Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.Г.Балашов
«18» 05 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Алгебраические основы криптографии»

Направление подготовки - 02.04.01 «Математика и компьютерные науки»

Направленность (профиль) «Компьютерные методы моделирования, обработки и анализа данных»

Москва 2023

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании компетенции **ПК-2 «**Способен к разработке и применению методов компьютерной математики для исследования математических моделей в инженерных и физических приложениях», сформулированной в результате анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, а также консультаций с ведущими работодателями.

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения подкомпетенций**
ПК-2. АоК. Способен использовать алгебраические и теоретико-числовые методы для составления алгоритмов шифрования и дешифрования	Разработка и применение моделей и методов представления, преобразования, анализа данных при решении исследовательских и проектных задач в области цифровых систем обработки сигналов и изображений	***Знает*** основы криптографии, алгебраические и теоретико-числовые методы шифрования и дешифрования информации. ***Умеет*** применять простейшие криптографические алгоритмы шифрования и дешифрования на практике, а также осваивать методы решения различных криптографических задач. ***Имеет опыт*** составления простейших криптографических алгоритмов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» образовательной программы (является элективной).

Для изучения дисциплины студент должен владеть математическим аппаратом в области линейной алгебры и аналитической геометрии.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	**Семестр**	**Общая трудоёмкость (ЗЕ)**	**Общая трудоёмкость (часы)**	**Контактная работа**			**Самостоятельная работа (часы)**	**Промежуточная аттестация**
				Лекции (часы)	**Лабораторные работы (часы)**	**Практические занятия (часы)**		
2	4	4	144	28	-	28	88	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
1. Теоретико-числовая подготовка	12	-	12	42	Контроль выполнения текущих домашних работ Контрольная работа № 1 по теме «Элементарная теория чисел»
2. Алгебра и шифрование	16	-	16	56	Контроль выполнения текущих домашних работ Контрольная работа № 2 на тему «Расширения полей. Дискретное логарифмирование» Контрольная работа № 3 по теме «Шифрование»

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1-2	4	Деление с остатком. Алгоритм Евклида. Сравнения. Основная теорема арифметики. Линейные диофантовы уравнения. Китайская теорема об остатках.
	3-4	4	Функция Эйлера. Теорема Эйлера. Малая теорема Ферма.
	5-6	4	Мультипликативные функции. Функция Мёбиуса. Формула обращения.
2	7-8	4	Расширения полей. Конечные поля. Группы. Абелевы группы. Циклические группы. Мультипликативная и аддитивная группы конечного поля.
	9	2	Мультипликативная группа кольца вычетов. Дискретное логарифмирование.
	10	2	Решение сравнений $f(x) \equiv 0 \pmod{n}$.
	11-12	4	Криптографические схемы. Шифрсистемы RSA и Эль-Гамаля. Схема Диффи – Хеллмана выработки общего ключа.
	13-14	4	Проективная плоскость. Эллиптические кривые. Криптографические схемы на эллиптических кривых.

4.2. ПРАКТИЧЕСКИЕ ЗАНЯТИЕ

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
1	1-2	4	Простые числа. Алгоритм Евклида. Сравнения.
	3	2	Линейные диофантовы уравнения и системы.
	4-5	4	Мультипликативные теоретико-числовые функции.
	6	2	Контрольная работа.
2	7-8	4	Конечные поля. Неприводимые многочлены.
	9	2	Мультипликативная группа кольца вычетов.
	10	2	Решение сравнений $f(x) \equiv 0 \pmod{n}$. Дискретное логарифмирование.
	11	2	Контрольная работа № 2.
	12-13	2	Криптографические схемы на эллиптических кривых.
	14	2	Контрольная работа № 3.

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	30	Выполнение текущих домашних работ по темам практических занятий
	8	Подготовка к контрольной работе № 1
2	36	Выполнение текущих домашних работ по темам практических занятий
	8	Подготовка к контрольной работе № 2
	8	Подготовка к контрольной работе № 3
1-2	8	Подготовка к зачету

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС// URL: http://orioks.miet.ru/):

Общее

- ✓ Методические указания студентам по изучению дисциплины

Модуль 1 «Теоретико-числовая подготовка**»**

- ✓ Теоретический материал по темам лекций (для всех видов самостоятельной работы)
- ✓ Материалы для подготовки к контрольной работе № 1

Модуль 2 «Алгебра и шифрование**»**

- ✓ Теоретический материал по темам лекций (для всех видов самостоятельной работы)
- ✓ Материалы для подготовки к контрольным работам № 2 и № 3.

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Основы криптографии: Учеб. пособие / А. П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черёмушкин. - 3-е изд., испр. и доп. - М.: Гелиос АРВ, 2005. - 480 с.
2. Введение в криптографию: Учебник / Под ред. В.В. Ященко. - СПб. : МЦНМО : Питер, 2001. - 288 с.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. Лань : Электронно-библиотечная система Издательства Лань. - СПб., 2011-. - URL: https://e.lanbook.com (дата обращения: 15.03.2023). - Режим доступа: для авторизированных пользователей МИЭТ
2. eLIBRARY.RU : Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru/defaultx.asp (дата обращения: 15.03.2023). - Режим доступа: для зарегистрированных пользователей
3. Math-Net.Ru: общероссийский математический портал: сайт. – Москва, Математический институт им. В. А. Стеклова РАН, 2020. – URL: http://www.mathnet.ru/ (дата обращения: 15.03.2023). – Режим доступа: для зарегистрированных пользователей.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Дисциплина реализуется путем проведения лекционных и практических занятий по расписанию в аудиториях вуза и внеаудиторной самостоятельной работы.

Процесс обучения строится по следующей схеме:

(1) лекция (читается еженедельно в аудиториях института по расписанию занятий) - СРС (проработка лекционного материала с использованием записей лекций и учебных пособий);

(2) практическое занятие (проводится еженедельно в аудиториях института по расписанию в форме совместного решения типовых заданий и обсуждения нетиповых задач) - СРС (выполнение текущей домашней работы по теме практического занятия (единого для всех студентов набора типовых и нетиповых заданий) с последующей выборочной проверкой силами преподавателя).

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: раздел «Домашние задания» ОРИОКС, электронная почта.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Учебная доска Специального оснащения не требуется	ПО не требуется
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ	Операционная система Microsoft Windows от 7 версии и выше, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Chrome); Acrobat reader DC

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ПК-2. АоК. Способен использовать алгебраические и теоретико-числовые методы для составления алгоритмов шифрования и дешифрования

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Особенности организации процесса обучения

Лекции и практические занятия проводятся в аудиториях института в соответствии с расписанием (2 часа лекций и 2 час практических занятия в неделю). Дополнительной формой контактной работы являются консультации. Консультации проводятся лектором еженедельно, их посещать необязательно.

В период изучения дисциплины студентам предоставляется в электронном виде учебно-методические материалы (перечень приведён в разделе 5 и 6), в том числе «Методические рекомендации студентам по изучению дисциплины» (включающие подробное описание организации процесса обучения, системы контроля и оценивания). Материалы размещаются в ОРИОКС по адресу http://orioks.miet.ru.

Большое значение придается соблюдению сроков сдачи контрольных мероприятий. Задержка в сдаче приводит к уменьшению числа баллов, начисляемых за выполнение.

Текущие домашние работы содержат практико-ориентированные задания на опыт деятельности. Выполнение текущих домашних работ учитывается при оценке активности студента в процессе обучении.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (включая экзамен), активность в семестре. По сумме баллов выставляется итоговая оценка по предмету. Описание структуры и график контрольных мероприятий доступны в ОРИОКС// URL: http://orioks.miet.ru/.

РАЗРАБОТЧИК:

Профессор каф. ВМ-1, д.ф.-м.н., профессор _____ /Кожухов И.Б./

Рабочая программа дисциплины «Алгебраические основы криптографии» по направлению подготовки 02.04.01 «Математика и компьютерные науки», направленность (профиль) «Компьютерные методы моделирования, обработки и анализа данных», разработана на кафедре ВМ-1 и утверждена на заседании кафедры 25.04 2023 года, протокол № 11

Заведующий кафедрой ВМ-1 _____/А.А. Прокофьев/

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества

Начальник АНОК _____/ И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ

Директор библиотеки _____/ Т.П.Филиппова /