МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С. В.

«31» августа 2021 г.

Рабочая программа дисциплины
Алгоритмы алгебры и теории чисел

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Гераськин А. С.		31.08.2021 г.
Председатель НМК	Кондратова Ю. Н.		31.08.2021 г.
Заведующий кафедрой	Абросимов М. Б.		31.08.2021 г.
Специалист Учебного управления			31.08.2021 г.

1. Цели освоения дисциплины

Целями освоения дисциплины «Алгоритмы алгебры и теории чисел» являются изучение представления алгебраических структур в виде объектов, поддающихся машинной обработки и рассмотрение использования наиболее эффективных алгоритмов для их обработки.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины (Модули)» учебного плана ООП и направлена на формирование у обучающихся профессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплины «Методы программирования».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплины «Теория псевдослучайных генераторов».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Методы алгебраической геометрии в криптографии».

3. Результаты обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора (индикаторов) достижения компетенции**	**Результаты обучения**
ПК-1. Способен применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.	ПК-1.1. Владеет методами построения научной работы, современными методами сбора и анализа полученного материала, способами аргументации; навыками научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и английском языках. ПК-1.2. Умеет решать научные задачи в связи с поставленной целью и в соответствии с выбранной методикой. ПК-1.3. Имеет практический опыт выступлений и научной аргументации в профессиональной деятельности.	Знать методы анализа учебной литературы и научных публикаций. Уметь решать научные задачи и представлять их решение. Владеть методами сбора и анализа полученного материала, способами аргументации.
ПК-2. Способен к самостоятельному построению алгоритмов,	ПК-2.1. Знает современные методы разработки, реализации, анализа и	Знать современные методы реализации и анализа алгоритмов.

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
проведению их анализа и реализации в современных программных комплексах.	оптимизации алгоритмов. ПК-2.2. Умеет разрабатывать и реализовывать алгоритмы в современных программных комплексах. ПК-2.3. Владеет навыками разработки, анализа и реализации алгоритмов.	Уметь реализовывать алгоритмы в программных комплексах. Владеть анализа и реализации алгоритмов.
ПК-3. Способен учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения.	ПК-3.1. Знает основные методы и подходы информатики и вычислительной техники, компьютерных технологий. ПК-3.2. Умеет применять современные методы информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности. ПК-3.3. Владеет навыками использования современных методов информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работы с программными средствами общего и специального назначения.	Знать основные методы и подходы вычислительной техники и компьютерных технологий. Уметь современные методы вычислительной техники и компьютерных технологий в своей учебной и профессиональной деятельности Владеть навыками использования современных методов вычислительной техники и компьютерных технологий при работе с программными средствами.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Практические занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	6		7		8	9
1	Теория делимости в кольце целых чисел.	7	1-5	10	10	4	1	10	*Контрольная работа* на 10-й неделе
2	Сравнения и их свойства.		6-10	10	10	4	1	10	
3	Полиномы от одной переменной.		11-17	14	14	10	2	16	
	Промежуточная аттестация - 36								**Экзамен**
	ИТОГО - 144ч.			**34**	**34**	**18**	**4**	**36**	

Содержание дисциплины

Теория делимости в кольце целых чисел. Простые числа. Разложение целых чисел на простые множители. Наибольший делитель и наименьшее кратное. Алгоритм Евклида. Целые систематические числа. Распределение простых чисел.

Сравнения и их свойства. Сравнения в кольце целых чисел. Простейшие свойства сравнений. Полная система вычетов. Аддитивная группа классов вычетов. Кольцо классов вычетов. Приведенная система вычетов. Мультипликативная группа классов вычетов, взаимно простых с модулем. Функция Эйлера. Теоремы Эйлера и Ферма. Степень и число решений сравнений. Сравнения первой степени. Сравнения высших степеней по простому модулю.

Полиномы от одной переменной. Кольцо полином. Полином над полем. Кольцо полиномов от нескольких переменных. Целые и рациональные корни полинома. Интерполяция над полем. Критерии неприводимости. Простое алгебраическое расширение поля.

План практических занятий

На практических занятиях студентам предоставляются темы для обсуждения и дискуссий и решения.

№ занятия	Тема	Задания для решения в аудитории	Задания для домашней работы
1	**2**	**3**	**4**
1–5	Сравнения и их свойства.	1	2
6–11	Проверка чисел на простоту.	3–5	6–8
12–17	Работа с полиномами над полем целых чисел.	9–11	12–14

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как анализ конкретных ситуаций; технология проблемного обучения, проектной деятельности.

В рамках *практической подготовки* по данной дисциплине используются кейс-задания, выполнение которых направлено на формирование таких профессиональных действий как построению алгоритмов, проведению их анализа и реализации в современных программных комплексах. Примеры кейс-заданий приведены в фондах оценочных средства.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом образовательных возможностей обучающихся.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты изучают материалы практических занятий; изучают дополнительную литературу; решают задачи для самостоятельного разбора.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для практических занятий, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (экзамен). Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Алгоритмы алгебры и теории чисел».

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	10	0	32	8	0	10	40	**100**

Программа оценивания учебной деятельности студента

7 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 10 баллов.

Лабораторные занятия

Не предусмотрены.

Практические занятия

Оценивается правильность выполнения заданий, самостоятельность при выполнении работы, уровень подготовки к занятиям – от 0 до 32 балла.

Самостоятельная работа

Выполнение заданий в рамках самостоятельной работы, хорошее выступление в течение семестра – от 0 до 8 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Выполнения *контрольной работы* – от 0 до 10 баллов:

– грамотность в оформлении, правильное выполнение всех заданий – 10 баллов;

– грамотность в оформлении, правильное выполнение 50 % всех заданий – 5 баллов;

– неправильное оформление, не выполнение заданий – 0 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой устный *экзамен,* проводимый в форме собеседования с предварительной подготовкой студента к ответу.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 30 до 40 баллов;

ответ на «хорошо» оценивается от 20 до 29 баллов;

ответ на «удовлетворительно» оценивается от 10 до 19 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 9 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за седьмой семестр по дисциплине «Алгоритмы алгебры и теории чисел» составляет **100** баллов.

Таблица 2.2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Алгоритмы алгебры и теории чисел» в оценку (экзамен)

86-100 баллов	«отлично»
76-85 баллов	«хорошо»
60-75 баллов	«удовлетворительно»
0-59 баллов	«не удовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. - Санкт-Петербург : Лань, 2022. - 456 с. URL: https://e.lanbook.com/book/189446. Загл. с экрана. Яз. рус.

2) Пилиди, В. С. Математические основы зашиты информации : учебное пособие / В. С. Пилиди ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 308 с. - ISBN 978-5-9275-3363-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088209. Загл. с экрана.

3) Виноградов, И. М. Основы теории чисел : учебное пособие / И. М. Виноградов. — 14-е изд., стер. — Санкт-Петербург : Лань, 2020. — 176 с. — ISBN 978-5-8114-5329-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139285. Загл. с экрана.

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Visual Studio 2010, Visual Studio 2012, Visual Studio 2013, Visual Studio 2015.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима мультимедийная лекционная аудитория.

Для проведения практических занятий необходимы компьютерный класс, класс с установленным программным обеспечением Microsoft Visual Studio версией не ниже 2015.

Реализация *практической подготовки* в рамках учебных занятий запланирована на базе кафедры теоретических основ компьютерной безопасности и криптографии и учебной лаборатории компьютерной безопасности.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Доцент кафедры теоретических основ компьютерной безопасности и криптографии к. п. н. А. С. Гераськин

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «31» августа 2021 года, протокол № 1.