РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Теория информации и теория кодирования

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в магистратуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 01.04.02 «Прикладная математика и информатика». Направленность (профиль) «Дискретные структуры и алгоритмы». Образовательная программа «Информационная безопасность компьютерных систем».

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть магистерской образовательной программы «Информационная безопасность компьютерных систем», изучается в 2-м семестре.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
Способность использовать терминологию в облас математического аппарата теории кодирования, основны утверждения из теории групп, арифметики конечных полей полиномв, используемых в теории кодирования; владен	З1 (СПК-57) Знать: математический аппарат теории кодирования, основные понятия и утверждения теории групп, арифметики конечных полей и полиномов У1 (СПК-57) Уметь

навыками анализа параметров линейных кодов и синте алгоритмов их декодирования(СПК-57).	уметь использовать основные утверждения теории групп, арифметики конечных полей и полиномов для синтеза и анализа линейных кодов, исправляющих ошибки В1 (СПК-57) Владеть навыками анализа параметров линейных кодов

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 2 зачетные единицы, всего 72 часа.

72 часов составляет контактная работа с преподавателем – 72 часf занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 0 часов групповых консультаций, 0 часов мероприятий текущего контроля успеваемости, 0 часа промежуточной аттестации.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по математическому анализу, линейной алгебре, теории групп, теории конечных полей, дискретной математике в объеме, соответствующем основным образовательным программам бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения не используются презентации и компьютерные программы авторской разработки.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе дается общая теория линейных кодов, исправляющих ошибки. Рассматриваются основные классы линейных кодов и их корректирующие возможности. Изучаются вопросы построения алгоритмов декодирования линейных кодов и оценки их эффективности.

Рассматриваются приложения линейных кодов, исправляющих ошибки, в области криптографии.

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	**Всего (часы)**	В том числе							
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						**Самостоятельная работа учащегося, часы** из них	
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости: коллоквиумы, практические контрольные занятия и др.	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п..

					ц и и				
Тема 1. Теория информации и теория кодирования. Информация и энтропия. Условная энтропия и взаимная информация. Дискретный канал передачи сообщений. Скорость передачи информации. Пропускная способность канала. Прямая и обратная теоремы кодирования К.Шеннона.	**12**								
Тема 2. Кодирование источников. Алфавитное кодирование. Стоимость кода относительно распределения. Разделимые и префиксные коды. Неравенство Крафта-	**12**								

Макмиллана. Код К.Шеннона. Теорема об оптимальном коде.									
Тема 3. Линейные коды, исправляющие ошибки. Основные параметры линейных кодов. Теоремы о порождающей и проверочной матрицах. Эквивалентность кодов. Группа автоморфизмов кода. Понятие ортогонального кода. Неравенства Синглтона, Хэмминга, Плоткина, Варшамова-Гилберта. Стандартное расположение кода. Коды с низкой плотностью проверок на четность. Каскадные коды и их параметры	**16**	-							
Тема 4. Коды Рида-Маллера и коды Рида-Соломона. Осповные параметры кодов Рида-Маллера. Замкнутость	**16**								

класса относи тельно операции «ортогональность». Алгоритм декодирования Рида. Быстрое преобразование Адамара. Алгоритм декодирования кодов Рида-Маллера первого порядка. Основные параметры кода Рида-Соломона и алгоритм его декодирования. Криптографические приложения линейных кодов. Криптосистема МакЭллиса. Корреляционно-иммунные функции.									
Тема 5. Циклические и альтернативные коды. Матричное описание циклических кодов. Основные параметры кодов Боуза-Чеудхури-Хоквингема(БЧХ). Теорема о конструктивном расстоянии БЧХ-кодов. Коды Гоппы и их	**16**								

алгоритмы декодирования.									
Промежуточная аттестация – контрольное задание	**-**								
Итого	**72**								

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к практическим заданиям текущего контроля и промежуточной аттестации.

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная учебно-методическая литература

1) Питерсон У. Коды, исправляющие ошибки. МИР, Москва, 1964, с. 338.
2) Мак-Вильямс Ф.Дж., Слоэн Н.Дж,А. Теория кодов, исправляющих ошибки. СВЯЗЬ, Москва, 1979, с.744.

Дополнительная учебно-методическая литература

1) Сидельников В.М. Теория кодирования.ФИЗМАТЛИТ,Москва, 2008, с. 322.
2) Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Булевы функции в теории кодирования и криптологии. ЛЕНАНД, Москва, 2015, с. 576.

Ресурсы информационно-телекоммуникационной сети «Интернет»

Информационные технологии, используемые в процессе обучения

Материально-техническая база

Для преподавания дисциплины требуется класс, оборудованный маркерной или меловой доской.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

к.ф.- м.н., доцент Логачев Олег Алексеевич (logol@iisi.msu.ru)

Приложение

Оценочные средства для промежуточной аттестации по дисциплине «Синтез и анализ криптосистем с открытым ключом»

Промежуточная аттестация состоит из практического контрольного задания, проверяющего приобретенные учащимся знания, умения и навыки.

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ	**КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ из соответствующих карт компетенций**	**ОЦЕНОЧНЫЕ СРЕДСТВА**			
	1	2	3	4	5
	Неудовлетворительно	**Неудовлетворительно**	**Удовлетворительно**	**Хорошо**	**Отлично**
З1 (СПК-57) Знать: математический аппарат криптографии с открытым ключом, основные алгебраические и теоретико-числовые понятия и утверждения	Отсутствие знаний	Фрагментарные представления о математическом аппарате криптографии с открытым ключом, основных алгебраических и теоретико-	В целом сформированные, но неполные знания о математическом аппарате криптографии с открытым ключом, основных алгебраических и теоретико-числовых понятиях и утверждениях.	Сформированные, но содержащие отдельные пробелы знания о математическом аппарате криптографии с открытым ключом, основных алгебраических и теоретико-числовых понятиях и утверждениях.	Сформированные систематические знания о математическом аппарате криптографии с открытым ключом, основных алгебраических и теоретико-числовых понятиях и

		числовых понятиях и утверждениях.			утверждениях.
У1 (СПК-57) Уметь: использовать основные утверждения алгебры, теории чисел для синтеза и анализа криптосистем с открытым ключом	Отсутствие умений	Фрагментарные умения использовать основные утверждения алгебры, теории чисел для синтеза и анализа криптосистем с открытым ключом	В целом сформированное, но не систематическое умение использовать основные утверждения алгебры, теории чисел для синтеза и анализа криптосистем с открытым ключом	Сформированное, но содержащее отдельные пробелы умение использовать основные утверждения алгебры, теории чисел для синтеза и анализа криптосистем с открытым ключом	Сформированное систематическое умение использовать основные утверждения алгебры, теории чисел для синтеза и анализа криптосистем с открытым ключом
В1 (СПК-57) Владеть навыками анализа безопасности криптосистем с открытым ключом	Отсутствие навыков	Фрагментарное владение навыками анализа безопасности криптосистем с открытым ключом	В целом сформированное, но не систематическое владение навыками анализа безопасности криптосистем с открытым ключом	Сформированное, но содержащее отдельные пробелы владение навыками анализа безопасности криптосистем с открытым ключом	Сформированное систематическое владение навыками анализа безопасности криптосистем с открытым ключом

Фонды оценочных средств

Примерное практическое контрольное задание для промежуточной аттестации.

Задание 1. Помогите Маше расшифровать сообщение c=68014, зашифрованное криптосистемой Рабина, если её секретный ключ равен sk=[p=307, q=401], а открытый ключ - pk=[N=pq].

Задание 2. Помогите Ане расшифровать сообщение c=55517, зашифрованное криптосистемой RSA, если её открытый ключ равен pk=[N=80851, e=10703], а секретный ключ равен d=15.

Задание 3. Семен-Редиска знает, что Борис, pk=(N=1415027, e=770531), использует достаточно малый секретный ключ. Помогите Семену найти p и q - делители N.

Задание 4. Помогите Борису построить класс эквивалентности своего секретного ключа RSA: d=112295, p=401, q=317.

Задание 5. Злодей Редиска украл две криптограммы c1=2788 и c2=804. Ему известно, что открытые тексты, соответствующие этим криптограммам, связаны соотношением m2=2m1+1. Помогите Редиске найти m1 и m2, если сообщения предназначались Ане (секретный ключ - N=3379, e=3).

Задание 6. Методом Полига-Хэллмана решить уравнение .

Задание 7. Методом Госпера найти номера двух одинаковых элементов в последовательности .

Задание 8. Построить LLL-приведённый базис решётки

Методические материалы для проведения процедур оценивания результатов обучения

Выполнение каждого практического задания промежуточного контроля может принести максимум 30 баллов, в итоге на промежуточной аттестации, учащийся может набрать максимум 240 баллов. Итоговая сумма, не меньшая 200, соответствует оценке «отлично», от 160 до 199 – оценке «хорошо», от 120 до 159 – оценке «удовлетворительно», меньшая 120 – оценке «неудовлетворительно».