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

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.Б.16 Криптографические методы защиты информации

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	Классификация криптографических систем	-	-	-	2	6
3	Простые шифры и их свойства	-	-	-	2	6
4	Симметричные системы шифрования (системы шифрования с секретным ключом)	-	-	-	2	6
5	Системы шифрования с открытым ключом	-	-	-	2	6
6	Поточные системы шифрования	-	-	-	2	6
7	Электронно-цифровая подпись	-	-	-	2	8
8	Протоколы идентификации	-	-	-	4	6
9	Протоколы управления ключами	-	-	-	2	6
10	Современные достижения науки и техники в области современной криптографии				2	6

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1 Законодательные и правовые основы защиты компьютерной информации и информационных технологий

При изучении вопроса необходимо обратить внимание на следующие особенности.

Основные понятия и определения в криптографии

2.2 Модульная арифметика

При изучении вопроса необходимо обратить внимание на следующие особенности.

Энтропия в криптографии

2.3 Схемы обмена секретными ключами: широкоротой лягушки, Ниджейма-Шредера, Отвэй-Риса

При изучении вопроса необходимо обратить внимание на следующие особенности.

Блочные и поточные шифры

2.4 Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Поточные шифры

2.5 Цифровые сертификаты и инфраструктура открытых ключей

При изучении вопроса необходимо обратить внимание на следующие особенности.

Общая схема функционирования систем с открытыми ключами

2.6 Цифровые сертификаты и инфраструктура открытых ключей

При изучении вопроса необходимо обратить внимание на следующие особенности.

Криптосистема RSA и ее модификации

2.7 Тесты на простоту: пробное деление, тест Ферма, тест Миллера-Рабина. Алгоритмы факторизации: пробное деление, гладкие числа, (P-1)-метод Полларда, разность квадратов, современные методы факторизации.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля

2.8 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

При изучении вопроса необходимо обратить внимание на следующие особенности.

Тесты на простоту и факторизация

2.9 Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость со случайным оракулом. Доказуемая стойкость без случайного оракула

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 Основные понятия и определения в криптографии

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Основные понятия и определения.

- История развития криптографии. Классификация криптографических систем.

3.2 Стойкость криптографических систем и алгоритмов

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Энтропия, теоретическая и практическая стойкость, вычислительная стойкость.
- Теоретико-информационная стойкость.

3.3 Вычислительные алгоритмы

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Модульная арифметика.
- Примеры вычислений по модульной арифметики.

3.4 Шифры DES, режимы работы DES, AES, ГОСТ 28147-89

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Шифры DES.
- Режимы работы шифров.

3.5 Поточные шифры: РСЛОС, RC4, шифр Рона

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Характеристика шифров.
- Режимы работы шифров.

3.6 Распределение ключей

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Схема обмена ключами.
- Основные схемы обмена ключами.

3.7 Общая схема функционирования систем с открытыми ключами

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Понятие открытого ключа.
- Схема функционирования систем с открытым ключом.

3.8 Криптосистема RSA и ее модификации. Криптосистема Эль Гамаля. Криптосистема Рабина

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Криптосистема RSA и ее модификации.
- Криптосистема Эль Гамаля.

- Криптосистема Рабина.