

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ

Проректор по учебной работе БГУ

А.Л.Толстик
(И.О.Фамилия)

Регистрационный № УД- 5022/уч.

Современные алгоритмы в теории информации

Учебная программа учреждения высшего образования
по учебной дисциплине для специальностей:

1-31 81 08 Компьютерная математика и системный анализ

2017 г.

Учебная программа составлена на основе образовательного стандарта ОСВО 1-31 81 08-2013 и учебных планов УВО: № G31-250/уч., № G31з-266/уч., 26.05.2017.

СОСТАВИТЕЛИ:

В.А. Липницкий, профессор кафедры дифференциальных уравнений и системного анализа Белорусского государственного университета, доктор технических наук, кандидат физико-математических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой дифференциальных уравнений и системного анализа Белорусского государственного университета
(протокол № 8 от 13.04.2017);

Учебно-методической комиссией механико-математического факультета
Белорусского государственного университета
(протокол № 7 от 16.05.2017).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Целью дисциплины «Современные алгоритмы в теории информации» является подготовка специалистов, способных использовать фундаментальные математические знания в качестве основы при решении прикладных задач, связанных с теорией информации и ее приложениями.

Преподавание дисциплины *решает следующие задачи:*

- формирование у магистрантов способностей самостоятельно разрабатывать алгоритмы решения задач и их анализировать;
- развивать и использовать инструментальные средства, информационные среды, автоматизированные системы;
- использовать математические и компьютерные методы и алгоритмы исследований при анализе современных естественнонаучных, экономических, социально-политических процессов;
- приобретение способностей самостоятельно расширять математические знания и компьютерные навыки с дальнейшим их использованием при анализе математических моделей широкого круга прикладных задач.

В результате изучения учебной дисциплины студент магистратуры должен:

знать:

- китайскую теорему об остатках и ее применение;
- свойства конечных полей;
- основы теории норм синдромов;
- основы классификации двоичных векторов и матриц.

уметь:

- корректно применять изученные в курсе алгоритмы;
- формировать полк Галуа заданного порядка и проводить вычисления в них;

владеть:

- методами вычислений в кольцах классов вычетов и в конечных полях;
- методами решения алгебраических уравнений над кольцами классов вычетов и над полями Галуа;
- алгоритмами групповой классификации векторов и матриц.

В результате изучения дисциплины «Современные алгоритмы в теории информации» студент должен обладать следующими компетенциями:

АК-1. Осуществлять самостоятельную научно-исследовательскую деятельность (включая анализ, сопоставление, систематизацию, абстрагирование, моделирование, проверку достоверности данных, принятие решений и др.).

СЛК-4. Пользоваться одним из государственных языков Республики Беларусь и иным иностранным языком как средством делового общения.

СЛК-7. Адаптироваться к новым ситуациям социально-профессиональной деятельности, реализовывать накопленный опыт, свои возможности.

ПК-2. Разрабатывать и использовать современное учебно-методическое обеспечение.

ПК-7. Квалифицированно проводить научные исследования в области математики и информационных технологий.

ПК-9. Пользоваться глобальными информационными ресурсами.

ПК-12. Применять современные методологии, формализованные языки и нотации, программные средства для построения и описания моделей процессов, данных, объектов.

ПК-17. Осваивать и реализовывать управленческие инновации в сфере высоких технологий.

Дисциплина «Современные алгоритмы в теории информации» является дисциплиной компонента учреждения высшего образования и преподается в четвертом семестре для дневной формы получения образования и в четвертом семестре для заочной формы. Она является ярким примером использования математики в информационных технологиях. Кроме того, обучение проходит в форме изучения действующих современных вычислительных стандартов, что полезно для системных аналитиков, поэтому изучение дисциплины «Современные алгоритмы в теории информации» связано с дисциплиной «Актуальные задачи прикладного системного анализа».

Форма получения высшего образования очная (дневная) и заочная.

Общее количество часов и количество аудиторных часов, отводимое на изучение учебной дисциплины в соответствии с учебным планом учреждения высшего образования по специальности, составляет соответственно 240 и 68 часа для дневной формы, из которых 34 часов лекций, 34 часов лабораторных занятий. На заочной форме 20 аудиторных часов в четвертом семестре, из которых 10 часов лекций и 10 часов лабораторных.

Формой текущей аттестации по учебной дисциплине является экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Китайская теорема об остатках и работа с большими числами.

Китайская теорема об остатках (CRT) и ее современная формулировка. Применение CRT к вычислениям с большими числами, в современных криптографических системах: RSA и Рабина.

Тема 2. Проблема дискретного логарифма и алгоритмы ее решения.

Крипtosистема Эль-Гамаля. Алгоритмы решения проблемы дискретного логарифма: baby step; baby step giant step; метод Нечаева-Силвера-Полига-Хеллмана с применением CRT.

Тема 3. Поля Галуа и вычисления в них.

Кольца, идеалы и максимальные идеалы, фактор-кольца и поля. Основы теории полей. Конечные поля: существование и единственность, цикличность мультиплекативной группы поля, примитивные элементы. Связь элементов полей с неприводимыми полиномами. Формирование элементов конечных полей: а) как элементов фактор-колец; б) как степеней примитивного элемента; в) как полиномов ограниченной степени. Алгоритмы вычислений в конечных полях.

Тема 4. Алгебраические уравнения над полями Галуа.

Методы и алгоритмы решения квадратных уравнений над полями Галуа. Нормальные базисы и формулы Чена для корней квадратных уравнений. Сведение квадратного уравнения над полем характеристики 2 к системе линейных уравнений. Кубические уравнения. Уравнения высших степеней.

Тема 5. Теоретико-групповой подход к защите информации от помех.

Циклическая и циклотомическая группы Γ и Φ , действующие на векторных пространствах V_n над полями Галуа. Их совместная группа G . Строение Γ -орбит и G -орбит векторов. Линейные коды как подпространства V_n . Синдромы ошибок. Спектры синдромов Γ -орбит и G -орбит ошибок. Нормы синдромов как инварианты Γ -орбит ошибок. Норменный метод коррекции ошибок БЧХ-кодами.

Тема 6. Норменные алгоритмы решения алгебраических уравнений.

Решение квадратных и кубических уравнений с помощью теории норм синдромов над полями Галуа характеристики два.

Тема 7. Классификация двоичных матриц с помощью квадрата симметрической группы.

Двоичные (0;1)-матрицы и их роль в теории графов, теории подстановок, теории и практике помехоустойчивого кодирования, в распознавании образов.

Действие симметрической группы на строках и столбцах двоичных матриц. Орбиты двоичных матриц относительно действия на них квадрата симметрической группы. Свойства орбит. Свойства орбит двоичных матриц большого ранга.

Тема 8. Третья проблема Кэммерона.

Методика решения третьей проблемы Кэммерона. Алгоритмы формирования образующих орбит двоичных матриц.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов						Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное	Количество часов УСР	
1	2	3	4	5	6	7	8	9
1.	Современные алгоритмы в теории информации	34			34			
1.1	Китайская теорема об остатках и работа с большими числами	6			4			Отчет по лабораторной работе с устной защитой, собеседование
1.2	Проблема дискретного логарифма и алгоритмы ее решения	4			4			Отчет по лабораторной работе с устной защитой, собеседование
1.3	Поля Галуа и вычисления в них	4			4			Отчет по лабораторной работе с устной защитой, собеседование
1.4	Алгебраические уравнения над полями Галуа	4			6			Отчет по лабораторной работе с устной защитой, собеседование
1.5	Теоретико-групповой подход к защите информации от помех	4			4			Собеседование

1.6	Норменные алгоритмы решения алгебраических уравнений	4			4			Отчет по лабораторной работе с устной защитой, собеседование
1.7	Классификация двоичных матриц с помощью квадрата симметрической группы	4			4			Собеседование
1.8	Третья проблема Кэммерона	4			4			Собеседование

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ ДЛЯ ЗАОЧНОЙ ФОРМЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Форма контроля знаний	
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	Современные алгоритмы в теории информации	10			10			
1.1	Китайская теорема об остатках и работа с большими числами	2			2			Отчет по лабораторной работе с устной защитой, собеседование
1.2	Проблема дискретного логарифма и алгоритмы ее решения	1			2			Отчет по лабораторной работе с устной защитой, собеседование
1.3	Поля Галуа и вычисления в них	2			2			Отчет по лабораторной работе с устной защитой, собеседование
1.4	Алгебраические уравнения над полями Галуа	2			2			Отчет по лабораторной работе с устной защитой, собеседование
1.5	Теоретико-групповой подход к защите информации от помех	2			2			Отчет по лабораторной работе с устной защитой, собеседование

1.6	Норменные алгоритмы решения алгебраических уравнений	1							Собеседование
-----	---	---	--	--	--	--	--	--	---------------

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Литература

Основная:

1. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001. – 324 с.
2. Крэндалл Р., Померанс Р. Простые числа. Криптографические и вычислительные аспекты. М.: УРСС, 2011. – 664 с.
3. Ленг С. Алгебра. М.: Мир, 1968. – 564 с.
4. Лиддл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988. – 822 с.
5. Липницкий, В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учебно- метод. пособие. – Мин.: БГУИР, 2005. – 88 с. 2-е издание – Мин.: БГУИР, 2006. – 88 с.
6. Липницкий, В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. – Мин.: Издательский центр БГУ, 2007. – 240 с.
7. Липницкий, В.А., Аль-Хайдар Е.К. Норменное декодирование ошибок посредством их модификации. – Доклады БГУИР, 2009, №5(43). – С. 12 – 16.
8. Липницкий, В.А. Теория норм синдромов. – Мин.: БГУИР, 2011. – 96 с.
9. Липницкий, В.А., Михайловская Л.В., Валаханович Е.В. Защита информации: практикум. – Мин.: ВА РБ, 2012. – 86 с.
10. Липницкий, В.А., Цветков В.Ю., Конопелько В.К. Предсказание, паспозвавание и формирование образов многоракусных изображений с подвижных объектов. – Мин.: Издат. центр БГУ, 2014. – 224 с.
11. Логачев О. А., Сальников А.А., Ященко В.В. Булевые функции в теории кодирования и криптологии. – М.: Изд-во МЦНМО, 2004. – 470 с.
12. Лосев В.В. Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки. Мин.: Вышэйшая школа. 1990. – 132 с.
13. Манин Ю.И., Пончишкин А.А. Введение в современную теорию чисел. – М.: Изд-во МЦНМО, 2009. – 552 с.
14. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. Учебное пособие для ВУЗов. М.: Техносфера, 2006. – 320 с.
15. Ноден, П., Китте К. Алгебраическая алгоритмика. М.: Мир, 1999. – 720 с.

16. Сидельников, В.М. Теория кодирования. М.: Физматлит, 2008. – 324 с.
17. Смарт, Н. Криптография/ Н. Смарт. М.: Техносфера, 2005. – 524 с.
18. Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. М.: МЦНМО, 2002. – 104 с.
19. Харин Ю. С. и др. Криптология: учебник. – Минск: БГУ, 2013. – 512 с.
20. Шнайер Б. Прикладная криптография. М.: Триумф, 2002. – 468 с.
21. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. – 326 с. Фергюсон, Нильс Практическая криптография = Practical Cryptography / Нильс Фергюсон, Брюс Шнайер ; [пер. с англ. Н. Н. Селиной ; под ред. А. В. Журавлева]. - Москва; Санкт-Петербург; Киев: Диалектика, 2005. - 422с.

Дополнительная:

1. Математические и компьютерные основы криптологии: Учеб. пособие для студ. матем. и инженерно-техн. спец. вузов / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. - Минск: Новое знание, 2003. - 381с.
2. Тилборг, Х.К.А. ван. Основы криптологии / Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с.
3. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации: Учеб. пособие для студ. матем. и инженерно-технических спец. вузов / Ю.С.Харин, С.В.Агиевич. – Минск : БГУ, 2001. - 190с.
4. Мао, Венбо Современная криптография = Modern Cryptography : теория и практика / Венбо Мао ; [пер. с англ. и ред. Д. А. Клюшина]. – Москва; Санкт-Петербург; Киев: Вильямс, 2005. - 764с.
5. Алферов, А.П. Основы криптографии. Учебное пособие, 2-е изд., испр. и доп. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.
6. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.
7. Эндрюс, Г. Теория разбиений / Г. Эндрюс. – М.: Наука, 1982. – 256 с.
8. Холл, М. Комбинаторика / М. Холл. – М.: Мир, 1970. – 424 с.
9. Cameron, P.J. Sequences realized by oligomorphic permutation groups / P.J. Cameron // Integer Sequences, 2000 – Vol. 3 (1). – Article 00.1.5. – [Электронный ресурс] – Режим доступа: <https://cs.uwaterloo.ca/journals/JIS/VOL3/groups.html>. – Дата доступа: 15.12.2013.

10. Cameron, P.J. Product action / P.J. Cameron, D.A. Gewurz, F. Merola // Discrete Math., 2008. – No. 308. – Pp. 386-394.
11. Cameron, P.J. Problems on permutation groups / P.J. Cameron – [Электронный ресурс] – Режим доступа: <https://www.maths.qmul.ac.uk/~pjc/pgprob.html>. – Дата доступа: 15.12.2013.
12. Cameron, P. Asymptotics for incidence matrix classes / P. Cameron, T. Prellberg, D. Stark // The Electronic Journal of Combinatorics, 2006. – Vol. 13.1. – [Электронный ресурс] – Режим доступа: https://www.researchgate.net/publication/2123422_Asymptotic_enumeration_of_incidence_matrices. – Дата доступа: 15.12.2013.

Перечень используемых средств диагностики результатов учебной деятельности

Контроль работы магистранта проходит в форме собеседования, контрольной работы в аудитории или над выполнением лабораторных работ в лаборатории и самостоятельно вне аудитории с предоставлением отчета по лабораторным работам с его устной защитой. Задания к контрольным и лабораторным работам составляются согласно содержанию учебного материала.

Для совершенствования педагогического мастерства и способностей учиться самостоятельно магистрантам могут выдаваться темы докладов, с которыми они выступают на занятиях.

Экзамен по дисциплине проходит в устной или письменной форме.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы УВО по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола) ¹
Актуальные задачи прикладного системного анализа	Кафедра дифференциальных уравнений и системного анализа	нет	Вносить изменения не требуется (протокол № 8 от 13.04.2017)

¹ При наличии предложений об изменениях в содержании учебной программы УВО.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
 _____ (протокол № _____ от _____ 201_ г.)
 (название кафедры)

Заведующий кафедрой

 (ученая степень, ученое звание) _____
 (подпись) _____
 (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

 (ученая степень, ученое звание) _____
 (подпись) _____
 (И.О.Фамилия)