Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Проректор по учебной работе учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
_____ Ю.П. Голубев
«28» 11 2022 г.

Регистрационный № УД-4831/22уч.

МОДУЛЬ «КРИПТОГРАФИЯ»

АРИФМЕТИЧЕСКИЕ И АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
1-98 01 01 «Компьютерная безопасность (по направлениям)»
направление специальности 1-98 01 01-01 «Компьютерная безопасность (математические методы и программные системы)»

2022 г.

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 1-98 01 01-2021 и учебного плана по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)». Регистрационный № 21-21/уч. ФКНЭ от 26.07.2021г. для дневной формы получения высшего образования.

СОСТАВИТЕЛИ:
КОЗЛОВ АЛЕКСАНДР АЛЕКСАНДРОВИЧ, доцент, кандидат физико-математических наук, доцент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
УСТЮГОВ ВЛАДИСЛАВ ВАЛЕРЬЕВИЧ, ассистент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 10 от «20» 10 2022 г.)

Методической комиссией факультета компьютерных наук и электроники учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 10 от «25» 11 2022 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цель учебной дисциплины «Арифметические и алгебраические основы криптографии»: введение в математические проблемы криптографии и разбор основных способов их решения.

Основные задачи учебной дисциплины: исследование и применения математических методов криптографии, 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.

Учебная дисциплина «Арифметические и алгебраические основы криптографии» основывается на учебных дисциплинах «Линейная алгебра», «Аналитическая геометрия» и, в свою очередь, является базовой при изучения учебной дисциплиы «Криптографические методы».

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

знать:

- методы интегрирования линейных стационарных дифференциальных уравнений и систем;
- методы интегрирования элементарных дифференциальных уравнений;
- условия существования и единственности решения задачи Коши;
- понятия первого интеграла и базиса первых интегралов;
- основные понятия теории устойчивости;
- схему построения решений линейных однородные и квазилинейных уравнений с частными производными первого порядка;
- принципы построения дифференциальных моделей;

уметь:

- использовать методы Лагранжа, Коши, Эйлера при построение общего решения и решения задачи Коши линейных дифференциальных уравнений и систем с постоянными коэффициентами;
- интегрировать элементарные дифференциальные уравнения;
- находить первые интегралы и строить их базис для нелинейных дифференциальных систем;
- исследовать устойчивость и асимптотическую устойчивость решений дифференциальных уравнения и систем;
- интегрировать линейные однородные и квазилинейные уравнения с частными производными первого порядка;
- строить и исследовать дифференциальные модели эволюционных процессов;

владеть:

- методами аналитического и численного решения алгебраических уравнений;
- навыками творческого аналитического мышления.

Подготовка специалиста при обучении дисциплине «Арифметические и алгебраические основы криптографии» должна обеспечивать формирование группы компетенций:

Специализированные компетенции:

– СК-8: владеть базовыми принципами построения и анализа математических задач дискретной математики, интерпритировать получаемые результаты анализа математических моделей и осуществлять выбор структур данных для разработки эффективных алгоритмов решения прикладных задач.

– СК-11: применять статистические методы для анализа стойкости криптографических алгоритмов и тестирования датчиков случайных и псевдослучайных чисел.

– СК-14: владеть основными методами построения надежных криптосистем, функций хеширования и систем электронной цифровой подписи.

– СК-20: владеть методами построения надежных блочных и поточных криптосистем, функций хеширования, криптосистем с открытым ключом и систем электронной цифровой подписи.

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

	Дневная форма обучения
Курс	2
Семестр	4
Лекции (количество часов)	34
Лабораторные занятия (количество часов)	16
Практические занятия (количество часов)	16
Аудиторных часов по учебной дисциплине	66
Всего часов по учебной дисциплине	108
Самостоятельная работа (количество часов)	42
Трудоемкость учебной дисциплины (зачетные единицы)	3
Формы промежуточной аттестации	зачет

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

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

Тема 1.1 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. 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 1.3 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 сравнений 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. (n-1) – тесты на простоту. Тест Рабина-Миллера. Тест Соловея-Штрассена на простоту. 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 полями.
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 образования)

Номер раздела, темы	Название раздела, темы.	Количество аудиторных часов					Литература	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Управляемой самостоятельной работы студента		
1	2	3	4	5	6	7	8	9
Арифметические и алгебраические основы криптографии		**34**	**16**		**16**			
	Раздел 1. ***Введение в математические проблемы криптографии. Основы теории чисел***	**6**	**4**		**4**			
1.1	Делимость, простые числа, наибольший общий делитель.	2			2		[1] [2] с. 34-67	

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. Цепные дроби. Разложение дробей в цепные дроби при помощи алгоритма Евклида. Асимптотический закон распределения простых чисел – вычисление примерного количества простых чисел на заданном интервале.	2	2		2		[1] [2] с. 34-67	ИДЗ *
1.3	Мультипликативные функции. Функция Эйлера.	2	2				[1] [2] с. 34-67	УО
	Раздел 2. ***Теория сравнений. Вычеты.***	**6**	**2**		**2**			
2.1	Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z*p. Построение приведенной системы вычетов от по заданному модулю	2					[3] [6] с. 104-138	
2.2	Обратный элемент в Zn. Вычисление обратного элемента в Zn при помощи расширенного алгоритма Евклида. Алгебраические структуры на целых числах.	2			2		[3] [6] с. 104-138	
2.3	Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения при помощи теоремы Эйлера.	2	2				[3] [6] с. 104-138	
	Раздел 3. ***Сравнения первой степени.***	**4**	**2**		**2**			
3.1	Сравнения первой степени и их решения.	2			2		[4] [7] с. 78-95	

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				[4] [7] с.78-95	МСР*
	Раздел 4. ***Квадратичные сравнения и криптосистемы на их основе***	**8**			**8**			
4.1	Квадратичные сравнения. Символ Лежандра. Закон взаимности. Существование решений квадратичного сравнения по простому модулю.	2 2			2		[5] [7] с.111-147	
4.2	Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства.	2	2				[5] [7] с.111-147	
4.3	Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных сравнений по составному модулю.	2			2		[5] [7] с.111-147	ИДЗ*
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				[5] [7] с.111-147	ЛПР*
	Раздел 5. ***Порождающий элемент и дискретный логарифм***	**4**	**2**		**2**			
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		[5] [7] с.111-147	

5.2	Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Тест Рабина-Миллера. Тест Соловея-Штрассена на простоту. 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				[5] [7] с. 111-147	УО
	Раздел 6. ***Конечные группы и поля многочленов***	**4**	**2**		**2**			
6.1	Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов.	2			2		[5] [9] с. 135-160	РКР*
6.2	Неприводимые многочлены, проверка многочлена на простоту. Нахождение обратного. Поля Галуа.	2	2				[5] [9] с. 135-160	

Принятые сокращения:
ИДЗ – индивидуальное домашнее задание;
ЛПР – лекционная проверочная работа;
МСР – мини-самостоятельная работа;
УО – устный опрос, в том числе и экспресс-опрос;
РКР – рейтинговая контрольная работа.

* мероприятия текущего контроля

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

ОСНОВНАЯ:

1. Введение в криптологию : учебное пособие : в 4 частях / Ю. В. Кулаков, О. Г. Иванова, Н. Г. Шахов, А. И. Елисеев. — Тамбов : ТГТУ, 2021 — Часть 1 — 2021. — 84 с. — ISBN 978-5-8265-2367-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/320465 (дата обращения: 20.01.2022).

2. Котов, Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов. — Новосибирск : НГТУ, 2016. — 59 с. — ISBN 978-5-7782-2959-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118209 (дата обращения: 20.01.2022).

3. Ильин, М. Е. Теоретико-числовые методы в криптографии : учебное пособие / М. Е. Ильин, К. А. Ципоркова. — Рязань : РГРТУ, 2020 — Часть 1 — 2020. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168360 (дата обращения: 20.01.2022).

4. Мартынов, Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 3 — 2018. — 83 с. — ISBN 978-5-949-41189-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129190 (дата обращения: 20.01.2022).

5. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2022. — 400 с. — ISBN 978-5-8114-1116-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/210746 (дата обращения: 20.01.2022).

ДОПОЛНИТЕЛЬНАЯ:

6. Элементы векторной алгебры. Элементы аналитической геометрии на плоскости и в пространстве : учебно-методический комплекс для студентов технических специальностей / Министерство образования Республики Беларусь, Полоцкий государственный университет ; под общей редакцией В.С. Вакульчик. - Новополоцк : ПГУ, 2009. - 219 с.

Чурилова Е. В.

7. Элементы линейной алгебры. Введение в математический анализ. Дифференциальное исчисление функции одной переменной : учебно-методический комплекс для студентов технических специальностей / Министерство образования Республики Беларусь, Полоцкий государственный университет ; составление и общая редакция В.С. Вакульчик. - Новопо- лоцк : ПГУ, 2007.- 351 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. Асимптотический закон распределения простых чисел.
7. Мультипликативные функции и их свойства.
8. Функция Эйлера и ее основные свойства.
9. Полная и приведенная система вычетов,
10. Множества Zn, Zp, Z*n, Z*p.
11. Обратный элемент в Zn Алгебраические структуры на целых числах.
12. Теорема Эйлера и теорема Ферма.
13. Тест Ферма на простоту.
14. Криптосистема RSA. Основные положения.
15. Понижение степени сравнения.
16. Сравнения первой степени. Методы их решения.
17. Системы сравнений первой степени и их решение.
18. Китайская теорема об остатках.
19. Применение китайской теоремы об остатках в криптографии (схема разделения секрета на ее основе и ее применение в RSA).
20. Квадратичные сравнения.
21. Символ Лежандра и его свойства.
22. Закон взаимности и его применение.
23. Существование решений квадратичного сравнения по простому модулю.
24. Решение квадратичных сравнений по простому модулю.
25. Символ Якоби и его свойства.
26. Существование и количество решений квадратичного сравнения по составному модулю.
27. Решение квадратичных сравнений по составному модулю.
28. Квадраты и псевдоквадраты.
29. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации.
30. Числа Блюма. BBS-генератор.
31. Криптосистемы Блюма-Гольдвассер и Гольдвассер-Микали.
32. Циклическая группа Zp (Up).
33. Порождающий элемент и дискретный логарифм.
34. Задача дискретного логарифмирования.
35. Криптосистема Диффи-Хэллман. Основные положения.
36. Криптосистема Эль-Гамаля. Основные положения
37. Теоремы Сэлфриджа и Поклингтона.
38. (n-1) – тесты на простоту.
39. Тест Рабина-Миллера.

40. Тест Соловея-Штрассена на простоту.
41. Вероятностные тесты на простоту.
42. Числа Ферма, теорема Пепина, тест Пепина.
43. Числа Мерсенна и тест Лукаса- Лемера.
44. Теорема Диемитко и процедура генерации простых чисел.
45. Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов.
46. Неприводимые многочлены.
47. 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 образования (42 часа)

Тематическое содержание	Используемые источники	Количество часов
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, 9	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	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, 9	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 пакетов (MAPLE, Mathematica, MATLAB). - Изучить применение квадратичных сравнений в криптографических методах шифрования. - Выполнить задания теста*	4, 5, 6, 7	8
Раздел 5. Порождающий элемент и дискретный логарифм. *- Изучить конспект лекций по данной теме.*	4, 5, 6, 7	8

- Проработать задания, вынесенные на самостоятельную работу *- Численно и, по возможности, графически 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 дискретного логарифма в криптографических методах шифрования.*		
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	8
Всего		**42**

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Методы обучения:

— методы проблемного обучения (проблемное изложение, частично-поисковый и исследовательский, а также проектный 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, примененение специализированных компьютерных программ Microsoft Word, Microsoft Office Excel, SPSS, MATHCAD PROFESSIONAL, MAPLE, MATLAB, POWERPOINT, MS ACCESS, MS VISI).

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Средства диагностики результатов учебной деятельности:

Для оценки достижений студентов используется следующий диагностический инструментарий:

- устный опрос, в том числе и экспресс-опрос;
- письменные проверочные работы (микроконтрольные);
- рейтинговая контрольная работа;
- индивидуальное домашнее задание.

Форма промежуточной аттестации зачет.

Заключение о *зачете* формируется по формуле:

$$З = k \cdot Т,$$

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.

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

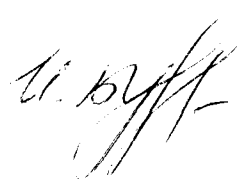
ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРОГРАММ

Microsoft Office Excel ver. 2003 и выше, MATHCAD 2010 PROFESSIONAL и выше, MAPLE 15 и выше, MATLAB 6 и выше.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО ДИСЦИПЛИНЕ «АРИФМЕТИЧЕСКИЕ И АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ» С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по дисциплине «Арифметические и алгебраические основы криптографии»	Решение, принятое кафедрой математики и компьютерной безопасности
Криптографические методы	математики и компьютерной безопасности	Предложений и изменений нет	
Линейная алгебра	математики и компьютерной безопасности	Предложений и изменений нет	
Аналитическая геометрия	математики и компьютерной безопасности	Предложений и изменений нет	

Заведующий кафедрой математики
и компьютерной безопасности,
кандидат технических
наук, доцент



И.Б. Бураченок