Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«19» _____ 2024 г.

Регистрационный № УД-4192/уч.

АРИФМЕТИЧЕСКИЕ И АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

Учебная программа учреждения образования
по учебной дисциплине для специальности
6-05-0533-12 «Кибербезопасность»

2024 г

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 6-05-0533-12-2023 и учебного плана специальности 6-05-0533-12 «Кибербезопасность». Регистрационный №14-23/уч. ФКНЭ от 04.04.2023 г. для дневной формы получения высшего образования.

СОСТАВИТЕЛЬ:

Козлов Александр Александрович, доцент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой», кандидат физ.-мат. наук, доцент,

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 10 от «18» 11 2024 г.)

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 3 от «19» 12 2024 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цель учебной дисциплины заключается во введении студентов в математические проблемы криптографии и в разборе основных способов решения таких проблем.

Основными **задачами** учебной дисциплины являются исследование и применение математических методов криптографии, а также развитие у студентов соответствующих навыков для работы с зашифрованной информацией.

При изложении материала учебной дисциплины важно показать возможности использования математических методов при решении криптографических задач, возникающих в различных областях криптографии.

Целесообразно выделить моменты построения математических моделей естественных процессов с целью их последующего изучения, а также обратить внимание на алгоритмические аспекты получаемых результатов.

В результате изучения учебной дисциплины «Арифметические и алгебраические основы криптографии» формируются следующие компетенции:

специализированные:

- Владеть базовыми принципами построения и анализа математических моделей типовых задач дискретной математики, интерпретировать получаемые результаты анализа математических моделей и осуществлять выбор структур данных для разработки эффективных алгоритмов решения прикладных задач;
- Применять статистические методы для анализа стойкости криптографических алгоритмов и тестирования датчиков случайных и псевдослучайных чисел;
- Владеть основными методами построения надежных криптосистем, функций хеширования и систем электронной цифровой подписи;
- Владеть методами построения надежных блочных и поточных криптосистем, функций хеширования, криптосистем с открытым ключом и систем электронной цифровой подписи.

В результате изучения учебной дисциплины «Арифметические и алгебраические основы криптографии» обучающийся должен

знать:

- теорию делимости целых чисел, в том числе решето Эратосфена, алгоритм Евклида;
- различные мультипликативные функции на множестве натуральных чисел (напр., функцию Эйлера);
- символы Лежандра и Якоби;
- теорию многочленов над конечными полями;

уметь:

- находить классы вычетов по различным модулям;
- решать сравнения первой степени и их системы;
- находить решения квадратичных сравнений;
- применять теоремы Вильсона, Эйлера, малую теорему Ферма;
- находить дискретные логарифмы от классов вычетов;
- получать псевдослучайные числа, например, псевдоквадраты целых чисел;

- с помощью различных тестов (в том числе теста Соловея-Штрассена) определять простоту чисел;
- производить операции над элементами конечных групп;
- использовать полученные методы теории чисел в криптографии;

владеть:

- методами аналитического и численного решений уравнений в целых числах;
- навыками творческого аналитического мышления.

Связи с другими учебными дисциплинами.

Учебная дисциплина «Арифметические и алгебраические основы криптографии» основывается на учебной дисциплине «Аналитическая геометрия и линейная алгебра», и, в свою очередь, является базой при изучении учебной дисциплины «Криптографический инжиниринг».

Форма получения образования – дневная.

В соответствии с учебным планом специальности на изучение учебной дисциплины «Арифметические и алгебраические основы криптографии» отводится:

Виды занятий, формы контроля знаний	Дневная форма обучения
Курсы	2
Семестры	4
Лекции (количество часов)	34
Практические занятия (количество часов)	18
Лабораторные занятия (количество часов)	16
Аудиторных часов по учебной дисциплине	68
Самостоятельная работа (количество часов)	40
Всего часов	108
Трудоемкость учебной дисциплины, з.е.	3
Форма промежуточной аттестации	зачет

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. ВВЕДЕНИЕ В МАТЕМАТИЧЕСКИЕ ПРОБЛЕМЫ КРИПТОГРАФИИ. ОСНОВЫ ТЕОРИИ ЧИСЕЛ

Тема 1. I Делимость.

Делимость, простые числа, наибольший общий делитель.

Тема 1.2 Алгоритм Евклида.

Алгоритм Евклида, расширенный алгоритм Евклида. Нахождение наибольшего общего делителя при помощи алгоритма Евклида, наименьшего общего кратного. Построение таблицы первых простых чисел с помощью решета Эратосфена. Нахождение канонического разложения числа на простые сомножители.

Тема 1.3 Цепные дроби.

Цепные дроби. Разложение дробей в цепные дроби при помощи алгоритма Евклида. Асимптотический закон распределения простых чисел — вычисление примерного количества простых чисел на заданном интервале.

Тема 1.4 Функция Эйлера.

Мультипликативные функции. Функция Эйлера.

Раздел 2. ТЕОРИЯ СРАВНЕНИЙ. ВЫЧЕТЫ.

Тема 2.1 Система вычетов по модулю.

Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z*p. Построение приведенной системы вычетов от по заданному модулю.

Тема 2.2 Алгебраические структуры на целых числах.

Обратный элемент в Zn. Вычисление обратного элемента в Zn при помощи расширенного алгоритма Евклида. Алгебраические структуры на целых числах.

Тема 2.3 Элементарные теоремы теории чисел и их применение в криптографии.

Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения при помощи теоремы Эйлера.

Раздел 3. СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ.

Тема 3.1 Линейные сравнения.

Сравнения первой степени и их решения.

Тема 3.2 Системы сравнений первой степени и их применение в криптографии.

Системы сравнений первой степени и их решение. Китайская теорема об остатках и ее применения в криптографии (схема разделения секрета на ее основе и ее применение в RSA).

Раздел 4. КВАДРАТИЧНЫЕ СРАВНЕНИЯ И КРИПТОСИСТЕМЫ НА ИХ ОСНОВЕ.

Тема 4.1 Квадратичные сравнения.

Квадратичные сравнения. Символ Лежандра. Закон взаимности. Существование решений квадратичного сравнения по простому модулю.

Тема 4. 2 Квадратичные сравнения по простому модулю.

Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства.

Тема 4.3 Квадратичные сравнения по составному модулю.

Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных уравнений по составному модулю.

Тема 4.4 Квадраты и псевдоквадраты чисел, их применение в криптографии.

Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.

Раздел 5. ПОРОЖДАЮЩИЙ ЭЛЕМЕНТ И ДИСКРЕТНЫЙ ЛОГАРИФМ.

Тема 5.1 Дискретный логарифм и его применение в криптографии.

Циклическая группа Zp (Up). Порождающий элемент и дискретный логарифм). Отыскание порождающего элемента. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля.

Тема 5.2 Простота чисел. Генерация простых чисел.

Теоремы Сэлфриджа и Поклингтона. (п-1) — тесты на простому. Тест Рабина-Миллера. Тест Соловея-Штрассена на простому. Вероятностные тесты на простоту. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса- Лемера. Теорема Диемитко и процедура генерации простых чисел.

РАЗДЕЛ 6. КОНЕЧНЫЕ ГРУППЫ И ПОЛЯ МНОГОЧЛЕНОВ.

Тема 6.1 Многочлены над простыми поляки.

Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов.

Тема 6.2 Приводимость многочлены над полем. Теория Галуа.

Неприводимые многочлены, проверка многочлена на простоту. Нахождение обратного. Поля Галуа.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ «АРИФМЕТИЧЕСКИЕ И АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ»

(дневная форма получения высшего образования)

Номер раздела, темы	Название раздела, темы.	Количество аудиторных					Литература	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Управляемой самостоятельной		
1	2	3	4	5	6	7	8	9
АРИФМЕТИЧЕСКИЕ И АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ (68 часов)		**34**	**18**		**16**			
IV семестр		**34**	**18**		**16**			
	Раздел 1. Введение в математические проблемы криптографии. Основы теории чисел	**8**	**4**		**4**			
Тема 1.1	Делимость, простые числа, наибольший общий делитель.	2	2				[1] с. 10-20 [5], 41- 45, [11]	
Тема 1.2	Алгоритм Евклида, расширенный алгоритм Евклида. Нахождение наибольшего общего делителя при помощи алгоритма Евклида, наименьшего общего кратного. Построение таблицы первых простых чисел с помощью решета Эратосфена. Нахождение канонического разложения числа на простые сомножители.	2			2		[1] с. 23-31 [7], с. 50- 55, [11]	ПДЗ, УО
Тема 1.3	Цепные дроби. Разложение дробей в цепные дроби при помощи алгоритма Евклида. Асимптотический закон распределения простых чисел.	2	2				[1] с. 45-47 [8], с. 10- 35, [11]	ПДЗ, УО
Тема 1.4	Мультипликативные функции. Функция Эйлера.	2			2		[3] с. 33-43 [11]	УО, ИДЗ
	Раздел 2. Теория сравнений. Вычеты.	**6**	**4**		**2**			
Тема 2.1	Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z*p. Построение приведенной системы вычетов от по заданному модулю.	2	2				[1] с. 48-51, [6], [7], [8]	УО
Тема 2.2	Обратный элемент в Zn. Вычисление обратного элемента в Zn при помощи расширенного алгоритма Евклида. Алгебраические структуры на целых числах.	2	2				[5] с. 48-52, [9], [10]	ИДЗ
Тема 2.3	Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения при помощи теоремы Эйлера	2			2		[1] с. 44-52, с. 65-72, [9], [10]	УО ПДЗ

	Раздел 3. Сравнения первой степени.	**4**	**2**		**2**			
Тема 3 1	Сравнения первой степени и их решения.	2	2				[2] с. 14-52, [3], с. 10-15	УО
Тема 3 2	Системы сравнений первой степени и их решение. Китайская теорема об остатках и ее применения в криптографии (схема разделения секрета на ее основе и ее применение в RSA).	2			2			ПДЗ, ИДЗ РКР*
	Контрольная работа «Основы теории чисел».							
	Раздел 4. Квадратичные сравнения и криптосистемы на их основе.	**8**	**4**		**4**			
Тема 4.1	Квадратичные сравнения. Символ Лежандра. Закон взаимности. Существование решений квадратичного сравнения по простому модулю.	2	2				[6] с. 54-60, 60-62, [11]	
Тема 4.2	Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства.	2			2		[4] с. 60-65, 65-68, [5], [11]	ПДЗ, УО
Тема 4.3	Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных уравнений по составному модулю.	2	2				[4] с. 59-63, 70-82, [5], [9]	
Тема 4.4	Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.	2			2		[4] с. 39-41, 83-86, [5], [9], [10]	УО, ПДЗ
	Раздел 5. Порождающий элемент и дискретный логарифм	**4**	**2**		**2**			
Тема 5.1	Циклическая группа Zp (Up). Порождающий элемент и дискретный логарифм). Отыскание порождающего элемента. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля.	2	2				[1], с 313-320 [9], [10]	ИДЗ
Тема 5.2	Теоремы Сэлфриджа и Поклингтона. (п-1) — тесты на простому. Тест Рабина-Миллера. Тест Соловея-Штрассена на простобу. Вероятностные тесты на простоту. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера. Теорема Диемитко и процедура генерации простых чисел.	2			2		[1], с 325-350 [5] [5], [7]	УО
	Раздел 6. ***Конечные группы и поля многочленов.***	**4**	**2**		**2**			
Тема 6.1	Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов.	2	2				[2], с 380-390 [11]	УО, ИДЗ

Тема 6.2	Неприводимые многочлены, проверка многочлена на простоту. Нахождение обратного. Поля Галуа.	2			2		[2], с 351-360 [10]	

Принятые сокращения:

ИДЗ - индивидуальное домашнее задание

ПДЗ - проверка домашнего задания

УО - устный опрос, в том числе и экспресс-опрос;

РКР- рейтинговая контрольная работа.

*мероприятия текущего контроля

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Деза, Е.И. Введение в криптографию. Теоретико-числовые основы защиты информации: учебное пособие / Е. И. Деза, Л. В. Котова. - издание стереотипное. - Москва : ЛЕНАНД, 2022. - 368 с.
2. Введение в теоретико-числовые методы криптографии : учебное пособие для вузов / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2024. — 396 с. - Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/397286 (дата обращения: 16.01.2025).
3. Мартынов, Л. М. Алгебра и теория чисел для криптографии / Л. М. Мартынов. — Санкт-Петербург : Лань, 2024. — 456 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/362942 (дата обращения: 16.01.2025).
4. Фомичев, В.М. Криптографические методы защиты информации: учебник для вузов : в 2 частях. Часть 1. Математические аспекты / В. М. Фомичев, Д. А. Мельников ; под редакцией В.М. Фомичева. - Москва : Юрайт, 2023. - 209 с. - Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.
5. Фомичев, В.М. Криптографические методы защиты информации : учебник для вузов : в 2 частях. Часть 2. Системные и прикладные аспекты / В. М. Фомичев, Д. А. Мельников ; под редакцией В.М. Фомичева. - Москва: Юрайт, 2023. - 245 с. - Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.
6. Васильева, И.Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва: Юрайт, 2023. - 349 с. - Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника и практикума для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.
7. Романьков, В.А. Введение в криптографию : курс лекций / В. А. Романьков. - 2 издание, исправленное и дополненное. - Москва : ИНФРА-М, 2023. - 234 с. - Рекомендовано в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям подготовки 01.03.01 "Математика", 02.03.01 "Математика и компьютерные технологии", 01.03.02 "Прикладная математика и информатика" (квалификация(степень) "бакалавр").
8. Вонг, Д. Реальная криптография = Real-World Cryptography / Д. Вонг ; пер. с англ. Д. Романовская. - Санкт-Петербург: Питер, 2024. - 432 с.

Турнова Е. В.

Дополнительная:

9. Введение в криптологию: учебное пособие в 4 частях / Ю. В. Кулаком, О. Г. Иванова, СІ. Г. Шахоп, А. И.Елисеев. — Тамбов : ТГУ, 2021. Часть 1 – 2021. — 84 с. —URL: https://e.lanbook.com/book/ 362942 /320465 (дата обращения: 20.01 .2025).

10. Котов, Ю. А. Криптографические методы защиты информации: учебное пособие /Ю. А. Котов. — Новосибирск: НГУ, 201 6. – 59 с. Текст: электронный // Лань. — URI.: https://e.lanbook.com/book/118209 (дата обращения: 20.01.2025).

11. Бухштаб А.А. Теория чисел [Учеб. пособие для физ.-мат. фак. пед. интов]. — 2-е изд., испр. — Москва : Просвещение, 1966. — 384 с.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

1. Делимость, простые числа.
2. Наибольший общий делитель и его свойства.
3. Алгоритм Евклида.
4. Расширенный алгоритм Евклида.
5. Цепные дроби.
6. Мультипликативные функции и их свойства.
7. Функция Эйлера и ее основные свойства.
8. Полная и приведенная система вычетов,
9. Множества Zn, Zp, Z*n, Z*p.
10. Обратный элемент в Zn Алгебраические структуры на целых числах.
11. Теорема Эйлера и теорема Ферма.
12. Тест Ферма на простоту.
13. Криптосистема RSA. Основные положения.
14. Сравнения первой степени. Методы их решения.
15. Системы уравнений первой степени и их решение.
16. Понижение степени в сравнениях.
17. Китайская теорема об остатках.
18. Применение китайской теоремы об остатках в криптографии (схема разделения секрета на ее основе и ее применение в RSA).
19. Квадратичные сравнения.
20. Символ Лежандра и его свойства.
21. Закон взаимности и его применение.
22. Существование решений квадратичного сравнения по простому модулю
23. Решение квадратичных сравнений по простому модулю.
24. Символ Якоби и его свойства.
25. Существование и количество решений квадратичного сравнения по составному модулю.
26. Решение квадратичных сравнений по составному модулю.
27. Квадраты и псевдоквадраты.
28. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации.
29. Числа Блюма. BBS-генератор.
30. Криптосистемы Блюма-Гольдвассер и Гольдвассер-Микали.
31. Циклические группы Zp и Up.
32. Порождающий элемент и вычисление дискретного логарифма.
33. Задача дискретного логарифмирования.
34. Криптосистема Диффи-Хэллмана. Основные положения.
35. Криптосистема Эль-Гамаля. Основные положения
36. Теоремы Сэлфриджа и Поклингтона.
37. (n-1)-тесты на простоту.
38. Тест Рабина-Миллера.
39. Тест Соловея-Штрассена на простоту.

40. Вероятностные тесты на простоту.

41. Числа Ферма, теорема Пепина, тест Пепина.

42. Числа Мерсена и тест Лукаса- Лемера.

43. Теорема Диемитко и процедура генерации простых чисел.

44. Многочлены над Zp, Zn. Операции сложения и умножения, а также факторизация многочленов.

45. Неприводимые многочлены.

46. Поля Галуа.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Цель самостоятельной работы студентов — содействие усвоению в полном объеме содержания учебной дисциплины и формирование самостоятельности как личностной черты и важного профессионального качества, сущность которых состоит в умении систематизации, планирования и контроля собственной деятельности. Задача самостоятельной работы студентов — усвоение определенных стандартом знаний, умений и навыков по учебной дисциплине, закрепление и систематизация полученных знаний, их применение при выполнении практических заданий и творческих работ, а также выявление пробелов в системе знаний по учебной дисциплине.

При изучении дисциплины используются следующие формы самостоятельной работы:

— выполнение домашних заданий (в т.ч. индивидуальных);

— составление информационных таблиц, графических схем и глоссариев по пройденным темам.

Методы планирования и организации самостоятельной работы студентов

- анализ учебной программы по учебной дисциплине «Арифметические и алгебраические основы криптографии» с целью выделения тематических блоков для самостоятельной работы студентов;
- проработка баланса времени, необходимого для самостоятельной работы студентов с выделенными тематическими блоками;
- структурирование тематических заданий, ориентированных на формирование и развитие компетенций студентов в контексте самостоятельной работы.

Содержание самостоятельной работы студентов дневной формы получения высшего образования

Вид работы	Тематическое содержание	Используемые источники	К-во часов
			IV сем.
Углубленное изучение теоретической части учебной дисциплины	**Раздел 1. Введение в математические проблемы криптографии. Основы теории чисел.** *Рассмотреть в научной литературе основные вопросы, связанные с криптографией в современном мире.*	[1, 3, 8, 11]	6
	Раздел 2. Теория сравнений. Вычеты. *- Изучить конспект лекций по данной теме.* *- Проработать задания, вынесенные на самостоятельную работу* *- Численно и, по возможности, символьно решить задания, предложенные для самостоятельной (домашней) работы, на одном из языков программирования C++, Python, Java, а также используя один из математических пакетов (MAPLE, Mathematica, MATLAB).*	[2, 3, 8, 9, 11]	6
	Раздел **3. Сравнения первой степени.** - *Изучить конспект лекций по данной теме.* *- Проработать задания, вынесенные на самостоятельную работу* *- Численно и, по возможности, символьно и решить задания, предложенные для самостоятельной (домашней) работы, на одном из языков программирования C++, Python, Java, а также используя один из математических пакетов (MAPLE, Mathematica, MATLAB).* *- Изучить применение сравнений первой степени в криптографических методах шифрования.* *Выполнить задания теста.*	[2, 3, 8, 10, 11]	6
	Раздел 4. Квадратичные сравнения и криптосистемы на их основе. *- Изучить конспект лекций по данной теме.* *- Проработать задания, вынесенные на самостоятельную работу* *- Численно и, по возможности, символьно решить задания, предложенные для самостоятельной (домашней) работы, на одном из языков программирования C++, Python, Java, а также используя один из математических пакетом (MAPLE, Mathematica, MATLAB).* *- Изучить применение квадратичных*	[4, 5, 6, 7, 9, 10, 11]	6

	сравнений в криптографических методах шифрования. *Выполнить задания теста*		
	Раздел 5. Порождающий элемент и дискретный логарифм. *- Изучить конспект лекций по данной теме.* *- Проработать задания, вынесенные на самостоятельную работу* *- Численно и, по возможности, графически решить задания, предложенные для самостоятельной (домашней) работы, на одном низ языков программирования C++, Python, Java, а maiaice используя один из математических пакетов (MAPLE, Mathematica, MATLAB).* *- Изучить применение дискретного логарифма в криптографических методах шифрования.*	[4, 5, 6, 7, 8, 9, 10]	6
	Раздел 6. Конечные группы и поля многочленов. *- Изучить информационную таблицу раздела, графическую схему раздела, глоссарий.* *- Проработать задания, вынесенные на самостоятельную работу* *- Изучить применение конченых групп и полей в шифровании.*	[4, 5, 6, 7, 10, 11]	6
	Подготовка рейтинговой контрольной работе	Конспект лекционных и практических занятий	4
Всего часов			**40**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Средства диагностики результатов учебной деятельности:

для оценки достижений студентов используется следующий диагностический инструментарий:

- индивидуальное домашнее задание
- проверка домашнего задания;
- письменная контрольная работа;
- устный опрос во время занятий.

Диагностика качества усвоения знаний проводится в форме текущего контроля и промежуточной аттестации.

Мероприятия текущего контроля проводятся в течение семестра и включают в себя следующие формы контроля: рейтинговая контрольная работа.

Отметка текущего контроля за семестр определяется по результату рейтинговой контрольной работы.

Форма промежуточной аттестации -зачет.

Заключение о зачете формируется по формуле:

$$З=k\times T,$$

где k— весовой коэффициент текущего контроля; Т — результат текущего контроля за семестр. Весовой коэффициент k принимается равным 1.

Если полученная отметка З<4 баллов, то проводится устный зачет отдельно по представленным в программе вопросам.

Перевод отметки по зачету осуществляется по следующим правилам: отметка «зачтено» выставляется студентам, получившим от 4 до 10 баллов, отметка «не зачтено» выставляется студентам, получившим от 1 до 3 баллов.

Примерное содержание билета для зачета по дисциплине «Арифметические и алгебраические основы криптографии»

1. НОД и НОК и их свойства.

2. Представить число в виде цепной дроби $-\frac{649}{125}$.

3. Найдите группу Z_9^* обратимых элементов для кольца Z_9.

ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРОГРАММ

MATHCAD 2000 PROFESSIONAL и выше, MATLAB 5 и выше.

Языки программирования: C++, Python, Java.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основной методической системой для организации учебного процесса по дисциплине «Арифметические и алгебраические основы криптографии» являются учебники, спроектированные с точки зрения полипарадигмального подхода (комплексного взаимодействия *системно-деятельностного, дифференцированного, модульного, когнитивно-визуального, компетентност-ного подходов)* с целью максимального использования его потенциальных возможностей в конкретном дидактическом процессе обучения данной дисциплине студентов. Указанная методическая система базируется на общедидактических принципах обучения (*научности, структуризации; информационной системности и целостности; доступности; пролонгации, профессиональной направленности, развивающей деятельности, реализации обратной связи в обучении дифференциальной геометрии, пролонгации, профессиональной направленности, развивающего обучения и других).*

Используемые методы обучения:

-методы проблемного обучения (проблемное изложение, частично-поисковый и исследовательский методы);

-личностно ориентированные (развивающие) технологии, основанные на активных (рефлексивно-деятельностных) формах и методах обучения («мозговой штурм», дискуссия, пресс-конференция);

-информационно-коммуникационные технологии, обеспечивающие проблемно-исследовательский характер процесса обучения и активизацию самостоятельной работы студентов (структурированные электронные презентации для лекционных занятий, использование аудио-, видеоподдержки учебных занятий, видио-лекции, применение специализированных компьютерных программ MATHCAD PROFESSIONAL и MATLAB, а также языков программирования C++, Python, Java).

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название 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)
Криптографический инжиниринг	математики и компьютерной безопасности	Предложений и замечаний нет	