Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УТВЕРЖДАЮ
Проректор по учебной работе
и менеджменту качества
Е. Н. Живицкая

06.01.2015г.
Регистрационный № УД-4-150/р.

«Математические основы кодирования»

Учебная программа учреждения высшего образования по учебной дисциплине
для специальностей
1-39 01 02 Радиоэлектронные системы
1-39 01 04 Радиоэлектронная защита информации

Кафедра радиотехнических систем

Всего часов по дисциплине 60

Зачетных единиц 1,5

2014 г.

Составитель: Д. М. Бильдюк, магистр технических наук, старший преподаватель

Учебная программа учреждения высшего образования составлена на основе учебной программы «Математические основы кодирования», утвержденной ректором БГУИР 22.01.2015 г., регистрационный номер № УД – 39-090/баз. и учебных планов специальностей 1-39 01 02 Радиоэлектронные системы, 1-39 01 04 Радиоэлектронная защита информации.

Рассмотрена и рекомендована к утверждению на заседании кафедры радиотехнических систем

протокол № 9 от 19.05.2014

Заведующий кафедрой И. Ю. Малевич

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

протокол № 1 от 22.09.2014

Председатель А.В. Короткевич

СОГЛАСОВАНО

Эксперт-нормоконтролер

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

План учебной дисциплины в дневной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов				Академ. часов на курс. работу (проект)	Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия ,семинары		
1-39 01 02	Радиоэлектронные системы	2	3	34	16	-	18	-	Зачет
1-39 01 04	Радиоэлектронная защита информации	2	3	34	16	-	18	-	Зачет

Место дисциплины.

Целью изучения учебной дисциплины является овладение необходимыми элементами математического аппарата теории кодирования.

Задачи учебной дисциплины состоят в формировании базовых знаний математического аппарата описания кодовых структур и алгоритмов, используемых в теории кодирования.

В результате изучения учебной дисциплины «Математические основы кодирования» формируются следующие компетенции:

академические:

– умение применять базовые научно-теоретические знания для решения теоретических и практических задач;

– умение работать самостоятельно;

– обладание навыками, связанными с использованием технических устройств, управлением информацией и работой с компьютером;

социально-личностные:

– способность к межличностным коммуникациям;

– умение работать в команде;

профессиональные:

– умение анализировать состояние научно-технической проблемы на основе подбора и изучения литературных и патентных источников;

– способность анализировать и оценивать собранные данные;

– умение готовить доклады, материалы к презентациям;

– умение пользоваться глобальными информационными ресурсами;

– способность составлять обзоры и отчеты по результатам исследований.

В результате изучения учебной дисциплины студент должен:

знать:

– основные понятия теории множеств, решеток и графов;

– основы конечных полей (элементы теории групп, основы теории чисел, колец полиномов, полей и матриц);

– основные свойства расширеных полей, функции следа, преобразования Фурье в поле Галуа;

– наиболее эффективные методы факторизации целых чисел;

– основные свойства эллиптических кривых над конечным полем;

уметь:

– использовать математические модели простейших дискретных структур;

– использовать для анализа дискретных физических моделей различные алгебраические структуры;

владеть:

– средствами компьютерного моделирования дискретных вычислительных алгоритмов;

– методами исследования моделей с учетом их иерархической структуры;

иметь представление:

– о современных тенденциях и направлениях развития в области дискретных вычислительных алгоритмов и отображений.

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

№ п.п.	Название дисциплины	Раздел, темы
1	Основы алгоритмизации и программирования	Все
2	Математика	В объёме 1,2 семестров

1. Содержание учебной дисциплины

№ тем	Наименование разделов, тем	Содержание тем
1	Множества	Множества и операции над ними. Графы. Отображение множеств.
2	Решетки	Ортогонализация Грамма-Шмидта. Алгоритм Ленстры-Ленстры-Ловаша. Задача об укладке ранца.
3	Основные теоретико-числовые алгоритмы	Теория делимости в кольце целых чисел. Алгоритм Евклида. Сравнения. Малая теорема Ферма и теорема Эйлера. Первообразные корни, индексы. Символ Лежандра. Квадратичный закон взаимности Гаусса. Символ Якоби. Решение квадратичных сравнений по простому модулю. Детерминированные и вероятностные методы тестирования на простоту. Методы факторизации целых чисел.
4	Алгебраические структуры.	Группы, кольца, поля. Конечные поля и их свойства. Конечные расширения. Функция следа. Преобразование Фурье в поле Галуа.
5	Эллиптические кривые	Уравнение эллиптической кривой в форме Вейерштрасса. Группа точек эллиптической кривой. Инварианты эллиптической кривой.

2. Информационно-методическая часть

2.1 Литература
2.1.1 Основная

2.1.1.1 Иванов, Б.Н. Дискретная математика. Алгоритмы и программы: учеб. пособие/ Б. Н. Иванов – М.: Лаборатория Базовых Знаний, 2003. – 288 с.
2.1.1.2 Новиков, Ф.А. Дискретная математика для программистов: учебник для вузов – СПб.: Питер, 2007. – 364 с.
2.1.1.3 Просветов, Г.И. Дискретная математика: задачи и решения: учеб. пособие/Г. И. Простветов. – М. : БИНОМ. Лаборатория знаний, 2008 – 222 с.
2.1.1.4 Плотников, А. Д. Дискретная математика: учеб. пособие/А.Д. Плотников. – Минск : Новое знание, 2008. – 320 с.
2.1.1.5 Самсонов, Б. Б. Компьютерная математика (основание информатики)/ Б. Б. Самсонов, Е. М. Плохов, А. И. Филоненков. – Ростов-на-Дону: Феникс, 2002. – 512 с.
2.1.1.6 Ахо, А. Построение и анализ вычислительных алгоритмов/ А. Ахо, Дж. Хопкрофт, Дж. Ульман– М.: Мир, 1979. – 536 с.
2.1.1.7 Рейнгольд, Э. Комбинаторные алгоритмы. Теория и практика/Э. Рейнгольд, Ю. Нивергельт, Н. Део. – М.: Мир, 1980. – 476 с.
2.1.1.8 Фомичев, В.М. Дискретная математика и криптология. Курс лекций /Под ред. Н.Д. Подуфалова.-М.: ДИАЛОГ - МИФИ, 2003.
2.1.1.9 Сизый, С. В. Лекции по теории чисел: учеб. пособие для студентов вузов/ С. В. Сизый. – М. : ФИЗМАТЛИТ, 2007. – 192 с.
2.1.1.10Бейкер, А. Введение в теорию чисел/А. Бейкер. – Мн. : Выш. шк., 1995. – 127 с.
2.1.1.11Гаврилов, Г. П. Задачи и упражнения по дискретной математики : учеб. пособие/ Г. П. Гаврилов, А. А. Сапоженко. – М. : Физматлит, 2004. – 418 с.

2.1.2 Дополнительная

2.1.2.1 Лидл, Р. Конечные поля: В 2 т/ Р. Лидл, Г. Нидеррайтер.- М.: Мир,1988.
2.1.2.2 Андерсон, Дж. А. Дискретная математика и комбинаторика/ Дж. А. Андерсон. – М. : Вильямс, 2004. – 960 с.
2.1.2.3 Белоусов А.И., Ткачев С.Б. Дискретная математика: Учеб. для вузов. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2001. – 704 с.
2.1.2.4 Хаггарти Р. Дискретная математика для программистов. – М.: Техносфера, 2003. – 320 с.
2.1.2.5 Шнеперман, Л. Б. Курс алгебры и теории чисел в задачах и упражнениях: учеб пособие. Ч. 1, 2/ Л. Б. Шнеперман. – Мн. : Выш. шк., 1986. – 272 с.
2.1.2.6 Препарата, Ф. Вычислительная геометрия: Введение: Пер с англ./Ф. Препарата, М. Шеймос. – М. : Мио, 1989. – 478 с.
2.1.2.7 Сачков, В. Н. Введение в комбинаторные методы дискретной математики : учеб. пособие/ В. Н. Сачков. – М. : Наука, 1982. – 384 с.

2.2 Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения

2.2.1 Наглядные пособия и методические указания

2.2.1.1 Эффективное кодирование информации: Метод. указ к лабораторной работе по курсу «Прикладная теория кодирования», для студентов радиотехнических специальностей/ Сост. В. К. Конопелько, А. М. Крот.- Мн.: БГУИР, 1995.
2.2.1.2 Митюхин, А. И. Элементы абстрактной алгебры: Учеб. пособие/ А. И. Митюхин. – Мн.: БГУИР, 2000.

2.2.2 Перечень компьютерных программ и технических средств обучения

2.2.2.1 Класс ПЭВМ с операционной системой WINDOWS.
2.2.2.2 Программный пакет Maple.

2.3. Перечень тем практических занятий, их название

№ темы по п.1	Название практического занятия	Содержание	Обеспеченность по пункту 2.2
1	Множества	Множества и операции над ними. Графы. Отображение множеств.	2.2.1 2.2.2
2	Решетки	Ортогонализация Грамма-Шмидта. Алгоритм Ленстры-Ленстры-Ловаша. Задача об укладке ранца.	2.2.1 2.2.2
3	Основные теоретико-числовые алгоритмы	Теория делимости в кольце целых чисел. Алгоритм Евклида. Сравнения. Малая теорема Ферма и теорема Эйлера. Первообразные корни, индексы. Символ Лежандра. Квадратичный закон взаимности Гаусса. Символ Якоби. Решение квадратичных сравнений по простому модулю. Детерминированные и вероятностные методы тестирования на простоту. Методы факторизации целых чисел.	2.2.1 2.2.2
4	Алгебраические структуры.	Группы, кольца, поля. Конечные поля и их свойства. Конечные расширения. Функция следа. Преобразование Фурье в поле Галуа.	2.2.1 2.2.2
5	Эллиптические кривые	Уравнение эллиптической кривой в форме Вейерштрасса. Группа точек эллиптической кривой. Инварианты эллиптической кривой.	2.2.1 2.2.2

.

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	ПЗ	Лаб. зан.		
1	Множества	2	2	-	2	Контрольная работа
2	Решетки	2	2	-	4	Контрольная работа
3	Основные теоретико-числовые алгоритмы	6	6	-	8	Контрольная работа
4	Алгебраические структуры..	4	6	-	8	Контрольная работа
5	Эллиптические кривые	2	2	-	4	Контрольная работа
	Текущая аттестация					Зачет
	Итого	16	18	-	26	

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
Методы и средства цифровой обработки сигналов	РТС	_	Рекомендовать к утверждению Протокол №9 от 19.05.2014	
Основы теории кодирования и криптологии	РТС	_	Рекомендовать к утверждению Протокол №9 от 19.05.2014	
Алгоритмы сжатия данных	РТС	_	Рекомендовать к утверждению Протокол №9 от 19.05.2014	

Заведующий кафедрой И. Ю. Малевич