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

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.В.ДВ.06.02 Системы обнаружения вторжений

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация 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 (*из табл. 5.1 РПД*)				
		подготовка курсового проекта (работы)	подготовка реферата/эссе	индивидуальные домашние задания (ИДЗ)	самостоятельное изучение вопросов (СИВ)	подготовка к занятиям (ПкЗ)
	2	3	4	5	6	7
1	Основные элементы технологий открытых информационных систем.	-	-	-	9	
2	Совместимость, переносимость и способность взаимодействовать открытых систем. Основные модели открытых систем.	-	-	-	9	
3	Уязвимость открытых систем на примере интранета. Базовые понятия. Основные угрозы. Уязвимость архитектуры клиент-сервер.	-	-	-	9	
4	Уязвимость открытых систем на примере интранета. Уязвимости системных утилит, команд, сервисов.	-	-	-	9	
5	Уязвимости современных технологий программирования. Ошибки в	-	-	-	9	

	ПО					
6	Принципы создания защищенных средств связи объектов в открытых системах	-	-	-	9	
7	Политика безопасности открытых систем.	-	-	-	9	
8	Управление безопасностью открытых систем	-	-	-	9	

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1 Основные элементы технологий открытых информационных систем.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Основные понятия и определения. Статистика вторжений на Web-ресурсы.

2.2 Совместимость, переносимость и способность взаимодействовать открытых систем. Основные модели открытых систем.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Проблемы обеспечения безопасности при удалённом доступе. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.

2.3 Уязвимость открытых систем на примере интранета. Базовые понятия. Основные угрозы. Уязвимость архитектуры клиент-сервер.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Обнаружение факта проведения и причин возникновения сетевой атаки подручными средствами. Дидактическая единица: Общие сведения об IDS snort.

2.4 Уязвимость открытых систем на примере интранета. Уязвимости системных утилит, ко-манд, сервисов.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Значение IDS для решения задач поиска злоумышленников в собственной ЛВС. Классификация, средства и методы защиты от атак.

2.5 Уязвимости современных технологий программирования. Ошибки в ПО.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Идентификация и аутентификация. Ознакомление с криптографическими системами. Экранирование, анализ защищенности.

2.6 Принципы создания защищенных средств связи объектов в открытых системах.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Виртуальные частные сети. Туннелирование. Сетевые уязвимости.

2.7 Политика безопасности открытых систем.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Типы угроз. Классификация атак по основным механизмам реализации угроз. Сетевые сканеры. Особенности сетевого сканера Nessus.

2.8 Управление безопасностью от-крытых систем.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Защита программ от изучения. Защита от разрушающих программных воздействий.