Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ С.М.Дудаков

«05» 03 2024 г.

Рабочая программа дисциплины (с аннотацией)

ПРИКЛАДНАЯ АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Направление подготовки

09.04.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Профиль подготовки

Интеллектуальные системы. Теория и приложения

Для студентов 1 курса

Очная форма

Составитель: д.ф.-м.н. доцент Дудаков С.М.

Тверь 2024

I. Аннотация

1. Цель и задачи дисциплины:

ознакомить обучающихся с некоторыми идеями и понятиями современной прикладной алгебры, теории чисел и связанными с ними вопросами кодирования и шифрования.

2. Место дисциплины в структуре ООП

Дисциплина входит в раздел «Дисциплины профиля подготовки» части, формируемой участниками образовательных отношений, блока 1.

Предварительные знания и навыки. Знание общих курсов линейной алгебры, общей алгебры.

Дальнейшее использование. Полученные знания могут применяться при выполнении научно-исследовательской работы, при прохождении научно-исследовательской практики, при написании выпускной квалификационной работы, а также в дальней трудовой деятельности выпускника.

3. Объем дисциплины: 4 зач. ед., 144 акад. ч., в том числе:

контактная аудиторная работа лекций 16 ч., практических занятий 16 ч.,

контактная внеаудиторная работа контроль самостоятельной работы 0 ч., в том числе курсовая (расчетно-графическая) работа 0 ч.;

самостоятельная работа 112 ч., в том числе контроль 36 ч.

4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы:

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ПК-3, Способен выбирать и применять методы инженерии знаний для создания систем, основанных на знаниях	ПК-3.1, Выбирает и применяет методы сбора и извлечения знаний ПК-3.3, Выбирает и применяет методы представления знаний

5. Форма промежуточной аттестации и семестр прохождения:

экзамен.

6. Язык преподавания:

русский

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Для студентов очной формы обучения

Учебная программа — наименование разделов и тем	Всего (час.)	Контактная работа (час.)					Сам. раб., в т.ч. контроль (час.)
		Лекции		Практ. занятия / Лаб. работы		Контроль сам. раб., в т.ч. курсовая работа	
		Всего	В т.ч. практ. подг.	Всего	В т.ч. практ. подг.		
1	2	3	4	5	6	7	8
Общие вопросы помехоустойчивого кодирования	41	4		4/0		0	33
Полиномиальные коды	51	6		6/0		0	39
Современные методы шифрования	52	6		6/0		0	40
Итого	144	16	0	16/0	0/0	0	112

Учебная программа дисциплины

1. Общие вопросы помехоустойчивого кодирования
   - Общая задача помехоустойчивого кодирования, пространства исходных и кодовых слов, метрика Хемминга, обнаружение и исправление ошибок
   - Коды Хемминга
   - Групповые коды, линейные коды, матричные коды. Кодирующая и проверочная матрицы
   - NP-полнота задачи корректного декодирования для матричного кода
2. Полиномиальные коды
   - Циклические коды. Полиномиальные коды как частный случай матричных
   - Построение некоторых полиномиальных кодов. Пакетные коды. Квадратично-вычетные коды
   - Коды Боуза-Чоузхури-Хоккенгейма: построение и алгоритм декодирования. Коды Соломона-Рида
3. Современные методы шифрования

- Схемы шифрования RSA. Алгебраические и теоретико-числовые задачи шифрования
- Средние значения теоретико-числовых функций
- Порождение простых чисел
- Элементы теории квадратичных вычетов
- Тесты на простоту
- Схема эль-Гамаля
- Циклические теоретико-числовые группы
- Группы точек на эллиптических кривых. Оценки порядка

III. Образовательные технологии

Учебная программа — наименование разделов и тем	Вид занятия	Образовательные технологии
Общие вопросы помехоустойчивого кодирования	лекции, практические занятия	изложение теоретического материала, решение задач
Полиномиальные коды	лекции, практические занятия	изложение теоретического материала, решение задач
Современные методы шифрования	лекции, практические занятия	изложение теоретического материала, решение задач

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Типовые контрольные задания и/или критерии для проверки индикатора ПК-3.1

Требования к обучающемуся	Типовые контрольные задания для оценки знаний, умений, навыков	Показатели и критерии оценивания, шкала оценивания
Владеть базовыми навыками самостоятельного исследования	Возможные темы для самостоятельного изучения • Теорема Хассе о количестве точек на эллиптической кривой • Тест на простоту Миллера-Рабина • Преобразование уравнения эллиптической кривой к каноническому виду Вейершстрасса	оценка 3 — способен самостоятельно изучить научные результаты, оценка 4 — кроме того, способен проинтерпретировать различные аспекты полученной информации, оценка 5 — кроме того, способен применить полученные знания для решения конкретных задач

Требования к обучающемуся	Типовые контрольные задания для оценки знаний, умений, навыков	Показатели и критерии оценивания, шкала оценивания
Знать материалы из алгебры, используемые в задачах помехоустойчивого кодирования	Примеры вопросов к экзамену/зачету: • Алгоритм декодирования БЧХ. • Доказать теорему о минимальном расстоянии для кодов БЧХ. Примеры задач для контрольных работ • Найти количество примитивных элементов в поле GF(257).	оценка 3 — знает некоторые алгебраические конструкции, используемые для построения кодов; оценка 4 — знает основные конструкции, применяемые для построения кодов различных видов, а также их свойства; оценка 5 — кроме того, знает доказательства соответствующих утверждений
Знать основы теории помехоустойчивого кодирования	Примеры вопросов к экзамену/зачету: • Дать определение метрики Хемминга, минимального расстояния кода, сформулировать условие, связывающее минимальное расстояние кода и количество обнаруживаемых (исправляемых) ошибок. • Метод построения кода Хемминга. • Дать определение линейного кода, кодирующей и проверочной матрицы. • Доказать NP-полноту задачи ошибочного линейного декодирования: нахождения вектора $\bar{x}$ заданного веса так, чтобы $A\bar{x} = \bar{0}$.	оценка 3 — знает базовые положения теории помехоустойчивого кодирования; оценка 4 — кроме того, знает основные свойства линейных кодов; оценка 5 — также знает доказательства соответствующих утверждений

Типовые контрольные задания и/или критерии для проверки индикатора ПК-3.3

Требования к обучающемуся	Типовые контрольные задания для оценки знаний, умений, навыков	Показатели и критерии оценивания, шкала оценивания
Уметь строить и применять основные типы помехоустойчивых кодов	Примеры задач для контрольных работ • Двоичный (4, 8)-код реализуется с помощью многочлена $1+x+x^4$. Построить матрицу кодирования. Построить множество кодовых слов (многочленов). Найти наименьшее расстояние между кодовыми словами. Определить, сколько ошибок код может обнаружить и сколько исправить. Определить, есть ли ошибка в многочлене $1+x^3+x^7$? Если есть, то можно ли ее исправить, и что получится в результате? • Двоичный (ℓ, m)-код построен с помощью многочлена $1+x^n+x^{2n}+\cdots+x^{kn}$, $n < \ell$. Доказать, что такой код в произвольном случае не сможет обнаружить две ошибки.	оценка 3 — умеет выполнять простейшие операции по кодированию, декодированию, обнаружению ошибок; оценка 4 — умеет применять алгоритмы исправления ошибок; оценка 5 — кроме того, может выполнять анализ свойств кода
Знать материалы из алгебры и теории чисел, используемые в задачах шифрования	Примеры вопросов к экзамену/зачету: • Доказать теоремы о количестве точек на эллиптической кривой над конечным полем. • Дать определение символа Лежандра и символа Якоби. Сформулировать основные свойства символа Лежандра. • Дать определение функции Эйлера, группы $\mathbb{Z}_m^*$. Сформулировать их основные свойства.	оценка 3 — знает некоторые из понятий, необходимых в вопросах шифрования; оценка 4 — знает основные математические понятия, используемые в задачах шифрования,

Требования к обучающемуся	Типовые контрольные задания для оценки знаний, умений, навыков	Показатели и критерии оценивания, шкала оценивания
	• Доказать китайскую теорему об остатках и теорему о корректности декодирования в алгоритме RSA. • Доказать теорему о корректности теста Соловея-Штрассена. • Дать определение эллиптической кривой. Сформулировать закон сложения точек на эллиптической кривой. Примеры задач для контрольных работ • Доказать, что на отрезке $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ квадратичные вычеты по модулю p располагаются относительно нуля или симметрично (x — вычет тогда и только тогда, когда $-x$ — вычет), или антисимметрично (x — вычет тогда и только тогда, когда $-x$ — невычет). • Доказать обобщение теоремы Ферма: если a и p взаимно просты, то $a^{\varphi(p)} \equiv 1 \pmod{p}$. Здесь φ — функция Эйлера. • Найти значение символа Якоби $\left(\frac{3}{p}\right)$ для произвольного нечётного числа p.	и их свойства; оценка 5 — кроме того, знает доказательства соответствующих утверждений
Уметь применять алгебраические и теоретико-числовые алгоритмы и конструкции	Примеры задач для контрольных работ • Найти пошагово с помощью алгоритма значение символа Якоби $\left(\frac{143}{225}\right)$. Найти его же по определению. • Построить группу точек эллиптической кривой, заданной уравнением $y^2 = x^3 + 2x + 1$ над полем GF(7). Определить, является ли она циклической. • Найти всех свидетелей в тесте Соловея-Штрассена, подтверждающих, что число 9 является составным.	оценка 3 — может реализовать некоторые алгебраические или теоретико-числовые конструкции; оценка 4 — может использовать методы и алгоритмы для решения базовых задач; оценка 5 — умеет применять различные методы и алгоритмы

V. Учебно-методическое и информационное обеспечение дисциплины

1. Рекомендованная литература

а) Основная литература

[1] Кнауб Л.В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. — Красноярск : Сибирский федеральный университет 2011. — 160 с. — ISBN 978-5-7638-2113-7. — Режим доступа: http://znanium.com/catalog.php?bookinfo=441493 — Загл. с экрана (ЭБС ИНФРА-М).

[2] Сидельников В.М. Теория кодирования [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : Физматлит, 2008. — 322 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=2311 — Загл. с экрана (ЭБС ЛАНЬ).

[3] Чечёта, С.И. Введение в дискретную теорию информации и кодирования

[Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : МЦНМО, 2011. — 224 с. — Режим доступа: https://e.lanbook.com/book/9437. — Загл. с экрана.

б) Дополнительная литература

[4] Вычислительно сложные задачи теории чисел [Электронный ресурс] : учеб. пособие / Е.А. Гречников [и др.]. — Электрон. дан. — Москва : МГУ имени М.В.Ломоносова, 2012. — 312 с. — Режим доступа: https://e.lanbook.com/book/73099. — Загл. с экрана.

[5] Терентьев, И.В. Теория чисел и ее применение. Справочник: учебное пособие для студентов всех специальностей [Электронный ресурс] : учеб. пособие — Электрон. дан. — Санкт-Петербург : СПбГЛТУ, 2010. — 142 с. — Режим доступа: https://e.lanbook.com/book/45571. — Загл. с экрана.

[6] Василенко О.Н. Теоретико-числовые алгоритмы в криптографии [Электронный ресурс] : монография. — Электрон. дан. — М. : МЦНМО (Московский центр непрерывного математического образования), 2006. — 336 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=9303 — Загл. с экрана (ЭБС ЛАНЬ).

2. Программное обеспечение

Наименование помещений	Программное обеспечение
Ауд. 308 (170002, Тверская обл., г. Тверь, пер. Садовый, д. 35)	Google Chrome — бесплатно; Microsoft Office 365 pro plus — Акт на передачу прав № 687 от 31 июля 2018; Microsoft Windows 10 Enterprise — Акт на передачу прав № 687 от 31 июля 2018; Kaspersky Endpoint Security 10 для Windows — Акт на передачу прав №2129 от 25 октября 2016 г.
Ауд. 201а (компьютерная лаборатория ПМиК) (170002, Тверская обл., г. Тверь, пер. Садовый, д. 35)	Перечень программного обеспечения (со свободными лицензиями): Linux OpenSuse Tumbleweed, KDE, TeXLive, Mozilla Firefox, TeXStudio, Qt, QtCreator, Gcc, Python, Eric, LibreOffice, Cervisia, Kdbg, Umbrello, wxMaxima, Blender, digikam, GIMP, Gwenview, hugin, Inkscape, Okular, showFoto, Kmail, Konqueror, Konversation, Kopete, TigerVNC viewer, Amarok, K3b, Kdenlive, VLC media player, Kontact, Korganizer, Yast, Ark, Dolphin, Info Center, Kget, Konsole, Krusader, Midnight commander, OpenJDK, pgadmin3, Xterm, Emacs, Kate, Kcalc, Kgpg, Kleopatra, Kompare, Sweeper, Perl, Apache, PostgreSQL, MariaDB, SQLite, PHP

3. Современные профессиональные базы данных и информационные справочные системы

[1] ЭБС «ZNANIUM.COM» http://www.znanium.com

[2] ЭБС «Университетская библиотека онлайн» https://biblioclub.ru

[3] ЭБС IPRbooks http://www.iprbookshop.ru

[4] ЭБС «Лань» http://e.lanbook.com

[5] ЭБС «Юрайт» https://urait.ru

[6] ЭБС ТвГУ http://megapro.tversu.ru/megapro/Web

[7] Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp

[8] Репозитарий ТвГУ http://eprints.tversu.ru

4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

[1] A Course in Universal Algebra, https://www.math.uwaterloo.ca/~snburris/htdocs/u

[2] An Invitation to General Algebra and Universal Constructions, https://math.berkeley.edu/~gbergman/245/

[3] Московский центр непрерывного математического образования, http://www.mccme.ru/

VI. Методические материалы для обучающихся по освоению дисциплины

Задачи для самостоятельной подготовки

- Доказать, что если фактор-группа группы G по центру группы G является циклической группой, то группа G является абелевой.
- Ассоциативное кольцо K с единицей, в котором $(xx) = x$ для всех x из K, называется булевым. Доказать, что каждое булево кольцо, содержащее больше двух элементов, не является полем.
- Найти все подгруппы циклической группы порядка 36.
- Рассматриваются многочлены над полем вычетов по модулю 2. Пусть $g(x) = (1+x)(1+x^2+x^3)$ определяет (3,7)-код. Доказать, что наименьший вес ненулевого кодового слова равен 4.
- Найти пошагово с помощью алгоритма и по определению значение символа Якоби $\left(\frac{747}{1725}\right)$.
- Построить группу точек эллиптической кривой, заданной уравнением $y^2 = x^3 + 2x + 1$ над полем GF(11). Определить, является ли она циклической.

Выставление оценок

Контрольная работа 1. Темы: полиномиальные коды. Пример задания:

Двоичный (4, 8)-код реализуется с помощью многочлена $1 + x + x^4$. Построить матрицу кодирования. Построить множество кодовых слов (многочленов). Найти наименьшее расстояние между кодовыми словами. Определить, сколько ошибок код

может обнаружить и сколько исправить. Определить, есть ли ошибка в многочлене $1 + x^3 + x^7$? Если есть, то можно ли ее исправить, и что получится в результате?

При решении задачи выставляется 5 баллов за выполнение каждой части (всего не более 30).

Контрольная работа 2. Темы: приложения теории чисел. Пример задания:

- Найти пошагово с помощью алгоритма значение символа Якоби $\left(\frac{145}{237}\right)$. Найти его же по определению.
- Построить группу точек эллиптической кривой, заданной уравнением $y^2 = x^3 + x + 3$ над полем GF(7). Определить, является ли она циклической.

За решение каждого этапа выставляется максимум 5 баллов (всего не более 20).

Общая сумма В сумме за все задачи выставляет не более 50 баллов.

За работу на практических занятиях (решение задач у доски, выполнение домашних заданий) выставляется максимум 10 баллов.

За ответ на экзамене выставляется максимум 40 баллов.

VII. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Для аудиторной работы

Наименование помещений	Материально-техническое оснащение помещений
Ауд. 308 (170002, Тверская обл., г. Тверь, пер. Садовый, д. 35)	Ауд. 308 приспособлена для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации и оснащена набором учебной мебели, меловой доской, настенным экраном (экран на треноге Da-lite versatal 213x213)) и проектором Samsung SP D300BX.

Для самостоятельной работы

Наименование помещений	Материально-техническое оснащение помещений
Ауд. 201а (компьютерная лаборатория ПМиК) (170002, Тверская обл., г. Тверь, пер. Садовый, д. 35)	Ауд. 201а (компьютерная лаборатория ПМиК) оснащена персональными ЭВМ (компьютер ПЭВМ «ХОПЕР» IS09001: 1.1/Intel Core i3-540/IntelH55-MLX/Hynix-11.4/DVD RW Sony/Монитор 21,5" AOC TFT/клавиатура/мышь — 10 штук) с доступом к сети Интернет и необходимым программным обеспечением, системным блоком BASE P4 3200MHz 800 512K/1024 Mb DDR400/400Gb, концентратором сетевым DFE-916 DX HUB 16x10/100.

VIII. Сведения об обновлении рабочей программы дисциплины

№ п/п	Обновленный раздел рабочей программы дисциплины	Описание внесённых изменений	Дата и протокол заседания кафедры, утвердившего изменения
1	I. Аннотация. 3. Объем дисциплины	Выделение часов на практическую подготовку	От 29.10.2020 года, протокол № 3 учёного совета факультета
2	II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	Выделение часов на практическую подготовку по темам	От 29.10.2020 года, протокол № 3 учёного совета факультета
3	I. Аннотация. IV. Оценочные материалы для проведения текущей и промежуточной аттестации	Изменения в учебные планы и в рабочие программы дисциплин, формирующих новые/измененные компетенции в соответствии с приказом Минобрнауки России от 26.11.2020 г. №1456	Решение научно-методического совета (протокол №6 от 02.06.2021 г.)