

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УТВЕРЖДАЮ

Проректор по учебной работе
и менеджменту качества

_____ Е. Н. Живицкая

26.06.2014г.

Регистрационный № УД -5-92/р.

«Прикладная математика»

Учебная программа учреждения высшего образования
по учебной дисциплине
для специальности

1-98 01 02 Защита информации в телекоммуникациях

Кафедра высшей математики

Всего часов по дисциплине	90
------------------------------	----

Зачетных единиц	2,5
-----------------	-----

2014 г.

Группа составителей:

О. А. Мокеева, доцент кафедры высшей математики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат физико-математических наук, доцент;

Н. В. Спичекова, доцент кафедры высшей математики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат физико-математических наук, доцент

Учебная программа учреждения высшего образования составлена на основе учебной программы «Прикладная математика», утвержденной ректором БГУИР 25.06.2014 г., регистрационный номер № УД – 98- 062/баз. и учебного плана специальности 1-98 01 02 Защита информации в телекоммуникациях.

Рассмотрена и рекомендована к утверждению на заседании кафедры высшей математики

протокол № 15 от 04.06.2014г.

Заведующий кафедрой _____ В. В. Цегельник

Одобрена и рекомендована к утверждению Советом факультета телекоммуникаций учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

протокол № 11 от 23.06.2014г.

Председатель _____ О. Д. Чернухо

СОГЛАСОВАНО

Эксперт-нормоконтролер _____

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

План учебной дисциплины в дневной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов			Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	
1-98 01 02	Защита информации в телекоммуникациях	2	3	48	32	16	зачет

Место дисциплины.

Изучение данной дисциплины опирается на знания по математике, полученные студентами в средней школе (вопросы из теории чисел – понятие делимости, свойства делимости, простые числа, составные числа, теорема о делении с остатком и т. д.), и на первом курсе по дисциплине «Математика». Материал дисциплины создает математическую базу для изучения дисциплин: «Прикладная теория кодирования», «Цифровая обработка и защита мультимедийной информации» и других специальных дисциплин, и для решения прикладных задач.

Цель преподавания учебной дисциплины: овладение студентами основами теории чисел, основными алгебраическими структурами (группами, кольцами и полями), сформировать алгебраические умения и навыки, необходимые для изучения других дисциплин.

Задачи изучения учебной дисциплины:

- усвоение основных понятий и фактов разделов теории чисел;
- овладение основными методами решения алгебраических задач;
- формирование умений и навыков применения полученных знаний в практической деятельности;
- познакомить студентов с криптографическими системами;
- формирование абстрактного алгебраического мышления;
- стимулирование самостоятельной деятельности по освоению содержания дисциплины и формированию необходимых компетенций.

В результате изучения учебной дисциплины «Прикладная математика» формируются следующие компетенции:

академические:

- 1) умение применять базовые научно-теоретические знания для решения теоретических и практических задач;
- 2) владение системным и сравнительным анализом;
- 3) владение исследовательскими навыками;
- 4) умение работать самостоятельно;
- 5) способность порождать новые идеи (обладать креативностью);
- 6) владение междисциплинарным подходом при решении проблем;
- 7) навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером;
- 8) обладание навыками устной и письменной коммуникации;
- 9) использование основных законов естественнонаучных дисциплин в профессиональной деятельности;
- 10) владение основными методами, способами и средствами получения, хранения, переработки информации с использованием компьютерной техники;

социально-личностные:

- 1) обладание способностью к межличностным коммуникациям;
- 2) умение работать в команде;

профессиональные:

- 1) владение основами разработки программного обеспечения, общими принципами структурного программирования.

В результате изучения учебной дисциплины студент должен:

знать:

- основные понятия теории делимости в кольце целых чисел, теории сравнений;
- определения основных алгебраических структур: группы, кольца, поля; определения соответствующих подструктур и морфизмов данных структур;
- основные понятия теории колец, полей и теории полей Галуа;
- базовые понятия криптографии, основные алгоритмы шифрования данных классическими и современными криптосистемами;

уметь:

- применять теорию делимости в кольце целых чисел при решении широкого круга задач;
- применять определение и свойства сравнений по заданному модулю; вычислять остатки арифметических выражений от деления на заданное число, используя свойства сравнений и теоремы Эйлера и Ферма; проводить вычисления в кольцах классов вычетов по заданному модулю; решать различными способами линейные сравнения;
- шифровать и дешифровать информацию в криптосистемах;
- формировать конечные поля и осуществлять вычисления в конечных полях;
- пользоваться стандартными программами пакетов «MatLab», «Mathematica»;

владеть:

- навыками использования важнейших методов теории делимости, в том числе и на языке теории сравнений;
- методами вычислений в кольцах классов вычетов;
- способами шифрования данных с помощью классических и современных криптосистем;
- алгоритмами формирования конечных полей и вычислений в них;
- стандартными программами пакетов «MatLab», «Mathematica».

**Перечень учебных дисциплин, усвоение которых необходимо
для изучения данной учебной дисциплины**

№ п.п.	Название дисциплины	Раздел, темы
1.	Математика	<i>Раздел 1.</i> <i>Аналитическая геометрия и линейная алгебра</i> Матрицы. Определители. Обратная матрица. Системы линейных алгебраических уравнений. Векторы. Линейные пространства. Линейные операторы. Линейные операторы в евклидовом пространстве. <i>Раздел 4.</i> <i>Многочлены</i> Многочлены и их делимость. Теорема Безу. Основная теорема алгебры. Разложение многочлена на множители. Критерий тождественности двух многочленов

1. Содержание учебной дисциплины

№ тем	Наименование разделов, тем	Содержание тем
1	2	3
	Раздел 1. Основы теории чисел	
1.1.	Теория делимости в кольце целых чисел	Отношение делимости. Теорема о делении с остатком. Систематическая запись натуральных чисел. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Взаимно простые числа. Простые числа. Бесконечность множества простых чисел. Числа Ферма и Марсена. Решето Эратосфена. Основная теорема арифметики. Факторизация целого числа в произведение простых множителей.
1.2.	Теория сравнений	Отношение сравнимости по модулю и его основные свойства. Полная и приведенная системы вычетов. Кольцо классов вычетов по простому и составному модулю. Обратимость классов вычетов. Китайская теорема об остатках. Система сравнений первой степени. Диофантовы уравнения. Малая теорема Ферма. Функция Эйлера и ее основные свойства. Теорема Эйлера. Малая теорема Ферма. Числа Кармайкла.
	Раздел 2. Основы теории групп	
2.3.	Группы и их подгруппы	Алгебраические операции. Понятие группы, подгруппы, примеры. Порядок элемента в группе. Циклические группы. Группы подстановок. Смежные классы. Теорема Лагранжа. Нормальные подгруппы и фактор-группы.
2.4.	Гомоморфизмы и автоморфизмы групп	Определение гомоморфизма, примеры гомоморфных отображений, теоремы о гомоморфизмах. Определение автоморфизма. Виды автоморфизмов.
	Раздел 3.	

	Элементы криптографии	
3.5.	Исторические и современные криптосистемы	Симметрические криптосистемы. Подстановочные шифры. Шифр Цезаря. Перестановочные шифры. Решетка Кардано. Шифр Виженера. Криптосистемы с открытым ключом. Криптосистемы RSA, Эль-Гамала.
	Раздел 4. Основы теории колец	
4.6.	Простейшие свойства колец	Понятия кольца, подкольца, примеры. Мультипликативная группа кольца. Делители нуля. Идеалы колец.
4.7.	Свойства кольца полиномов	Арифметические свойства полиномов. Делимость полиномов. Наибольший общий делитель и наименьшее общее кратное полиномов. Алгоритм Евклида. Соотношение Безу. Неприводимые полиномы. Корни полиномов. Кратные корни. Формальная производная полинома и ее применение.
4.8.	Гомоморфизмы колец	Фактор-кольца и теоремы о гомоморфизмах колец.
	Раздел 5. Основы теории полей	
5.9.	Поля и их свойства	Определение поля, подполя, расширения, примеры. Характеристика поля. Классификация расширений полей. Трасцедентные, алгебраические и конечные расширения. Степень расширения.
5.10.	Конечные поля	Характеристика и количество элементов конечного поля. Существование и единственность конечного поля. Цикличность мультипликативной группы. Свойства примитивных элементов конечных полей. Формирование конечных полей.
5.11.	Группа Галуа	Группа Галуа. Норма и след. Вычисления в конечных полях. Квадратные уравнения в полях Галуа. Автоморфизмы полей.

2. Информационно-методическая часть

2.1. Литература

2.1.1. Основная

1. Бейкер, А. Введение в теорию чисел / А. Бейкер; пер. с англ. – Мн.: Высшая школа, 1995.
2. Борович, З. И. Теория чисел / З. И. Борович, И. Р. Шафаревич. – 3-е изд., доп. – М.: Наука, 1985.
3. Виноградов, И. М. Основы теории чисел. Учебник для университетов по спец. «Математика» / И. М. Виноградов. – 9-е изд., перераб. – М.: Наука, 1981.
4. Каргополов, М. И. Основы теории групп / М. И. Каргополов, Ю. И. Мерзляков. – 2-е изд., перераб. – М.: Наука, 1977.
5. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа [Текст]: учеб.-метод. пособие по курсу «Высшая математика» для студ. спец. «Сети телекоммуникаций» и «Информатика» всех форм обуч. / В. А. Липницкий. – 2-е изд., испр. – Мн: БГУИР, 2006.
6. Мао, В. Современная криптография: теория и практика / В. Мао; пер. с англ. – М.: Вильямс, 2005.
7. Нестеренко, Ю. В. Введение в теорию чисел: учебное пособие для вузов по спец. «Математика» / Ю. В. Нестеренко, А. Б. Шидловский, А. И. Галочкин, под ред. А. Б. Шидловского. – М.: МГУ, 1984.
8. Нидеррайтер, Г. Конечные поля. В 2-х т. Т. 1 / Г. Нидеррайтер, Р. Лидл; пер. с англ. А. Е. Жукова, В. И. Петрова, под ред. В. И. Нечаева. – М.: Мир, 1988.
9. Основы криптографии: учебное пособие для студентов вузов [доп. МО РФ] / А. П. Алферов [и др.]. – 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002.
10. Прикладная математика: метод. пособие для студ. спец. 1-45 01 05 «Сети телекоммуникаций», 1-45 01 03 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях» днев. Формы обуч. / В. А. Липницкий [и др.]. – Минск: БГУИР, 2010.

2.1.2. Дополнительная

11. Беньаш-Кривец, В. В. Лекции по алгебре: группы, кольца, поля: пособие для студентов фак. прикл. математики и информатики и мех.-мат. фак. / В. В. Беньаш-Кривец, О. В. Мельников. – Минск: БГУ, 2009.
12. Введение в криптографию: новые математические дисциплины: учебник / под ред. В. В. Яценко. – СПб.: Питер, 2001.
13. Вейль, А. Основы теории чисел / А. Вейль; пер. с англ. А. Н. Вассерштейна, А. Н. Паршина; под ред. И. И. Пятецкого-Шапиро. – М.: Мир, 1972.

14. Куликов, Л. Я. Алгебра и теория чисел / Л. Я. Куликов. – М.: Высш. шк., 1979.
15. Куликов, Л. Я. Сборник задач по алгебре и теории чисел / Л. Я. Куликов, А. И. Москаленко, А. А. Фомин. – М.: Просвещение, 1993.
16. Лельчук, М. П. Практические занятия по алгебре и теории чисел / М. П. Лельчук, И. И. Полевченко, А. М. Радьков, Б. Д. Чеботаревский. – Минск: Вышэйш. шк., 1986.
17. Монахов, В. С. Введение в теорию конечных групп и их классов / В. С. Монахов. – Минск: Вышэйш. шк., 2006.
18. Радьков, А. М. Алгебра и теория чисел / А. М. Радьков, Б. Д. Чеботаревский. – Минск: Вышэйш. шк., 1992.
19. Стрейникова, Е. Д. Основы прикладной алгебры [+ электр. вариант]: учебно-методическое пособие для студентов вузов [рек. УМО РБ] / Е. Д. Стрейникова. – Мн.: БГУИР, 2010.
20. Ширяев, В. М. Прикладная алгебра. Теория чисел: сб. задач для студентов фак. прикл. математики и информатики / В. М. Ширяев – Минск: БГУ, 2009.
21. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел / Л. Б. Шнеперман. – Минск: Вышэйш. шк., 1982.
22. Интернет-ресурсы: иллюстрированный самоучитель по «MatLab», «Mathematica»: <http://samoucka.ru>.

2.2. Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения, оборудования для выполнения лабораторных работ

1. Пакет «Mathematica».
2. Пакет «MatLab».
3. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа [Текст]: учеб.-метод. пособие по курсу «Высшая математика» для студ. спец. «Сети телекоммуникаций» и «Информатика» всех форм обуч. / В. А. Липницкий. – 2-е изд., испр. – Мн: БГУИР, 2006.
4. Прикладная математика: метод. пособие для студ. спец. 1-45 01 05 «Сети телекоммуникаций», 1-45 01 03 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях» днев. Формы обуч. / В. А. Липницкий [и др.]. – Минск: БГУИР, 2010.

2.3. Перечень тем лабораторных занятий, их название

Основная цель проведения лабораторных занятия состоит в закреплении теоретического материала курса, приобретении навыков выполнения эксперимента, обработки экспериментальных данных, анализа результатов, грамотного оформления отчетов.

№ темы по п. 1	Наименование лабораторной работы	Содержание	Обеспеченность по пункту 2.2
1	2	3	4
1.1.	Теория делимости в кольце целых чисел	Теорема о делении с остатком. Систематическая запись натуральных чисел. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Взаимно простые числа. Простые числа. Основная теорема арифметики. Факторизация целого числа в произведение простых множителей.	1- 4
1.2.	Теория сравнений	Составление таблиц сложения и умножения в кольце классов вычетов по заданному модулю. Обратимость классов вычетов. Линейные сравнения и системы сравнений. Функция Эйлера и ее основные свойства. Теоремы Эйлера и Ферма.	1- 4
2.3.	Группы	Понятие группы. Порядок элемента в группе. Циклические группы. Группы подстановок.	1- 4
2.3.	Подгруппы	Понятие подгруппы. Смежные классы. Составление таблиц смежных классов группы по данной подгруппе. Теорема Лагранжа. Нормальные подгруппы и фактор-группы.	1- 4
3.5.	Исторические и современные криптоси-	Освоение древних методов шифрования. Шифр Цезаря.	1- 4

	стемы	Решетка Кардано. Шифр Виженера. Криптосистемы RSA, Эль-Гамала. Обработка криптосистемы RSA с применением китайской теоремы об остатках.	
4.6., 4.7.	Простейшие свойства колец. Свойства кольца полиномов	Понятия кольца. Мультипликативная группа кольца. Идеалы колец. Арифметические свойства полиномов. Делимость полиномов. Неприводимые полиномы. Корни полиномов.	1- 4
5.9., 5.10.	Формирование конечных полей	Определение поля, подполя, расширения, примеры. Характеристика поля. Классификация расширений полей. Степень расширения. Характеристика и количество элементов конечного поля. Цикличность мультипликативной группы. Свойства примитивных элементов конечных полей. Формирование конечных полей.	1- 4
5.11.	Вычисления в полях Галуа	Формирование поля Галуа заданного порядка, нахождение примитивных элементов в нем. Решение систем линейных уравнений над данным конечным полем. Норма и след. Квадратные уравнения в полях Галуа. Вычисления в конечных полях.	1- 4

3. 1. Учебно-методическая карта учебной дисциплины в дневной форме обучения

Номер раздела, темы по п. 1	Название раздела, темы	Количество аудиторных часов		Самостоятельная работа, часы	Форма контроля знаний студентов
		ЛК	Лаб. зан.		
1	2	3	4	5	6
	Раздел 1. Основы теории чисел	6	4	7	
1.1.	Теория делимости в кольце целых чисел	3	2	3	Защита ЛР «Теория делимости в кольце целых чисел»
1.2.	Теория сравнений	3	2	4	Защита ЛР «Теория сравнений»
	Раздел 2. Основы теории групп	6	4	9	
2.3.	Группы и их подгруппы	4	4	6	Защита ЛР «Группы», Защита ЛР «Подгруппы»
2.4.	Гомоморфизмы и автоморфизмы групп	2	-	3	устный опрос
	Раздел 3. Элементы криптографии	4	2	8	
3.5.	Исторические и современ- ные криптосистемы	4	2	8	Защита ЛР «Исторические и современные криптосистемы»
	Раздел 4. Основы теории колец	8	2	9	
4.6.	Простейшие свойства колец	3	1	3	Защита ЛР «Простейшие свойства колец. Свойства кольца полиномов»
4.7.	Свойства кольца полиномов	3	1	4	

4.8.	Гомоморфизмы колец	2	-	2	устный опрос
	Раздел 5. Основы теории полей	8	4	9	
5.9.	Поля и их свойства	2	1	2	Защита ЛР «Формирование конечных полей»
5.10.	Конечные поля	4	1	4	
5.11.	Группа Галуа	2	2	3	Защита ЛР «Вычисления в полях Галуа»
	Текущая аттестация				зачет
	Итого	32	16	42	

**ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ
УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ**

Перечень учебных дисциплин	Кафедра обеспечивающая учебную дисциплину по п.1	Предложения об изменениях в содержании по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)	Подпись заведующего кафедрой обеспечивающей учебную дисциплину по п.1
1	2	3	4	5
«Прикладная теория кодирования»	кафедра сетей и устройств телекоммуникаций		Рекомендовать к утверждению, Протокол № 14 от 09.06.2014г.	
«Цифровая обработка и защита мультимедийной информации»	кафедра сетей и устройств телекоммуникаций			

Заведующий кафедрой _____

В. В. Цегельник