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

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.Б.1.26 Криптографические методы защиты информации

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				
		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	Классификация криптографических систем	-	-	-	4	8
2	Простые шифры и их свойства	-	-	-	4	10
3	Симметричные системы шифрования (системы шифрования с секретным ключом)	-	-	-	4	8
4	Системы шифрования с открытым ключом	-	-	-	4	10
5	Общая схема функционирования систем с открытыми ключами	-	-	-	4	10
6	Криптосистема RSA и ее модификации	-	-	-	4	8
7	Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля	-	-	-	4	8
8	Тесты на простоту и факторизация	-	-	-	2	10
					30	72

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

5.1 **Классификация криптографических систем**

При изучении вопроса необходимо обратить внимание на следующие особенности.

Законодательные и правовые основы защиты компьютерной информации и информационных технологий

5.2 Простые шифры и их свойства.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Модульная арифметика

5.3 Симметричные системы шифрования (системы шифрования с секретным ключом).

При изучении вопроса необходимо обратить внимание на следующие особенности.

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

5.4 Системы шифрования с открытым ключом.

При изучении вопроса необходимо обратить внимание на следующие особенности.

Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний.

5.5 Общая схема функционирования систем с открытыми ключами

При изучении вопроса необходимо обратить внимание на следующие особенности.

Цифровые сертификаты и инфраструктура открытых ключей

5.6 Криптосистема RSA и ее модификации

При изучении вопроса необходимо обратить внимание на следующие особенности.

Цифровые сертификаты и инфраструктура открытых ключей

5.7 Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля.

При изучении вопроса необходимо обратить внимание на следующие особенности.

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.

5.8 Тесты на простоту и факторизация

При изучении вопроса 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.

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 **ПЗ № 1-2** Поточные системы шифрования (РСЛОС, RC4, Рона) к занятию необходимо обратить внимание на следующие моменты.

1. Основные понятия и определения.
2. История развития криптографии. Классификация криптографических систем.

6.2 **ПЗ № 3-4** Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)
При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Модульная арифметика.
2. Примеры вычислений по модульной арифметики.

6.3 ПЗ № 5-6 Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Понятие открытого ключа.
2. Схема функционирования систем с открытым ключом.

6.4 ПЗ № 7-8 Асимметричные криптосистемы (***RSA***, ElGamal, Рабина) Формирование ассиметричных криптосистем

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Характеристика шифров.
2. Режимы работы шифров.

6.5 ПЗ № 9 Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Схема обмена ключами.
2. Основные схемы обмена ключами.