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
Прикладная универсальная алгебра

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	Молчанов В. А.		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 «Прикладная универсальная алгебра» являются: знакомство с базисными структурами прикладной универсальной алгебры; овладение основными приемами их применения в работе с дискретными системами; использование универсально-алгебраических методов и конструкций в криптографии.

2. Место дисциплины в структуре ООП

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

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Алгебра», «Геометрия», «Дискретная математика», «Математическая логика и теория алгоритмов».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Нечёткая логика и алгоритмы», «Интеллектуальные системы».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**1.1.УК-1.** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. **1.2.УК-1.** Осуществляет поиск алгоритмов решения поставленной проблемной ситуации на основе доступных источников информации. Определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей детальной разработке. Предлагает способы их решения. **1.3.УК-1.** Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой	Знать основные понятия универсальной алгебры и методы их применения в компьютерной науке. Уметь находить решения поставленной проблемной ситуации с помощью методов универсальной алгебры. Владеть навыками эффективного решения алгоритмических задач универсальной алгебры.

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	деятельности и на взаимоотношения участников этой деятельности	
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 построения научной работы, сбора и анализа полученного материала, навыки изучения научных обзоров, публикаций, рефератов и библиографий по прикладной универсальной алгебре. Уметь решать прикладные задачи универсальной алгебры в связи с поставленной целью и в соответствии с выбранной методикой. Владеть навыками публичных выступлений и научной аргументации в профессиональной деятельности.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов.

№ 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	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	5-й семестр								
1	Введение в универсальную	5	1-4	8	–	–	–	8	Опрос на 9-й неделе

№ п/п	Раздел дисциплины	Се-местр	Неделя се-местра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	алгебру								
	Упорядоченные множества и решетки		5-8	8	–	–	–	8	
2	Универсальные алгебры: основные понятия и главные конструкции		9-12	8	–	–	–	6	
3	Теория моделей		13-14	4	–	–	–	4	
4	Теория конечных автоматов.		15-18	8	–	–	2	8	*Контрольная работа* №1 на 18 неделе
	Промежуточная аттестация								**Зачет**
	ИТОГО в 5-м семестре – 72ч.			**36**	**–**	**–**	**2**	**34**	
	6-й семестр								
5	Комбинаторная теория групп	6	1-4	8	8	4	–	10	Опрос на 8-й неделе
6	Комбинаторная теория полей		5-8	8	8	4	–	10	
7	Полугруппы, автоматы и языки		9-13	10	10	4	2	10	
8	Алгебраическое распознавание языков		14-16	6	6	4	2	10	*Контрольная работа* №2 на 16 неделе
	Промежуточная аттестация - 36								**Экзамен**

№ 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	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	ИТОГО в 6-м семестре – 144ч.			32	32	16	4	40	
	ВСЕГО			216ч.					

Содержание дисциплины

Введение в универсальную алгебру. Алгебра отношений. Классификация отношений и операции над отношениями. Задание бинарных отношений (предикатное, графическое и матричное). Произведение бинарных отношений, его ассоциативность. Отношение эквивалентности и фактор-множество.

Упорядоченные множества и решетки. Отношение порядка и упорядоченные множества. Экстремальные элементы в конечных упорядоченных множествах. Линейные продолжения порядков. Решетки и системы замыканий. Контексты и концептуальные решетки. Булевы алгебры и теорема Стоуна.

Универсальные алгебры и основные конструкции. Алгебраические операции, алгебры и алгебраические системы. Порождающие множества, подалгебры и фактор-алгебры. Гомоморфизмы и изоморфизмы алгебр. Теоремы о гомоморфизмах. Прямые произведения алгебр и прямо неразложимые алгебры. Подпрямые произведения алгебр и подпрямо неприводимые алгебры. Решетки подалгебр и решетки конгруэнций.

Теория моделей. Определение языка узкого исчисления предикатов и его интерпретации. Классы алгебр и операции над классами алгебр. Свободные алгебры и многообразия.

Теория конечных автоматов. Многосортные алгебры и автоматы. Моноид автомата и автомат моноида. Подавтоматы и фактор-автоматы. Операции над автоматами. Оптимизация автоматов.

Комбинаторная теория полей. Основные понятия теории колец: кольцо, область целостности и поле. Поле частных области целостности. Отношение делимости в кольцах. Идеалы и фактор-кольца. Гомоморфизмы колец и теорема о гомоморфизмах. Главные идеалы. Простые элементы области целостности. Кольца главных идеалов, факториальные и евклидовы кольца. Конечные поля. Теорема о примитивном корне. Характеристика поля. Алгебраические и трансцендентные элементы над конечным полем.

Простые поля. Строение конечных полей. Неприводимые многочлены и разложение многочленов над конечными полями. Построение поля Галуа.

Комбинаторная теория групп. Основные понятия теории групп. примеры. Симметрическая группа перестановок, ее специальные элементы. Подгруппы, порождающие элементы. Порядок элемента группы, его свойства. Циклические группы, их описание. Морфизмы групп. Теорема Кэли о представлении групп перестановками. Разложение группы по подгруппе и теорема Лагранжа. Нормальные делители и фактор-группы. Построение гомоморфизмов групп, фактор-групп и декартовых произведений групп. Полугруппа слов и копредставление групп. Теория перечисления Пойа: цикловой индекс группы перестановок множества, транзитивные множества группы перестановок и лемма Бернсайда, классы эквивалентных отображений, перечень фигур и конфигураций, теорема Пойа о перечне классов эквивалентных конфигураций.

Полугруппы, автоматы и языки. Основные понятия теории полугрупп. Симметрическая полугруппа бинарных отношений, ее специальные элементы. Приложения полугрупп бинарных отношений к анализу криптографических свойств преобразований информации. Симметрическая полугруппа преобразований, ее специальные элементы. Подполугруппа, порождающие элементы. Морфизмы полугрупп. Теорема Кэли о представлении полугрупп преобразованиями. Конгруэнции, фактор-полугруппы и основные теоремы о гомоморфизмах. Идеалы полугрупп и отношения Грина. Строение конечных полугрупп. Свободные полугруппы и определяющие отношения. Копредставления полугрупп. Конструирование полугрупп. Подполугруппы свободных полугрупп и коды.

Алгебраическое распознавание языков. Формальные языки конечных слов. Распознавание формальных языков полугруппами и автоматами. Описание языков рациональными выражениями. Определение языков логическими формулами. Теорема Клини-Нероуда-Майхилла-Буши о эквивалентности альтернативных подходов к распознаваемым языкам. Потоки распознаваемых языков и псевдомногообразия конечных полугрупп. Иерархии распознаваемых языков. Понятие –полугруппы и разновидности автоматов (Буши, Мюллера и др.). Алгебраическое распознавание языков бесконечных слов: распознавание языков –полугруппами и автоматами, описание языков рациональными выражениями и определение языков логическими формулами. Сравнение альтернативных подходов к распознаваемым языкам бесконечных слов. Общее понятие алгебраической распознаваемости множеств дискретных структур.

План лабораторных занятий

На лабораторных занятиях студенты с преподавателем разбирают примеры решения типовых задач из [1,3,5,6], самостоятельно выполняют задания из учебно-методических пособий [1,3,5,6] с практической реализацией основных алгоритмов теории дискретных систем в форме компьютерных программ с использованием системы компьютерной алгебры

GAP (Группы, алгоритмы и программирование) и языков программирования высокого уровня, делают доклады по самостоятельно разобранным темам лабораторных работ.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1	Алгебра отношений.	1-2
2	Разбиения и порядки	3-4
3	Решетки и системы замыканий	5
4	Контексты и концептуальные решетки	6
5	Конечные автоматы: элементарные конструкции	7-8
6	Каскадные соединения автоматов	9
7	Минимизация автоматов	10
8	Полугруппы: элементарные конструкции	11-12
9	Построение полугрупп	13
10	Полугруппа бинарных отношений	14
11	Строение конечных полугруппина	15
12	Группы: элементарные конструкции и представление групп	16-17
13	Кольца и поля: строение конечных полей	18-19
14–16	Алгебраическое распознавание языков	20-21

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как проведение коллоквиумов по ключевым для приложений темам, привлечение студентов к работе в научном семинаре кафедры, к переводам текстов из зарубежных изданий по дисциплине, демонстрация работы компьютерных программ по прикладной универсальной алгебре и теории автоматов, встречи со специалистами из профильных организаций и фирм.

При проведении занятий по данному курсу используются следующие активные и интерактивные формы обучения: контрольные работы, коллоквиумы.

В рамках *практической подготовки* по данной дисциплине используются кейс-задания, выполнение которых направлено на формирование таких профессиональных действий как применение современного математического аппарата и фундаментальных концепций при решении прикладных задач с помощью информационных технологий; разработка алгоритмических и программных решений в области компьютерных наук. Примеры кейс-заданий приведены в фонде оценочных средств дисциплины.

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 более углубленно осваивают преподаваемый материал и могут проявить себя в научно-исследовательской работе, тематика которой предполагается тесно связанной с изучаемым материалом.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольных работ, контрольные вопросы, вопросы для проведения промежуточной аттестации (*зачёт*), вопросы для проведения промежуточной аттестации (*экзамен*). Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Прикладная универсальная алгебра».

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
5	25	0	0	20	0	25	30	**100**
6	10	20	0	15	0	25	30	**100**

Программа оценивания учебной деятельности студента

5 семестр

Лекции

Посещаемость, опрос, активность и др. – от 0 до 25 баллов.

Лабораторные занятия

Не предусмотрены

Практические занятия

Не предусмотрены.

Самостоятельная работа

Выполнение домашних работ в течение семестра – от 0 до 20 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа № 1 – от 0 до 25 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический *зачёт*, проводимый в виде устного собеседования.

При проведении промежуточной аттестации

ответ на «отлично» / «зачтено» оценивается от 25 до 30 баллов;

ответ на «хорошо» / «зачтено» оценивается от 15 до 24 баллов;

ответ на «удовлетворительно» / «зачтено» оценивается от 5 до 14 баллов;

ответ на «неудовлетворительно» / «не зачтено» оценивается от 0 до 4 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 5-й семестр по дисциплине «Прикладная универсальная алгебра» составляет **100** баллов

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Прикладная универсальная алгебра» в оценку (зачет)

50 баллов и более	«зачтено»
меньше 50 баллов	«не зачтено»

6 семестр

Лекции

Посещаемость, активность, умение выделить главную мысль и др. – от 0 до 10 баллов.

Лабораторные занятия

Самостоятельность при выполнении работы, грамотность в оформлении, правильность выполнения и т.д. – от 0 до 20 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Качество и количество выполненных домашних работ, грамотность в оформлении, правильность выполнения и т.д. – от 0 до 15 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа № 2 – от 0 до 25 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический *экзамен,* проводимый в виде устного собеседования с использованием экзаменационных билетов, составленных в соответствии с программой.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 21 до 30 баллов;

ответ на «хорошо» оценивается от 11 до 20 баллов;

ответ на «удовлетворительно» оценивается от 6 до 10 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 5 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 6-й семестр по дисциплине «Прикладная универсальная алгебра» составляет **100** баллов

Таблица 2.2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Прикладная универсальная алгебра» в оценку (экзамен)

80-100 баллов	«отлично»
60-79 баллов	«хорошо»
20-59 баллов	«удовлетворительно»
0-19 баллов	«неудовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины.

а) литература:

1) Богомолов, А. М. Алгебраические основы теории дискретных систем [Текст] / А. М. Богомолов, В. Н. Салий. - Москва: Наука. Физ.-мат. лит., 1997. - 367, [1] с.

2) Курош, А. Г. Лекции по общей алгебре [Электронный ресурс] : учебник / А. Г. Курош. - 3-е изд., стер. - Санкт-Петербург : Лань, 2018. - 556 с. - ISBN 978-5-8114-0617-3 : Б. ц. URL: https://e.lanbook.com/book/104951. Загл. с экрана. Яз. рус.

3) Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс] / В. Н. Салий. - Саратов : [б. и.], 2017. - 45 с. : ил. - Библиогр.: с. 44-45 (15 назв.). URL: http://elibrary.sgu.ru/uch_lit/622.pdf. Загл. с экрана. Яз. рус.

4) Фаддеев, Д. К. Лекции по алгебре : учебное пособие / Д. К. Фаддеев. — 7-е изд., стер. — Санкт-Петербург : Лань, 2020. — 416 с. — ISBN 978-5-8114-4867-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126709.

5) Фаддеев, Д. К. Задачи по высшей алгебре [Текст] : учеб. пособие / Д. К. Фаддеев, И. С. Соминский. - 17-е изд., стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2021. - 287, [1] с. - (Классические задачники и практикумы) (Классическая учебная литература по математике) (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-0427-8 (в пер.). URL: https://e.lanbook.com/book/399.

6) Сборник задач по алгебре [Текст] : учеб. пособие : для вузов : в 2 т. / В. А. Артамонов [и др.] ; под ред. А. И. Кострикина. - Москва : ФИЗМАТЛИТ, 2007. Т. 2, ч. 3 : Основные алгебраические структуры. - Москва : ФИЗМАТЛИТ, 2007. - 168 с. - ISBN 978-5-9221-0726-6 (в пер.)

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Visual C++ 4.2, Visual Studio 2010, Visual Studio 2012, Visual Studio 2013, Visual Studio 2015

2) Свободное программное обеспечение: Java Developers Kit, NetBeans IDE, Eclipse, CPython, Jython, IronPython.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения лабораторных занятий необходимо наличие компьютерного класса, оснащенного соответствующим программным обеспечением, с возможностью выхода в сеть Интернет из расчета одна ПЭВМ на одного человека. В целях сохранения результатов работы желательно наличие у студентов носителей информации.

Реализация практической подготовки в рамах 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

Профессор кафедры теоретических основ компьютерной безопасности и криптографии д.ф.-м.н., профессор В. А. Молчанов

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