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

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.В.09 Информационная безопасность

Специальность: 38.05.01 Экономическая безопасность
Специализация: Экономико-правовое обеспечение экономической безопасности
Форма обучения: заочная

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	**Раздел 1. Информационная безопасность и уровни её обеспечения. Компьютерные вирусы и защита от них**				30	18
1.1.	Тема 1 Понятие «Информационная безопасность». Составляющие информационной безопасности				6	9
1.2.	Тема 2 Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»				6	9
1.3.	Тема 3 Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ				6	
1.4.	Тема 4 Административный уровень обеспечения информационной безопасности. Классификация угроз «Информационной безопасности»				6	
1.5.	Тема 5 - Классификация компьютерных вирусов и характеристика вирусоподобных программ. Антивирусные программы и профилактика компьютерных вирусов				6	
2.	**Раздел 2. Информационная безопасность вычислительных сетей. Механизмы обеспечения информационной безопасности**				30	18
2.1.	Тема 6 - Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях.				8	9
2.2.	Тема 7 Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей				6	9
2.3	Тема 8 - Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа.				8	
2.4	Тема 9 Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN)				8	
3.	**Самостоятельная работа**				60	36

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1. Основы обеспечения информационной безопасности предприятия

При изучении вопроса необходимо обратить внимание в чем заключается проблема информационной безопасности. На составляющие информационной безопасности

2.2. Основные способы защиты информации предприятия

При изучении вопроса необходимо обратить внимание на уровни формирования режима информационной безопасности. Особенности уровней формирования режима информационной безопасности.

2.3. Структура информационного законодательства

При изучении вопроса необходимо обратить внимание на основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации; ответственность за нарушения в сфере информационной безопасности.

2.4 Информационно-правовые нормы международных актов

При изучении вопроса необходимо обратить внимание на информационно-правовые нормы международных актов

2.5 Стандарты информационной безопасности распределенных систем

При изучении вопроса необходимо обратить внимание на основное содержание стандартов по информационной безопасности распределенных систем;

основные сервисы безопасности в вычислительных сетях;

наиболее эффективные механизмы безопасности;

2.6 Стандарты информационной безопасности в РФ

При изучении вопроса необходимо обратить внимание на основное содержание оценочного стандарта ISO/IEC 15408;

отличия функциональных требований от требований доверия;

классы функциональных требований и требований доверия.

2.7 . Административный уровень обеспечения информационной безопасности

При изучении вопроса необходимо обратить внимание на задачи информационной безопасности;

уровни формирования режима информационной безопасности;

особенности законодательно-правового и административного уровней;

2.8 Классификация угроз «Информационной безопасности»

При изучении вопроса необходимо обратить внимание на классы угроз информационной безопасности; причины и источники случайных воздействий на информационные системы; каналы несанкционированного доступа к информации.

2.9 . Характерные черты компьютерных вирусов

При изучении вопроса необходимо обратить внимание на классы компьютерных вирусов и их характеристику. Изучить характерные черты и деструктивные возможности "вирусоподобных" программ.

2.10 Особенности работы антивирусных программ. Классификация антивирусных программ

При изучении вопроса необходимо обратить внимание на основные понятия по борьбе с вирусами, виды антивирусных программ и их характеристику.

Изучить основы профилактики компьютерных вирусов, пути проникновения вирусов в компьютеры и основные правила защиты от компьютерных вирусов

2.11 Особенности обеспечения информационной безопасности в компьютерных сетях

При изучении вопроса необходимо обратить внимание на задачи информационной безопасности; уровни формирования режима информационной безопасности; особенности законодательно-правового и административного уровней;

2.12 Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика

При изучении вопроса необходимо обратить внимание на классы удаленных угроз и их характеристику. Типовые удаленные атаки и механизмы их реализации

2.13 Причины успешной реализации удаленных угроз в вычислительных сетях.

При изучении вопроса необходимо обратить внимание на причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях. Принципы защиты распределенных вычислительных сетей

2.14 Принципы защиты распределенных вычислительных сетей

При изучении вопроса необходимо обратить внимание на причины успеха удаленных атак и принимать меры к их устранению. Использование принципов защиты для разработки и реализации механизмов защиты вычислительных сетей

2.15 Идентификация и аутентификация. Криптография и шифрование

При изучении вопроса необходимо обратить внимание на механизмы идентификации и аутентификации; идентификаторы, используемые при реализации механизма идентификации и аутентификации; структуру криптосистемы; методы шифрования данных.

2.16 Методы разграничения доступа.

При изучении вопроса необходимо обратить внимание на механизм электронной цифровой подписи. Методы разграничения доступа. Мандатное и дискретное управление доступом

2.17Регистрация и аудит. Межсетевое экранирование.

При изучении вопроса необходимо обратить внимание на механизм межсетевого экранирования; составляющие технологии виртуальных частных сетей.

2.18 Технология виртуальных частных сетей (VPN)

При изучении вопроса необходимо обратить внимание на сущность и содержание технологии виртуальных частных сетей

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 Понятие «Информационная безопасность». Составляющие информационной безопасности

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания

- Доступность информации
- Целостность информации
- Конфиденциальность информации

3.2.Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»

При подготовке к занятию необходимо обратить внимание на ключевые моменты и на более сложные из них для лучшего запоминания:

основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

- ответственность за нарушения в сфере информационной безопасности

3.3 Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях.

При подготовке к вопросам необходимо акцентировать внимание на следующем:

- Специфика средств защиты в компьютерных сетях

3.4 Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей

При подготовке к вопросам необходимо акцентировать внимание на следующем:

- Причины успешной реализации удаленных угроз в вычислительных сетях

Разработал(а): _____ О.Я. Набокина