

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ
КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

АЛГЕБРАИЧЕСКАЯ ТЕОРИЯ КОДИРОВАНИЯ

Направление подготовки
(специальность)

[1] 10.03.01 Информационная безопасность
[2] 09.03.01 Информатика и вычислительная техника

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/ В	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
7	3	108	32	16	0		6-24	0	Э
Итого	3	108	32	16	0	0	6-24	0	

АННОТАЦИЯ

В курсе рассматриваются следующие темы:

- основы теории конечных полей;
- линейный блочный код;
- метрические пространства;
- границы кодов
- декодированием по методу максимального правдоподобия
- алгоритм синдромного декодирования линейного кода
- двоичный линейный код Хемминга
- операции над кодами
- коды БЧХ

Знания и практические навыки, полученные в курсе, используются при изучении других дисциплин профессионального цикла, а также при выполнении курсовых и дипломных работ.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Познакомить студентов с алгебраическими вопросами теории кодирования и декодирования, а также с основными типами линейных кодов.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

От студентов требуется владение основными понятиями и аппаратом математического анализа и линейной алгебры в объеме стандартных базовых курсов.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-1.3 [1] – Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	З-ОПК-1.3 [1] – знать методы защиты информации при работе с базами данных, при передаче информации по компьютерным сетям У-ОПК-1.3 [1] – уметь применять методы защиты информации при работе с базами данных, при передаче информации по компьютерным сетям В-ОПК-1.3 [1] – владеть навыками практического применения методов защиты информации при работе с базами данных, при передаче информации по компьютерным сетям

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача	Объект или	Код и наименование	Код и наименование
--------	------------	--------------------	--------------------

профессиональной деятельности (ЗПД)	область знания	профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)	индикатора достижения профессиональной компетенции
экспериментально-исследовательский			
Анализ современных систем и средств защиты объектов критической информационной инфраструктуры	Научоёмкие информационные технологии и системы критической информационной инфраструктуры, функционирующие в условиях существования угроз в информационной сфере и включающие компоненты, подлежащие защите	ПК-2.3 [1] - Способен проводить оценку эффективности систем и средств защиты объектов критической информационной инфраструктуры <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-2.3[1] - Знать методы, способы и средства оценки эффективности систем и средств защиты объектов критической информационной инфраструктуры; У-ПК-2.3[1] - Уметь применять современные методы, способы и средства оценки эффективности систем и средств защиты объектов критической информационной инфраструктуры; В-ПК-2.3[1] - Владеть методиками оценки эффективности систем и средств защиты объектов критической информационной инфраструктуры
Анализ современных систем и средств защиты объектов критической информационной инфраструктуры	Научоёмкие информационные технологии и системы критической информационной инфраструктуры, функционирующие в условиях существования угроз в информационной сфере и включающие компоненты, подлежащие защите	ПК-2.4 [1] - Способен выявлять уязвимости в системах и средствах защиты объектов критической информационной инфраструктуры <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-2.4[1] - Знать основные методы и способы обнаружения уязвимостей в системах и средствах защиты объектов критической информационной инфраструктуры; У-ПК-2.4[1] - Уметь классифицировать обнаруженные уязвимости в системах и средствах защиты объектов критической информационной инфраструктуры; В-ПК-2.4[1] - Владеть методикой обнаружения уязвимостей в системах и средствах защиты

			объектов критической информационной инфраструктуры
проектный			
Сбор и анализ исходных данных для проектирования. Проектирование программных и аппаратных средств (систем, устройств, деталей, программ, баз данных) в соответствии с техническим заданием с использованием средств автоматизации проектирования. Разработка и оформление проектной и рабочей технической документации. Контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам. Проведение предварительного технико-экономического обоснования проектных расчетов. Планирование, проектирование, производство и применение высокотехнологичных компьютерных систем на глобальном рынке.	Вычислительные машины, комплексы, системы и сети; автоматизированные системы обработки информации и управления; системы автоматизированного проектирования и информационной поддержки жизненного цикла промышленных изделий; программное обеспечение средств вычислительной техники и автоматизированных систем (программы, программные комплексы и системы); математическое, информационное, техническое, лингвистическое, программное, эргономическое, организационное и правовое обеспечение перечисленных систем.	ПК-1.1 [2] - Способен разрабатывать требования и в соответствии с ними аппаратные и программные компоненты защищенных высокопроизводительных вычислительных систем <i>Основание:</i> Профессиональный стандарт: 06.003	З-ПК-1.1[2] - Знать: современные требования к аппаратным и программным компонентам защищенных высокопроизводительных вычислительных систем; У-ПК-1.1[2] - Уметь: разрабатывать требования к аппаратным и программным компонентам защищенных высокопроизводительных вычислительных систем; В-ПК-1.1[2] - Владеть: навыками разработки требований и в соответствии с ними аппаратных и программных компонентов защищенных высокопроизводительных вычислительных систем
научно-исследовательский и инновационный			
Изучение научно-	Вычислительные	ПК-1 [2] - Способен	З-ПК-1[2] - Знать:

технической информации, отечественного и зарубежного опыта по тематике исследования. Математическое моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований. Проведение экспериментов по заданной методике и анализ результатов. Проведение измерений и наблюдений, составление описания проводимых исследований, подготовка данных для составления обзоров, отчетов и научных публикаций. Составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок. Участие в составе коллектива исполнителей во внедрении результатов научно-технических исследований в высокотехнологичных сферах экономики и коммерциализации разработок.	машины, комплексы, системы и сети; автоматизированные системы обработки информации и управления; системы автоматизированного проектирования и информационной поддержки жизненного цикла промышленных изделий; программное обеспечение средств вычислительной техники и автоматизированных систем (программы, программные комплексы и системы); математическое, информационное, техническое, лингвистическое, программное, эргономическое, организационное и правовое обеспечение перечисленных систем.	обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности <i>Основание:</i> Профессиональный стандарт: 06.001	основы верификации и аттестации аппаратного и программного обеспечения, стандарты качества и процессов его обеспечения, способы оптимизации, принципы и виды отладки, методы оценки качества, методики постановки экспериментов; У-ПК-1[2] - Уметь: разрабатывать и специфицировать требования, осуществлять составление описания проводимых исследований, подготовку данных для составления обзоров и отчетов, обосновывать принимаемые проектные решения, выполнять эксперименты по проверке корректности решений; В-ПК-1[2] - Владеть: навыками построения моделей объектов профессиональной деятельности с использованием инструментальных средств, навыками тестирования, отладки и верификации
---	---	--	---

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели	Задачи воспитания (код)	Воспитательный потенциал
------------------	-------------------------	--------------------------

воспитания		дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры информационной безопасности (В23)	Использование воспитательного потенциала дисциплин профессионального модуля для формирования базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уроне пользователям.

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практи. (семинары) / Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>7 Семестр</i>						
1	Первый раздел	1-8	16/8/0		25	КИ-8	3-ПК-1, У-ПК-1, В-ПК-1, 3-ПК-1.1, У-ПК-1.1, В-ПК-1.1, 3-ПК-2.3, У-ПК-2.3, В-ПК-2.3, 3-ПК-2.4, У-ПК-2.4, В-ПК-2.4
2	Второй раздел	9-16	16/8/0		25	КИ-16	3-ОПК-1.3, У-ОПК-1.3, В-ОПК-1.3, 3-ПК-1, У-ПК-1, В-ПК-1, 3-ПК-2.3, У-ПК-2.3, В-ПК-2.3, 3-ПК-2.4,

							У-ПК-2.4, В-ПК-2.4
	<i>Итого за 7 Семестр</i>		32/16/0		50		
	Контрольные мероприятия за 7 Семестр				50	Э	3-ПК-2.3, У-ПК-2.3, В-ПК-2.3, 3-ПК-2.4, У-ПК-2.4, В-ПК-2.4

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
КИ	Контроль по итогам
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	<i>7 Семестр</i>	32	16	0
1-8	Первый раздел	16	8	0
	Основы теории конечных полей Идеалы: левые, правые, двусторонние. Примеры. Факторкольцом по идеалу. Гомоморфизмы колец, ядро и образ гомоморфизма. Теоремы о гомоморфизмах. Целостное кольцо, тело. Теорема о связи между полем, телом и целостным кольцом. Главный идеал. Элемент, порождающий (образующий) идеал. Примеры главных идеалов и образующих их элементов. Базис идеала, конечный базис. Теорема Гильберта о базисе. Простое кольцо, простой идеал, максимальный идеал, Утверждения о связи максимального идеала и поля, простого идеала и области целостности, максимального и простого идеала. Кольцо многочленов. Кольцо формальных степенных рядов. Степень многочлена, постоянный многочлен. Умножение и сложение в $R[x]$, $R[[x]]$. Понятие делимости многочленов. Алгоритм деления. Неприводимый многочлен. НОД многочленов. Свойства идеала порожденного многочленом. Факториальное кольцо. Простые элементы кольца. Факториальность кольца главных идеалов. Корень многочлена. Теорема Безу. Кольцо многочленов от нескольких переменных. Поле отношений или поле дробей. Примеры полей: поле рациональных функций, поле формальных рядов Лорана,	Всего аудиторных часов		
		16	8	0
		Онлайн		
		0	0	0

	поле рациональных чисел. Подполе поля, собственное подполе, расширение поля. Теорема об изоморфизме полей. Простое поле. Теорема об изоморфизме простых полей. Метод построения расширений полей. Примеры построения расширений полей по неприводимому многочлену. Теорема Кронекера. Вполне разложимый многочлен. Поле разложения и теорема об их существовании. Поле, полученное присоединением элементов. Теоремы о полях разложения. Расширения поля: простое, алгебраическое, трансцендентное. Степень поля. Теоремы о трансцендентном и алгебраическом расширении. Примеры расширений. Минимальный многочлен элемента. Степень элемента. Конечные и бесконечные расширения. Теоремы о свойствах конечного расширения. Примеры построений конечных расширений. Сепарабельный многочлен. Формальная производная. Критерии сепарабельности. Алгебраически замкнутое поле. Алгебраическое замыкание. Основная теорема алгебры. Конечные поля. Порядок конечного поля. Свойства мультипликативной группы конечного поля. Примитивный элемент поля. Свойства конечного поля. Примеры конечных полей. Автоморфизм Фробениуса. Группа Галуа. Структура подполей конечного поля. Диаграмма подполей. Свойства группы автоморфизмов поля.			
9-16	Второй раздел	16	8	0
	Основы теории кодирования	Всего аудиторных часов		
	Введит Развитие теории кодирования. Способы кодирования. Основные задачи теории кодирования.	16	8	0
	Двоичный симметричный канал с вероятностью ошибки p .	Онлайн		
	Информационные символы. Проверочные символы.	0	0	0
	Кодовое расстояние.			
	Понятие метрического пространства. Метрика Хемминга на n -мерном векторном пространстве над полем F , вес Хемминга. Норма. Пространство Джонсона.			
	Линейный блочный код над полем F . Проверочная и порождающая матрицы линейного кода. Проверочные уравнения. Связь проверочной и порождающей матрицы.			
	Каноническая запись порождающей матрицы.			
	Алгоритм кодирования. Кодовое слово, вектор ошибки.			
	Систематический линейный код. Примеры кодов.			
	Эквивалентные коды. Доказать, что каждый линейный код эквивалентен систематическому линейному коду.			
	Декодирование по методу максимального правдоподобия. Декодирование в ближайшее кодовое слово.			
	Минимальное расстояние линейного кода. Утверждение о равенстве минимального расстояния линейного кода наименьшему весу ненулевого кодового слова.			
	Шар радиуса r . Понятие кода, исправляющего t ошибок и			

	обнаруживающего s ошибок. Доказать, что линейный код $C \subset V_n(q)$ с минимальным расстоянием d исправляет $\lfloor (d-1)/2 \rfloor$ и обнаруживает $d-1$ ошибок. Ошибка декодирования. Понятия полного и неполного декодирования. Вероятность ошибки $p_{\text{ош}}$ метода декодирования. Пропускная способность двоичного симметричного канала с вероятностью ошибки p. Теорема Шеннона о существовании кодов. Двойственный (дуальный, ортогональный) код. Доказать, что если $C \subseteq (n, k)$ - код, $k = \dim_{F_q} C$, то код $C^\perp$ является линейным кодом над полем F_q размерности $n-k$. Слабо и строго самодуальные коды. Границы кодов. Граница Хемминга или граница сферической упаковки. Теорема Варшавова-Гилберта. Граница Плоткина. Совершенный и его свойства. Квазисовершенный код и его свойства. Смежный класс по подпространству C пространства $V_n(q)$. Факторпространство $V_n(q)/C$. Лидер смежного класса. Таблица стандартного расположения кода. Синдром вектора и его свойства. Алгоритм синдромного декодирования линейного кода. Существование взаимно однозначного соответствия между смежными классами и синдромами. Интерпретация синдрома для двоичных линейных кодов. Алгоритм неполного декодирования, использующий стандартное расположение. Двоичный линейный код Хемминга H_m длины 2^m-1. Доказать, что: H_m есть $(2^m-1, 2^m-1-m, 3)$-кодом, который исправляет ошибки веса 1 и обнаруживает ошибки веса 2. Доказать, что H_m является совершенным кодом, исправляющим одну ошибку. Алгоритм декодирования кода Хемминга H_m. Обобщенный код Хемминга над F_q. Распределение весов и нумератор весов кода. Тождество Мак-Вильямс и его эквивалентная форма. Операции над кодами. Добавление общей проверки на четность. Выкалывание кодовых координат. Код с выбрасыванием. Пополнение кода путем добавления новых кодовых слов. Удлиненный код. Двоичный симплексный код. Код Рида-Маллера первого порядка. Коды БЧХ, исправляющие 2 ошибки. Алгоритм декодирования кодов БЧХ, исправляющих 2 ошибки. е здесь подробное описание пункта			
--	--	--	--	--

Сокращенные наименования онлайн опций:

Обозначение	Полное наименование
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы

АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Основными образовательными технологиями в освоении дисциплины являются традиционные лекции и работа на семинарах. Дополнительное оборудование и программное обеспечение не требуется.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	Индикаторы освоения	Аттестационное мероприятие (КП 1)
ОПК-1.3	З-ОПК-1.3	КИ-16
	У-ОПК-1.3	КИ-16
	В-ОПК-1.3	КИ-16
ПК-2.3	З-ПК-2.3	Э, КИ-8, КИ-16
	У-ПК-2.3	Э, КИ-8, КИ-16
	В-ПК-2.3	Э, КИ-8, КИ-16
ПК-2.4	З-ПК-2.4	Э, КИ-8, КИ-16
	У-ПК-2.4	Э, КИ-8, КИ-16
	В-ПК-2.4	Э, КИ-8, КИ-16
ПК-1	З-ПК-1	КИ-8, КИ-16
	У-ПК-1	КИ-8, КИ-16
	В-ПК-1	КИ-8, КИ-16
ПК-1.1	З-ПК-1.1	КИ-8
	У-ПК-1.1	КИ-8
	В-ПК-1.1	КИ-8

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех	Оценка	Требования к уровню освоению
--------------	----------------	--------	------------------------------

	балльной шкале	ECTS	учебной дисциплины
90-100	5 – «отлично»	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «хорошо»	B	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «удовлетворительно»	E	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64			
Ниже 60	2 – «неудовлетворительно»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Л 25 Алгебра и теория чисел. Группы, кольца и поля : учебное пособие для вузов, Ларин С. В., Москва: Юрайт, 2023
2. 512 Л55 Конечные поля Т.2 , Лидл Р. , Москва: Мир, 1988
3. 621.39 М15 Теория кодов, исправляющих ошибки : , Мак-Вильямс Ф.Дж., Слоэн Н.Дж., М.: Связь, 1979

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 519 С13 Введение в алгебраические коды : учебное пособие, Сагалович Ю.Л., Москва: ИППИ, 2010

2. 512 Г 95 Конечные поля и группы перестановок: приложение в теории кодирования и комбинаторике : учебное пособие, Гуров С. И., Москва: Книжный дом "Университет", 2018

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

<https://online.mephi.ru/>

<http://library.mephi.ru/>

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Задания по самостоятельной работе включают:

- конспектирование лекций;
- проработку учебного материала;
- выполнение домашних заданий.

Текущий контроль освоения материала осуществляется через контроль посещения занятий, проведение контрольных работ в течение семестра и по разделам.

Для допуска к аттестации студент должен предоставить конспекты лекций по пропущенным темам.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

При подготовке к занятиям преподавателю следует помнить, что вузовская лекция – главное звено дидактического цикла обучения. Ее цель – формирование у студентов ориентировочной основы для последующего усвоения материала студентом методом самостоятельной работы. Содержание лекции должно отвечать следующим дидактическим требованиям:

- изложение материала от простого к сложному, от известного к неизвестному;
- логичность, четкость и ясность в изложении материала;
- тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью студентов.

Автор(ы):

Смирнов Антон Михайлович

Пудовкина Марина Александровна, д.ф.-м.н.