Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
_____ / А.В. Язенин /
«1» июня 2019 года

Рабочая программа дисциплины (с аннотацией)

ПРИКЛАДНАЯ АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Направление подготовки
02.03.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА
И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Профиль подготовки
Информатика и компьютерные науки

Для студентов 4-го курса

Форма обучения – очная

Составитель:

д.ф.-м.н., доцент С.М. Дудаков _____

Тверь, 2019

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 «Элективные дисциплины» 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: 2 зач. ед., 72 акад. ч., в том числе:

контактная аудиторная работа лекций 30 ч., практических занятий 30 ч.,

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

самостоятельная работа 12 ч., в том числе контроль 0 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-1, Способен к поиску научно-технической информации в области теоретической и прикладной информатики	ПК-1.1, Знает основные приемы поиска научно-технической информации ПК-1.2, Отбирает научно-техническую информацию в соответствии с поставленной задачей ПК-1.3, Изучает и анализирует научно-техническую информацию на предмет их применимости для решения поставленной задачей
ПК-2, Способен к анализу научно-технических задач теоретической и прикладной информатики	ПК-2.1, Классифицирует области ИКТ, к которой относится поставленная задача ПК-2.2, Анализирует известные методы на

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
	предмет их применимости для решения поставленной задачей ПК-2.3, Применяет типовые методы для решения поставленной задачи ПК-2.4, Анализирует полученные при решении задачи результаты

5. Форма промежуточной аттестации и семестр прохождения:

зачет в 7 семестре

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	9	4		4/0		0	1
Полиномиальные коды	29	12		12/0		0	5
Современные методы шифрования	34	14		14/0		0	6
Итого	72	30	0	30/0	0/0	0	12

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 индикаторов ПК-1.1, ПК-1.2, ПК-1.3

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

Типовые контрольные задания и/или критерии для проверки индикатора ПК-2.1

Требования к обучающемуся	Типовые контрольные задания для оценки знаний, умений, навыков	Показатели и критерии оценивания, шкала оценивания
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-2.2

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 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. • 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	оценка 3 — знает некоторые из понятий, необходимых в вопросах шифрования; оценка 4 — знает основные математические понятия, используемые в задачах шифрования, и их свойства; оценка 5 — кроме того, знает доказательства соответствующих утверждений

Требования к обучающемуся	Типовые контрольные задания для оценки знаний, умений, навыков	Показатели и критерии оценивания, шкала оценивания
	• 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.	

Типовые контрольные задания и/или критерии для проверки индикаторов ПК-2.3, ПК-2.4

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
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://biblioclub.ru/index.php?page=book_red&id=63307. — 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. 201а (компьютерная лаборатория ПМиК) (170002, Тверская обл., г. Тверь, пер. Садовый, д. 35)	Перечень программного обеспечения (со свободными лицензиями): Linux Kubuntu, KDE, TeXLive, TeXStudio, LibreOffice, GIMP, Gwenview, ImageMagick, Okular, Skanlite, Google Chrome, KDE Connect, Konversation, KRDC, KTorrent, Thunderbird, Elisa, VLC media player, PulseAudio, KAppTemplate, KDevelop, pgAdmin4, PostgreSQL, Qt, QtCreator, R, RStudio, Visual Studio Code, Perl, Python, Ruby, clang, clang++, gcc, g++, nasm, flex, bison, Maxima, Octave, Dolphin, HTop, Konsole, KSystemLog, Xterm, Ark, Kate, KCalc, Krusader, Spectacle, Vim.

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

Важной составляющей данного раздела РПД являются требования к рейтинг-контролю с указанием баллов, распределенных между модулями и видами работы обучающихся.

Максимальная сумма баллов по учебной дисциплине, заканчивающейся зачетом, по итогам семестра составляет 100 баллов. Распределение баллов по модулям устанавливается преподавателем и может корректироваться.

Студенту, набравшему 40 баллов и выше по итогам работы в семестре, в экзаменационной ведомости и зачетной книжке выставляется оценка «зачтено». Студент, набравший до 39 баллов включительно, сдает зачёт.

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)	Набор учебной мебели, экран проектор.

Для самостоятельной работы

Наименование помещений	Материально-техническое оснащение помещений
Ауд. 201а (компьютерная лаборатория ПМиК) (170002, Тверская обл., г. Тверь, пер. Садовый, д. 35)	Набор учебной мебели, доска маркерная, компьютер, сервер (системный блок), концентратор сетевой.

VIII. Сведения об обновлении рабочей программы дисциплины

№ п/п	Обновленный раздел рабочей программы дисциплины	Описание внесённых изменений	Дата и протокол заседания кафедры, утвердившего изменения