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

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.В.ДВ.06.01 Технология защиты информации в различных отраслях деятельности

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)
1	2	3	4	5	6	7
1	Основные понятия и определения.	-	-	-	2	2
2	Системный подход к построению систем обеспечения информационной безопасности	-	-	-	2	2
3	Структура органов государственной власти РФ	-	-	-	2	2
4	Роль стандартизации в регулировании области обеспечения ИБ	-	-	-	2	2
5	Сравнение модели стека протоколов TCP/IP с моделью OSI	-	-	-	2	2
6	Флаги TCP-пакета	-	-	-	4	4
7	Проблемы и задачи, разрешаемые криптографическими методами	-	-	-	4	4
8	DES и его модификации	-	-	-	2	2
9	Основные протоколы IPSec.	-	-	-	2	4
10	Схема реализации систем безопасности в ОС Windows Server	-	-	-	4	2
11	Встроенные средства безопасности NTFS	-	-	-	2	2
12	Классификация нарушителей в зависимости от целей и мотивов атак	-	-	-	2	2
13	Утилиты удаленного	-	-	-	4	4

	администрирования					
14	Уязвимости ОС при наличии неограниченного физического доступа к аппаратной платформе	-	-	-	2	2

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1 Определение понятия «информция, ее существенные признаки.

Определение понятия информация, ее существенные признаки. Основные виды информации.

2.2 Системный подход к построению систем обеспечения информационной безопасности.

Системный подход к построению систем обеспечения информационной безопасности. Составляющие модели ИБ: основы, направления, этапы. Сводная матрица задач реализации модели ИБ.

Угрозы, их классификация: объективные (естественные) и субъективные (непреднамеренные и преднамеренные).

2.3 Структура органов государственной власти РФ.

Информационное право: предмет и методы отрасли.

Нормативно-правовое обеспечение защиты информации: законы, федеральные и локальные нормативные акты.

2.4 Роль стандартизации в регулировании в области обеспечения ИБ.

Серия стандартов ISO/IEC (ИСО/МЭК) 27000.

Стандарты ИТ: ITIL, ISO/IEC 20000. Оценка безопасности: стандарты ISO/IEC 15408, CobIT

Политика РФ в области лицензирования и технического регулирования

2.5 Сравнение модели стека протоколов TCP/IP с моделью OSI.

Общие понятия. Протокол. Стек протоколов. Протоколы взаимодействия приложений и протоколы транспортной подсистемы.

Стек протоколов TCP/IP

Сетевая модель OSI

2.6 Флаги TCP-пакета.

Трехступенчатая процедура установления соединения в протоколе TCP

Процедуры разрыва TCP-соединения

2.7 Проблемы и задачи, разрешаемые криптографическими методами.

Основные алгоритмы шифрования, используемые для защиты информации в компьютерных сетях.

2.8 DES и его модификации.

Виды атак: Атака Винера на RSA, атаки на RSA основанные на решетках, атака Хостада, атака Франклина-Рейтера, частичное раскрытие ключа. Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость со случайным оракулом. Доказуемая стойкость без случайного оракула

2.9 Основные протоколы IPSec.
Прозрачность IPSec для конечных пользователей и приложений. Защита от изменения данных. Глубокая защита протоколов и приложений верхнего уровня. Основные протоколы IPSec: Authentication Header (AH) и Encapsulating Security Payload (ESP). Уровень реализации IPSec

2.10 Схема реализации систем безопасности в ОС Windows Server.
Настройка шифрования в Windows Server.
Навык шифрования в Windows Server.

2.11 Встроенные средства безопасности NTFS.
Виды разграничения доступа. Комбинация прав доступа к сетевым файловым ресурсам и доступа к объектам NTFS.
Организация сетевого доступа к папкам. Виды разграничения доступа. Комбинация прав доступа к сетевым файловым ресурсам и доступа к объектам NTFS

2.12 Классификация нарушителей в зависимости от целей и мотивов атак.
Классификация нарушителей в зависимости от целей и мотивов атак

2.13 Утилиты удаленного администрирования.
Утилиты удаленного администрирования (консольный доступ): текстовая и графическая консоли

2.14 Уязвимости ОС при наличии неограниченного физического доступа к аппаратной платформе.
Уязвимости ОС при наличии неограниченного физического доступа к аппаратной платформе

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 Основные понятия и определения. Законодательные и правовые основы защиты компьютерной информации и информационных технологий
При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Законодательные и правовые основы защиты компьютерной информации и информационных технологий
3.2 Энтропия, теоретическая и практическая стойкость, вычислительная стойкость.
При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Основные понятия и определения области знаний ИБ (политика ИБ, аутентификация, авторизация, аудит). Компоненты сетевой безопасности

(межсетевой экран, DMZ, NAT, IDS/IPS, прокси-сервер, DLP, NAC, VPN, Honeypot).

3.3 Спецификации Internet-сообщества IPsec.

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Архитектура средств безопасности IP-уровня. Контексты безопасности и управление ключами. Протокольные контексты и политика безопасности. Обеспечение аутентичности IP-пакетов. Обеспечение конфиденциальности сетевого трафика

3.4 Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей.

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Основные понятия и идеи стандарта FIPS 140-2. Требования безопасности. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация. Требования безопасности. Модель в виде конечного автомата, физическая безопасность. Требования безопасности. Эксплуатационное окружение, управление криптографическими ключами

3.5 Взаимодействие компьютеров в сети

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Требования безопасности. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации

3.6 RFC 4291 — Архитектура шестой версии протокола межсетевого обмена в Internet (IPv6-адресация)

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Общие понятия. Протокол. Стек протоколов. Протоколы взаимодействия приложений и протоколы транспортной подсистемы.

3.7 Основные алгоритмы шифрования, используемые для защиты информации в компьютерных сетях

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Групповые IPv6-адреса. Предварительно назначенные групповые IPv6-адреса. IPv6-адреса, которые IP-узел должен распознавать. Вопросы безопасности

3.8 Тесты на простоту и факторизация. Надежность криптосистем. Элементы криптоанализа

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Основные алгоритмы шифрования, используемые для защиты информации в компьютерных сетях.

3.9 Возможности протокола IPSec

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Виды атак: Атака Винера на RSA, атаки на RSA основанные на решетках, атака Хостада, атака Франклина-Рейтера, частичное раскрытие ключа. Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость со случайным оракулом. Доказуемая стойкость без случайного оракула

3.10 Реализация IPSec компанией Microsoft в Windows Server

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Прозрачность IPSec для конечных пользователей и приложений. Защита от изменения данных. Глубокая защита протоколов и приложений верхнего уровня
Физическое расположение копий реестра. Резервная копия.
Утилиты работы с реестром Windows.

3.11 Операции импорта-экспорта ветвей реестра.

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Консоль настройки IPSec, ее интерфейс. Способы безопасной передачи данных в IPSec.

3.12 Механизмы контроля на примере IDS и IPS-систем. Система журналирования в ОС Windows. Определение понятия. Типы объектов журналирования.

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Механизмы ограничения доступа к реестру Windows
Объект GPO. Последовательность действия политик. Результирующая политика.

3.13Базовые понятия: вирусы, сетевые черви, «троянские кони», вредоносное ПО (Malware), Adware, СПАМ, фишинг.

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Классификация событий, журналируемых в ОС Windows. Утилиты работы с системными журналами ОС Windows. Структура записи о событии. Обязательные поля. Настройка аудита событий через GPO и локальную групповую политику.
Требования безопасности. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации

3.14 Способы идентификации доступных сетевых сервисов и версий ОС хостов.

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Условия распространения вирусов: популярность, документированность, наличие уязвимостей ОС. Средства противодействия вирусов антивирусным программам.
Обзор современного антивирусного программного обеспечения.

3.15 Межсетевые экраны: классификация, механизм работы и схемы установки.

Тенденции вирусных угроз и развития антивирусного ПО

Системы обнаружения и предотвращения вторжений. Схемы мониторинга инцидентов ИБ и реакции на них.

При подготовке к занятию необходимо обратить внимание на следующие

особенности.

Основные этапы и средства получения информации о сети: Network Reconnaissance, Mapping the Network, Sweeping the Network, Scanning the Network. Scanning the Network: основные источники информации, механизмы сканирования портов, утилиты сканирования Атаки, основанные на уязвимостях: получение контроля, DoS-атаки.