ.»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Общие положения
2. Требования к организации защиты информации в автоматизированной системе управления
3. Определение класса защищенности автоматизированной системы управления

3.3 Лабораторная работа 4-5 «Изучение «Базовой модели угроз безопасности информации в ключевых системах информационной инфраструктуры»»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

Секретно

3.4 Лабораторная работа 6-7 «Изучение «Методики определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

Секретно

3.5 Лабораторная работа 8-9 «Изучение «Общих требований по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

Секретно

3.6 Лабораторная работа 10 «Категорирование критически важных объектов»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Основные термины и определения
2. Состав и содержание исходных данных для проведения расчетов

3.7 Лабораторная работа 11 «Оценка уязвимости объектов информационной и телекоммуникационной инфраструктуры и объектов информатизации от актов незаконного вмешательства и деструктивных информационных воздействий.»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Основные понятия
2. Особенности обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры

3.8 Лабораторная работа 12 «Разработка требований к оформлению концепции обеспечения информационной безопасности объекта.»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Общие положения. Объекты защиты. Основные угрозы.
2. Основные положения технической политики в обеспечении безопасности информации
3. Принципы построения комплексной системы защиты

3.9 Лабораторная работа 13 «Разработка требований безопасности при взаимодействии с открытыми (публичными) информационными системами и сетями.»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Требования по ограничению доступа к сетевым конференциям
2. Требования по организации электронной почты
3. Требования по антивирусной защите

3.10 Лабораторная работа 14 «Определение конкретных способов реагирования на инциденты различной длительности и тяжести.»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Основные термины и определения
2. Рекомендации по планированию в рамках системы менеджмента инцидентов ИБ
3. Рекомендации по реализации в рамках системы менеджмента инцидентов ИБ

3.11 Лабораторная работа 15 «Определение информационных и технических ресурсов, подлежащих защите»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Категории защищаемой информации
2. Критерии присвоения информации категорий

3.12 Лабораторная работа 16-17 «Разработка рекомендаций по выбору средств защиты информации»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Цель применения СЗИ НСД и какие задачи необходимо решать с их помощью
2. Какие СЗИ НСД существуют на рынке и какие из них удовлетворяют заданным требованиям и подходят под принятую в организации технологию обработки данных