

Белорусский государственный университет

УТВЕРЖДАЮ

Проректор по учебной работе
и образовательным инновациям

О.Г.Прохоренко

«03» июня 2024 г.

Регистрационный № УД- 1522/б.

ПРИКЛАДНАЯ АЛГЕБРА

Учебная программа учреждения образования
по учебной дисциплине для специальности:

6-05-0533-10 Информатика

Минск, 2024 г.

Учебная программа составлена на основе ОСВО 6-05-0533-10-2023; учебных планов БГУ: № 6-5.3 – 58/01, № 6-5.3 – 58/02, № 6-5.3 – 58/03, № 6-5.3 – 58/04, № 6-5.3 – 58/05 от 15.05.2023.

СОСТАВИТЕЛИ:

Максим Михайлович Васьковский, заведующий кафедрой высшей математики ФПМИ Белорусского государственного университета, доктор физико-математических наук, профессор.

Георгий Прокофьевич Размыслович, доцент кафедры высшей математики ФПМИ Белорусского государственного университета, кандидат физико-математических наук, доцент.

Задорожнюк Анна Олеговна, доцент кафедры высшей математики ФПМИ Белорусского государственного университета, кандидат физико-математических наук.

РЕЦЕНЗЕНТЫ:

Кононов Сергей Гаврилович, доцент кафедры геометрии, топологии и методики преподавания математики ММФ Белорусского государственного университета, кандидат физико-математических наук, доцент;

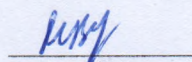
Палуха Владимир Юрьевич, заведующий НИЛ математических методов защиты информации НИИ ППМИ БГУ, кандидат физико-математических наук, доцент кафедры математического моделирования и анализа данных ФПМИ.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой высшей математики БГУ
(протокол № 10 от 24.05.2024 г.);

Научно-методическим советом БГУ
(протокол №8 от 31.05.2024 г.);

Заведующий кафедрой
высшей математики
доктор физико-математических наук



М.М. Васьковский

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Большинство приложений современной алгебры и родственной теории чисел тесно связаны с вопросами защиты информации. Дисциплина «Прикладная алгебра» призвана познакомить слушателя с рядом важнейших разделов современной алгебры и теории чисел, нашедших применение в криптографии. К их числу относятся: теория сравнений и систем сравнений первой степени, функция Эйлера, китайская теорема об остатках и некоторые другие вопросы. На этой основе дается строгое описание математических моделей RSA-криптосистемы и электронной цифровой подписи на ее основе, а также хранения секрета в разделенном виде и CRT-пороговых схем.

Цели и задачи учебной дисциплины

Основными целями преподавания учебной дисциплины «Прикладная алгебра» являются:

- изучение теоретических основ алгебры и теории чисел и их применений в информатике;
- формирование навыков практического применения полученных знаний для решения задач по обеспечению компьютерной и информационной безопасности.

Основные задачи, решаемые при изучении учебной дисциплины «Прикладная алгебра»:

- овладение алгоритмическими средствами систем защиты информации;
- формирование практических навыков решения типовых задач защиты информации с помощью стандартного программного обеспечения.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина «Прикладная алгебра» является дисциплиной государственного компонента и входит **в модуль** «Геометрия и алгебра».

Учебная дисциплина «Прикладная алгебра» основываясь на теоретических положениях, моделях и методах учебных дисциплин «Основы высшей алгебры» и «Линейная алгебра» обобщает и развивает их применительно к актуальным задачам современной информатики.

Знания, полученные в рамках данной дисциплины, будут использованы при изучении других дисциплин специальности 6-05-0533-10 Информатика, направленных на углубленную подготовку специалистов в данной области, включая дисциплины: «Теория алгоритмов» и «Компьютерные сети».

Требования к компетенциям

Освоение учебной дисциплины «Прикладная алгебра» должно обеспечить формирование следующих **базовых профессиональных** компетенций:

БПК Решать математические задачи и строить логические цепочки утверждений.

БПК Использовать методы аналитической геометрии и линейной алгебры в задачах информационных технологий и применять их при разработке алгоритмов.

В результате изучения дисциплины студент должен:

знать:

- основы модулярной арифметики и оценки сложности ее базовых алгоритмов;
- основные свойства показателей, первообразных корней и дискретного логарифма;
- RSA-криптосистему и электронную цифровую подпись на ее основе;
- основы теории групп, колец и полей;
- свойства расширений полей конечной степени и основы теории полей Галуа и помехоустойчивого кодирования;

уметь:

- решать сравнения и системы сравнений первой степени и применять для этой цели функцию Эйлера и китайскую теорему об остатках;
- решать показательные и степенные сравнения путем индексирования;
- строить кодирующие и проверочные матрицы;

владеть:

- основными понятиями теории групп, колец и полей;
- методами решения основных задач по обеспечению компьютерной и информационной безопасности с применением RSA-криптосистем и эллиптических кривых;
- навыками применения протокола Диффи-Хеллмана и современных стандартов цифровой подписи для решения конкретных задач;

Структура учебной дисциплины

Учебная дисциплина изучается в третьем семестре. Всего на изучение дисциплины «Прикладная алгебра» отведено:

- для очной формы получения высшего образования - 100 часов, в том числе 68 аудиторных часов, из них: лекции – 34 часа, практические занятия – 30 часов, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Введение

Предмет курса и его цели и задачи, основные определения.

Тема 1. Теория делимости

Простые числа. Каноническое разложение. Понятие о тестах на простоту и о проблеме факторизации. Применение алгоритма Евклида к проблеме факторизации.

Тема 2. Теория сравнений

Решения сравнений первой степени и диофантовых уравнений. Функция Эйлера. Китайская теорема об остатках. Первообразные корни и индексы. Показательные и полиномиальные сравнения. Задача дискретного логарифмирования.

Тема 3. Кольца и поля

Группа, кольцо и поле. Простые и максимальные идеалы. Евклидовы кольца. Поля Галуа. Расширения полей Галуа. Строение полей Галуа. Дискретное логарифмирование в полях Галуа. Поле разложения. Группы Галуа.

Тема 4. Шифрование

Криптосистемы с открытым ключом. Криптосистема Рабина, RSA-криптосистема и электронная цифровая подпись на ее основе. Протокол Диффи-Хеллмана. Хранение секрета в разделенном виде. CRT-пороговые схемы. Эллиптические кривые.

Тема 5. Эллиптические кривые

Понятие эллиптической кривой. Кривые над полями действительных и комплексных чисел. Кривые над конечными полями. Группа эллиптической кривой. Задача дискретного логарифма и криптография на эллиптических кривых.

Тема 6. Кодирование

Коды и их применение в криптографии. Линейные коды. Код Хэмминга.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения образования

Номер темы	Название раздела, темы	Количество аудиторных часов			Форма контроля знаний
		Лекции	Практи- ческие занятия	Количе- ство часов УСР	
1	2	3	4	5	6
	Введение.	1			
1.	Теория делимости.	3	4		Отчеты по аудиторным и домашним практическим упражнениям с их устной защитой, контрольная работа
2.	Теория сравнений.	8	6	2	Отчеты по аудиторным и домашним практическим упражнениям с их устной защитой, контрольная работа
3.	Кольца и поля.	8	6	2	Отчеты по аудиторным и домашним практическим упражнениям с их устной защитой, контрольная работа

4.	Шифрование.	6	6		Отчеты по аудиторным и домашним практическим упражнениям с их устной защитой, контрольная работа, коллоквиум
5.	Эллиптические кривые.	4	4		Отчеты по аудиторным и домашним практическим упражнениям с их устной защитой, контрольная работа
6.	Кодирование.	4	4		Отчеты по аудиторным и домашним практическим упражнениям с их устной защитой, контрольная работа

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Криптология : учебник для студентов учреждений высшего образования по математическим и техническим специальностям / [Ю. С. Харин и др.] ; БГУ. - 2-е изд., пересмотр. - Минск : БГУ, 2023. - 511 с. - URL: <https://elib.bsu.by/handle/123456789/309839>.
2. Васьковский, М. М. Криптографические системы с открытым ключом : учебные материалы для курсантов военного факультета БГУ : в 2 ч. / М. М. Васьковский ; БГУ, Факультет прикладной математики и информатики, Кафедра высшей математики. - Минск : БГУ, 2022.
3. Васьковский, М. М. Криптографические системы с открытым ключом : лабораторные работы для курсантов военного факультета БГУ / М. М. Васьковский, А. О. Задорожнюк ; БГУ, Факультет прикладной математики и информатики, Кафедра высшей математики. - Минск : БГУ, 2024. - 40 с. - URL: <https://elib.bsu.by/handle/123456789/310055>.
4. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие [для вузов] / Л. М. Мартынов. - Изд. 2-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2022. - 454 с. - URL: <https://e.lanbook.com/book/189446>.

Перечень дополнительной литературы

1. Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.: ил. ISBN 978
2. Бейкер А., Введение в теорию чисел. – Мн.: Высш. шк., 1995. – 127 с.
3. Биркгоф Г., Барти Т. Современная прикладная алгебра. – М.: Мир, 1976. – 400 с.
4. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии – М.: МЦНМО, 2003. – 328 с.
5. Виноградов И.М. Основы теории чисел. – М.: Наука, 1991. – 180 с.
6. Лидл Р., Нидеррайтер Г. Конечные поля. – М.: Мир, Т.1,2. 1988 – 812 с.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Для аттестации обучающихся на соответствие их персональных достижений поэтапным и конечным требованиям образовательной программы создаются фонды оценочных средств, включающие следующие формы:

Письменные формы:

- коллоквиумы;
- контрольные работы.

Устно-письменные формы:

- отчеты по аудиторным практическим упражнениям с их устной защи-

той;

- отчеты по домашним практическим упражнениям с их устной защитой;

- зачет.

Оценочными средствами предусматривается оценка способности обучающихся к творческой деятельности, их готовность вести поиск эффективного решения новых задач.

Формой промежуточной аттестации по дисциплине «Прикладная алгебра» учебным планом предусмотрен зачет.

При формировании итоговой отметки используется рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов в ходе проведения контрольных мероприятий текущей аттестации.

Примерные весовые коэффициенты, определяющие вклад текущей аттестации в отметку при прохождении промежуточной аттестации:

Формирование отметки за текущую аттестацию:

- ответы на практических занятиях – 33,3 %;

- контрольные работы 66,7%.

Рейтинговая отметка по дисциплине рассчитывается на основе отметки текущей аттестации - 40%, и отметки на зачете – 60%.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Тема 2. Теория сравнений

Решение полиномиальных сравнений.

Задание: найдите все решения сравнения $8x^{27} - 2x^2 - x \equiv 1 \pmod{70}$.

Форма контроля: отчеты по аудиторным практическим упражнениям с их устной защитой.

Тема 3. Кольца и поля

Решение показательных и степенных сравнений путем индексирования.

Задание: найдите поле разложения многочлена $x^3 + x + 2$ над полем $\mathbb{Q}$.

Форма контроля: отчеты по аудиторным практическим упражнениям с их устной защитой.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

На лекционных занятиях по учебной дисциплине «Прикладная алгебра» возможно использование элементов **эвристического обучения**: проблемное изложение некоторых аспектов, использование частично-поискового метода.

На практических занятиях по учебной дисциплине «Прикладная алгебра» рекомендуется использовать **практико-ориентированный подход**: освоение содержания курса через решение практических задач, приобретение навыков эффективного выполнения разных видов профессиональной деятельности, реализация групповых проектов.

Методические рекомендации по организации самостоятельной работы обучающихся

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются:

- наличием и полным доступом обучающегося к библиотечным фондам, электронным средствам обучения, доступностью электронных (и бумажных) вариантов лекций, учебно-методических пособий и сборников задач по основным разделам учебной дисциплины, указаниями к решению типовых задач.

Примерный перечень вопросов к зачету

1. Делимость целых чисел, деление с остатком
2. Наибольший общий делитель, алгоритм Евклида
3. Расширенный алгоритм Евклида и его алгоритмическая сложность
4. Взаимно простые числа, критерий взаимной простоты
5. Наименьшее общее кратное
6. Простые числа, каноническое разложение и проблема факторизации
7. Основные свойства сравнений
8. Классы вычетов, леммы о пробегании
9. Функция Эйлера
10. RSA-криптосистема
11. Сравнения первой степени
12. Системы сравнений первой степени, китайская теорема об остатках
13. Свойства показателей
14. Первообразные корни и индексы
15. Задача дискретного логарифма. Протокол Диффи-Хеллмана
16. Факторизация RSA-модуля при известной секретной экспоненте
17. Криптосистема Рабина
18. Связь извлечения квадратного корня по модулю и факторизации модуля
19. Группа, примеры, простейшие свойства, симметрические группы
20. Нормальные подгруппы. Факторгруппы
21. Конечные циклические группы
22. Определение, примеры и простейшие свойства колец и полей
23. Кольца. Идеалы колец, максимальные идеалы

24. Гомоморфизмы колец, факторкольца
25. Расширения полей конечной степени
26. Структура конечных полей
27. Эллиптические кривые над конечными полями
28. Задача дискретного логарифмирования на эллиптических кривых
29. Сравнение криптографии на эллиптических кривых с RSA.
30. Групповые коды, расстояние Хэмминга, декодирование по лидерам смежных классов
31. Линейные коды, кодовое расстояние и корректирующая способность кода
32. Каноническая проверочная матрица, каноническая кодирующая матрица, код Хэмминга

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола) ¹
Учебная дисциплина не требует согласования			

Заведующий кафедрой
высшей математики
доктор физико-математических наук,
профессор



М.М. Васьковский

«24» мая 2024 г.

**ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО
ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ**

на ____/____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 202_ г.)

Заведующий кафедрой

УТВЕРЖДАЮ
Декан факультета
