БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.Н. Здрок
«08» января 2020 г.

Регистрационный № УД-7893/уч.

Современные алгоритмы в теории информации

Учебная программа учреждения высшего образования по учебной дисциплине для специальностей:

1-31 80 03 Математика и компьютерные науки

профилизация Компьютерная математика и системный анализ

2020 г.

Учебная программа составлена на основе образовательного стандарта ОСВО 1-31 80 03-2019 и учебных планов: G31з-090/уч., №G31-049/уч. от 11.04.2019.

СОСТАВИТЕЛИ:

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

А.В. Кушнеров, старший преподаватель кафедры дифференциальных уравнений и системного анализа Белорусского государственного университета;

Д.Н. Чергинец, доцент кафедры дифференциальных уравнений и системного анализа Белорусского государственного университета, кандидат физико-математических наук.

.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой дифференциальных уравнений и системного анализа Белорусского государственного университета
(протокол № 5 от 30.12.2019);

Научно-методическим советом Белорусского государственного университета
(протокол № 3 от 03.01.2020).

Зав. кафедрой дифференциальных уравнений
и системного анализа, профессор В. И. Громак

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.

Дисциплина «Современные алгоритмы в теории информации» является дисциплиной компонента учреждения высшего образования и входит в состав модуля «Защита информации». Её преподавание тесно связано с дисциплиной «Практическая криптография».

Освоение учебной дисциплины «Современные алгоритмы в теории информации» должно обеспечить формирование следующей **специализированной компетенции**:

СК-5. Быть способным применять на практике алгоритмы криптографии и помехоустойчивого кодирования.

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.

Структура учебной дисциплины

Дисциплина изучается во 2 семестре. Всего на изучение учебной дисциплины «Современные алгоритмы в теории информации» отведено:

– для очной формы получения высшего образования – 200 часов, в том числе 72 аудиторных часа, из них: лекции – 36 часов, лабораторные занятия – 36 часов;

– для заочной формы получения высшего образования – 16 аудиторных часов, из них лекции – 8 часов, лабораторные занятия – 8 часов.

Трудоемкость учебной дисциплины составляет 6 зачетных единиц.

Форма текущей аттестации по учебной дисциплине – 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.

Криптосистема 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 мультипликативной 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 Ченя 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 Г и Ф, действующие на векторных пространствах V_n над полями Галуа. Их совместная группа G. Строение Г-орбит и G-орбит векторов. Линейные коды как подпространства V_n. Синдромы ошибок. Спектры синдромов Г-орбит и G-орбит ошибок. Нормы синдромов как инварианты Г-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

Дневная форма получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
	Современные алгоритмы в теории информации	**36**			**36**			
1.	Китайская теорема об остатках и работа с большими числами	6			4			Отчет по лабораторной работе с устной защитой, собеседование
2.	Проблема дискретного логарифма и алгоритмы ее решения	4			4			Отчет по лабораторной работе с устной защитой, собеседование
3.	Поля Галуа и вычисления в них	4			4			Отчет по лабораторной работе с устной защитой, собеседование
4.	Алгебраические уравнения над полями Галуа	4			6			Отчет по лабораторной работе с устной защитой, собеседование
5.	Теоретико-групповой подход к защите	4			4			Собеседование

	информации от помех							
6.	Норменные алгоритмы решения алгебраических уравнений	6			6			Отчет по лабораторной работе с устной защитой, собеседование
7.	Классификация двоичных матриц с помощью квадрата симметрической группы	4			4			Собеседование
8.	Третья проблема Кэммерона	4			4			Собеседование

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Заочная форма получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
	Современные алгоритмы в теории информации	**8**			**8**			
1.	Китайская теорема об остатках и работа с большими числами	1			1			Отчет по лабораторной работе с устной защитой, собеседование
2.	Проблема дискретного логарифма и алгоритмы ее решения	1			1			Отчет по лабораторной работе с устной защитой, собеседование
3.	Поля Галуа и вычисления в них	1			1			Отчет по лабораторной работе с устной защитой, собеседование
4.	Алгебраические уравнения над полями Галуа	1			1			Отчет по лабораторной работе с устной защитой, собеседование

5.	Теоретико-групповой подход к защите информации от помех	1			1			Собеседование
6.	Норменные алгоритмы решения алгебраических уравнений	1			1			Отчет по лабораторной работе с устной защитой, собеседование
7.	Классификация двоичных матриц с помощью квадрата симметрической группы	1			1			Собеседование
8.	Третья проблема Кэммерона	1			1			Собеседование

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Березкин, Е.Ф. Основы теории информации и кодирования: учеб. пособие / Е. Ф. Березкин. - Изд. 2-е, испр. - Санкт-Петербург; Москва; Краснодар: Лань, 2018.
2. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001. – 324 с.
3. Крэндалл Р., Померанс Р. Простые числа. Криптографические и вычислительные аспекты. М.: УРСС, 2011. – 664 с.
4. Ленг С. Алгебра. М.: Мир, 1968. – 564 с.
5. Лиддл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988. – 822 с.
6. Липницкий, В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учебно- метод. пособие. – Мн.: БГУИР, 2005. – 88 с. 2-е издание – Мн.: БГУИР, 2006. – 88 с.
7. Липницкий, В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. – Мн.: Издательский центр БГУ, 2007. – 240 с.
8. Липницкий, В.А., Аль-Хайдар Е.К. Норменное декодирование ошибок посредством их модификации. – Доклады БГУИР, 2009, №5(43). – С. 12 – 16.
9. Липницкий, В.А. Теория норм синдромов. – Мн.: БГУИР, 2011. – 96 с.
10. Липницкий, В.А., Михайловская Л.В., Валаханович Е.В. Защита информации: практикум. – Мн.: ВА РБ, 2012. – 86 с.
11. Липницкий, В.А., Цветков В.Ю., Конопелько В.К. Предсказание, паспознавание и формирование образов многоракусных изображений с подвижных объектов. – Мн.: Издат. центр БГУ, 2014. – 224 с.
12. Логачев О. А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М.: Изд-во МЦНМО, 2004. – 470 с.
13. Лосев В.В. Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки. Мн.: Вышэйшая школа. 1990. – 132 с.
14. Манин Ю.И., Пончишкин А.А. Введение в современную теорию чисел. – М.: Изд-во МЦНМО, 2009. – 552 с.
15. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. Учебное пособие для ВУЗов. М.: Техносфера, 2006. – 320 с.
16. Ноден, П., Китте К. Алгебраическая алгоритмика. М.: Мир, 1999. –

720 с.
17. Сидельников, В.М. Теория кодирования. М.: Физматлит, 2008. – 324 с.
18. Смарт, Н. Криптография/ Н. Смарт. М.: Техносфера, 2005. – 524 с.
19. Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. М.: МЦНМО, 2002. – 104 с.
20. Харин Ю. С. и др. Криптология: учебник. – Мн.: БГУ, 2013. – 512 с.
21. Шнайер Б. Прикладная криптография. М.: Триумф, 2002. – 468 с.
22. 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.

Перечень дополнительной литературы

1. Криптографическая защита информации: учеб. пособие / С. О. Крамаров [и др.]; под ред. С.О. Крамарова. - Москва: РИОР: ИНФРА-М, 2018.
2. Меженцев, Г.Г. Кодирование и цифровая обработка сигналов: пособие / Г. Г. Меженцев, В. В. Пискун; Вооруженные Силы Республики Беларусь, Военная академия Республики Беларусь. - Минск : ВА РБ, 2017.
3. 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.
4. Тилборг, Х.К.А. ван. Основы криптологии / Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с.
5. 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. – Мн. : БГУ, 2001. - 190с.
6. 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.
7. 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.
8. 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.

9. Эндрюс, Г. Теория разбиений / Г. Эндрюс. – М.: Наука, 1982. – 256 с.
10. Холл, М. Комбинаторика / М. Холл. – М.: Мир, 1970. – 424 с.
11. 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.
12. Cameron, P.J. Product action / P.J. Cameron, D.A. Gewurz, F. Merola // Discrete Math., 2008. – No. 308. – Pp. 386-394.
13. 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.
14. Cameron, P. Asymptotics for inicidence 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 рекомендуемых средств диагностики и методика формирования итоговой оценки

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

Экзамен по дисциплине проходит в устной или письменной форме.

При формировании итоговой оценки используется рейтинговая оценка знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний и текущей аттестации в рейтинговую оценку:

Формирование оценки за текущую успеваемость:

– ответы на лекциях – 20 %;
– отчеты по лабораторным работам – 80 %;

Рейтинговая оценка по дисциплине рассчитывается на основе оценки текущей успеваемости и экзаменационной оценки с учетом их весовых коэффициентов. Весовой коэффициент текущей успеваемости – 0.4, весовой коэффициент экзаменационной оценки – 0.6.

Описание инновационных подходов и методов к преподаванию учебной дисциплины (эвристический, проектный, практико-ориентированный)

При организации образовательного процесса используется ***эвристический подход,*** который предполагает**:**

– осуществление студентами личностно-значимых открытий окружающего мира;

– демонстрацию многообразия решений большинства профессиональных задач и жизненных проблем;

– творческую самореализацию обучающихся в процессе создания образовательных продуктов;

– индивидуализацию обучения через возможность самостоятельно ставить цели, осуществлять рефлексию собственной образовательной деятельности.

При организации образовательного процесса используется ***практико-ориентированный подход,*** который предполагает***:***

– освоение содержание образования через решения практических

задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

При организации образовательного процесса ***используется метод проектного обучения,*** который предполагает***:***

– способ организации учебной деятельности студентов, развивающий актуальные для учебной и профессиональной деятельности навыки планирования, самоорганизации, сотрудничества и предполагающий создание собственного продукта;

– приобретение навыков для решения исследовательских, творческих, социальных, предпринимательских и коммуникационных задач.

Методические рекомендации по организации самостоятельной работы обучающихся

При изучении учебной дисциплины рекомендуется использовать следующие формы самостоятельной работы:

– выполнение домашнего задания;

– работы, предусматривающие решение задач и выполнение упражнений, выдаваемых на лабораторных занятиях;

– подготовка отчета по лабораторной работе.

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]
Практическая криптография	Кафедра дифференциальных уравнений и системного анализа	нет	Вносить изменения не требуется (протокол № 5 от 30.12.2019)

[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)