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

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	2	72	0	32	0		40	0	З
Итого	2	72	0	32	0	0	40	0	

АННОТАЦИЯ

В курсе рассматриваются следующие темы:
• основы теории конечных полей;
• линейный блоковый 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 объёме 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-1.4 [1] – Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	З-ОПК-1.4 [1] – знать нормативными и корпоративными требованиями по безопасности компьютерных систем и сетей У-ОПК-1.4 [1] – уметь применять нормативные и корпоративные требованиями по безопасности компьютерных систем и сетей В-ОПК-1.4 [1] – владеть методами оценки уровня безопасности компьютерных систем и сетей

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

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции;**	**Код и наименование индикатора достижения**

		Основание (профессиональный стандарт-ПС, анализ опыта)	**профессиональной компетенции**
проектно-технологический			
Разработка способов и средств защиты объектов критической информационной инфраструктуры	Наукоёмкие информационные технологии и системы критической информационной инфраструктуры, функционирующие в условиях существования угроз в информационной сфере и включающие компоненты, подлежащие защите	ПК-2 [1] - способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов *Основание:* Профессиональный стандарт: 06.032	З-ПК-2[1] - знать действующие нормативные и методические документы по проектированию подсистемы безопасности информации ; У-ПК-2[1] - уметь проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов; В-ПК-2[1] - владеть принципами проектирования подсистемы безопасности информации
экспериментально-исследовательский			
Анализ современных систем и средств защиты объектов критической информационной инфраструктуры	Наукоёмкие информационные технологии и системы критической информационной инфраструктуры, функционирующие в условиях существования угроз в информационной сфере и включающие компоненты, подлежащие защите	ПК-3 [1] - способен исследовать модели систем защиты информации *Основание:* Профессиональный стандарт: 06.032	З-ПК-3[1] - знать основные модели систем защиты информации ; У-ПК-3[1] - уметь проводить исследование моделей систем защиты информации; В-ПК-3[1] - владеть принципами проведения исследования моделей систем защиты информации

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих,	Использование воспитательного потенциала дисциплин

	формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (В18)	профессионального модуля для формирования у студентов ответственности за свое профессиональное развитие посредством выбора студентами индивидуальных образовательных траекторий, организации системы общения между всеми участниками образовательного процесса, в том числе с использованием новых информационных технологий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (В19)	1.Использование воспитательного потенциала дисциплин/практик «Научно-исследовательская работа», «Проектная практика», «Научный семинар» для: - формирования понимания основных принципов и способов научного познания мира, развития исследовательских качеств студентов посредством их вовлечения в исследовательские проекты по областям научных исследований. 2.Использование воспитательного потенциала дисциплин "История науки и инженерии", "Критическое мышление и основы научной коммуникации", "Введение в специальность", "Научно-исследовательская работа", "Научный семинар" для: - формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед; - формирования критического мышления, умения рассматривать различные исследования с экспертной позиции посредством обсуждения со студентами современных исследований, исторических предпосылок появления тех или иных открытий и теорий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование профессионально значимых	1. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)",

	установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (В40)	Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры написания и оформления программ, а также привития навыков командной работы за счет использования систем управления проектами и контроля версий. 2.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования культуры решения изобретательских задач, развития логического мышления, путем погружения студентов в научную и инновационную деятельность института и вовлечения в проектную работу. 3.Использование воспитательного потенциала профильных дисциплин для формирования навыков цифровой гигиены, а также системности и гибкости мышления, посредством изучения методологических и технологических основ обеспечения информационной безопасности и кибербезопасности при выполнении и защите результатов учебных заданий и лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях. 4.Использование воспитательного потенциала дисциплин " "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры безопасного программирования посредством тематического акцентирования в содержании дисциплин и учебных заданий. 5.Использование воспитательного

		потенциала дисциплины "Проектная практика" для формирования системного подхода по обеспечению информационной безопасности и кибербезопасности в различных сферах деятельности посредством исследования и перенятия опыта постановки и решения научно-практических задач организациями-партнерами.

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	7 Семестр						
1	Первый раздел	1-8	0/16/0		25	КИ-8	У-ПК-3, В-ПК-3, З-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3
2	Второй раздел	9-16	0/16/0		25	КИ-16	З-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3
	Итого за 7 Семестр		0/32/0		50		
	Контрольные мероприятия за 7 Семестр				50	З	З-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, З-ПК-2, У-ПК-2, В-ПК-2,

							З-ПК-3, У-ПК-3, В-ПК-3

* – 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
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	7 Семестр	0	32	0
1-8	**Первый раздел**	0	16	0
1 - 8	**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, 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 построение расширений полей по неприводимому многочлену. Теорема Кронекера.	Всего аудиторных часов 0 Онлайн 0	16 0	0 0

	Вполне разложимый многочлен. Поле разложения и теорема об их существование. 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 сепарабильности. 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 конченого поля. Диаграмма подполей. Свойства группы автоморфизмов поля.			
9-16	**Второй раздел**	0	16	0
9 - 16	**Основы теории кодирования** Введит Развитие теории кодирования. Способы кодирования. Основные задачи теории кодирования. Двоичный симметричный канал с вероятностью ошибки p. Информационные символы. Проверочные символы. Кодовое расстояние. Понятие метрического пространства. Метрика Хемминга на -мерном векторном пространстве над полем , вес Хемминга. Норма. Пространство Джонсона. Линейный блоковый код над полем . 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. Декодированием по методу максимального правдоподобия. Декодированием 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 $p_{ош}$ метода декодирования.	Всего аудиторных часов 0 Онлайн 0	16 0	0 0

	Пропускная способность двоичного симметричного канала с вероятностью ошибки p. Теорема Шеннона о существовании кодов. Двойственный (дуальный, ортогональный) код. Доказать, что если C □ (n,k) - код, k=dim C, то код C^⊥ является линейным кодом над полем F_q размерности n-k. Слабо и строго самодуальные коды. Границы кодов. Граница Хемминга или граница сферической упаковки. Теорема Варшамова-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-1.4	З-ОПК-1.4	З, КИ-8, КИ-16
	У-ОПК-1.4	З, КИ-8, КИ-16
	В-ОПК-1.4	З, КИ-8, КИ-16
ПК-2	З-ПК-2	З, КИ-8, КИ-16
	У-ПК-2	З, КИ-8, КИ-16
	В-ПК-2	З, КИ-8, КИ-16
ПК-3	З-ПК-3	З, КИ-8, КИ-16
	У-ПК-3	З, КИ-8, КИ-16
	В-ПК-3	З, КИ-8, КИ-16

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 балльной шкале	Оценка ECTS	Требования к уровню освоению 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 твёрдо 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 –		Оценка «удовлетворительно»

60-64	«*удовлетворительно*»	E	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.
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.