

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра алгебры и дискретной математики



УТВЕРЖДАЮ

Декан факультета математики и информационных
технологий

С.А. Герасименко

(подпись, расшифровка подписи)

"30" октября 2015 г.

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.7.1 Теория псевдослучайных генераторов»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

02.03.01 Математика и компьютерные науки

(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики

(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа академического бакалавриата

Квалификация

Бакалавр

Форма обучения

Очная

Оренбург 2015

**Рабочая программа дисциплины «Б.1.В.ДВ.7.1 Теория псевдослучайных генераторов» /сост.
А.Н. Благовисная - Оренбург: ОГУ, 2015**

Рабочая программа предназначена студентам очной формы обучения по направлению подготовки 02.03.01 Математика и компьютерные науки

Содержание

1 Цели и задачи освоения дисциплины	
2 Место дисциплины в структуре образовательной программы	
3 Требования к результатам обучения по дисциплине	
4 Структура и содержание дисциплины	
4.1 Структура дисциплины	
4.2 Содержание разделов дисциплины	
4.3 Практические занятия (семинары)	
5 Учебно-методическое обеспечение дисциплины	
5.1 Основная литература	
5.2 Дополнительная литература	
5.3 Периодические издания	
5.4 Интернет-ресурсы	
5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий	
6 Материально-техническое обеспечение дисциплины	
Лист согласования рабочей программы дисциплины	
Дополнения и изменения в рабочей программе дисциплины	
Приложения:	
Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	
Методические указания для обучающихся по освоению дисциплины	

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

- формирование у студентов теоретических знаний, практических умений и навыков решения задач теории псевдослучайных генераторов.

Задачи:

- изучение основных идей и фундаментальных понятий теории псевдослучайных генераторов;
- изучение математических основ псевдослучайных генераторов;
- овладение способами задания псевдослучайных генераторов;
- приобретение навыков решения задач оценки качества генераторов псевдослучайных последовательностей.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: Б.1.Б.14 Фундаментальная и компьютерная алгебра, Б.1.Б.16 Дискретная математика, математическая логика и их приложения в информатике и компьютерных науках, Б.1.В.ОД.6 Теория конечных графов

Требования к входным результатам обучения, необходимым для освоения дисциплины

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
Знать: - содержание ключевых понятий и определений, используемых в теории и практике решения алгебраических задач; - основные понятия теории множеств, способы задания множеств, операции над множествами, их свойства, представление множеств и результатов операций над ними диаграммами Эйлера-Венна; - основы алгебры бинарных отношений, графическое представление бинарных отношений, свойства бинарных отношений, специальные виды бинарных отношений; отношение эквивалентности и отношение порядка, примеры таких отношений; - описание бинарных отношений и операций над ними матрицами и действиями над ними; - определения основных комбинаторных схем и способы подсчета их количества; - виды функций, оценки числа функций, действующих на конечных множествах; - бином Ньютона, полиномиальную формулу, формулу включений-исключений, примеры их применений; - основные понятия теории графов; - задание графов матрицами; - основные алгоритмы на графах: фронта волны, Форда-Беллмана, Дейкстры, поиска максимального потока в сети, метод ветвей и границ; - булевы функции, способы их задания и представления формулами; - свойства булевых операций; - описание контактных схем булевыми многочленами; - примеры полных систем булевых функций, алгоритм проверки системы булевых функций на полноту; - элементарные функции k-значной логики, примеры полных систем	ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
функций; - алгоритм распознавания полноты, представление функций из P_k полиномами, особенности функций k-значной логики; - основные понятия теории графов; - задание графов матрицами; Уметь: - применять прикладное программное обеспечение для решения задач в профессиональной деятельности, науке и образовании; - использовать методы дискретной математики для решения задач соответствующего содержания; - составлять алгоритм выделения компонент связности; - описывать алгоритм фронта волны; Владеть: - навыками пользования прикладного программного обеспечения для решения задач в профессиональной деятельности, науке и образовании; - методами дискретной математики и математической логики для решения теоретических задач теоретической механики в будущей профессиональной деятельности; - теоретическими и практическими знаниями, касающихся основных понятий теории графов.	
Знать: - принципы построения научного исследования в соответствующей области наук; - алгоритмы на графах (фронта волны, Форда-Беллмана, Дейкстры, Форда-Фалкерсона); - цикломатику графов, метрические свойства деревьев; Уметь: - обосновать актуальность, новизну, теоретическую и практическую значимость собственного исследования, определять методологию исследования, уметь делать выводы из проведенного исследования и определять перспективы дальнейшей работы, анализировать собранный эмпирический материал и делать достоверные выводы, отстаивать собственную научную концепцию в дискуссии, выступать оппонентом и рецензентом по научным работам; - составлять алгоритм Форда-Беллмана; - составлять алгоритм Форда-Фалкерсона; Владеть: - навыками работы с источниками научной литературе, владеть логикой научного исследования, научным стилем изложения собственной концепции; - использовать на практике математические алгоритмы, реализованные на языках программирования.	ОПК-4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем
Знать: - методы теории групп, колец, полей, векторных пространств; - корректные постановки классических задач; - аппарат алгебры высказываний и границы применимости языка исчисления высказываний для анализа логической выводимости; - аппарат логики предикатов, возможности применения формул логики предикатов для записи математических утверждений, для анализа логической выводимости; - критерий эйлеровых графов, признаки гамильтоновых графов; - решение задачи коммивояжера методом ветвей и границ; - проблему пяти, четырех красок; Уметь:	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
- сформулировать и доказать основные результаты изучаемых разделов, применять алгебраические методы; - понимать корректность постановок задач; - формулировать утверждения любой природы (не только математической) на языке логических исчислений; - понять поставленную задачу; - формулировать результат; - строго доказать утверждение; - грамотно пользоваться языком предметной области; - писать алгоритм Форда-Фалкерсона поиска максимального потока в сети; - решать задачу о наименьшем покрытии графа; <u>Владеть:</u> - понятийным аппаратом алгебраической теории и прикладных задач; - навыками самостоятельного построения алгоритма и его анализа; - методами дискретной математики и математической логики для решения и анализа теоретических и прикладных задач; - алгоритмами построения различных задач профессиональной направленности.	
<u>Знать:</u> - новые научные результаты, связанные с алгеброй; - метод резолюций как алгоритм проверки логической выводимости и основу логического программирования; - основные концепции теории алгоритмов; - вычислимость по Тьюрингу, по Черчу, по Маркову; - теореме Холла и ее приложения; - задачу о клике и алгоритмы ее решения; - понятие производной графа по событию и его применение в решении задач; <u>Уметь:</u> - использовать современные методы для исследования и решения научных и практических задач; использовать новые знания и применять их в своей профессиональной деятельности; - ориентироваться в постановках задач; - обрабатывать полученные формулы с помощью равносильных преобразований или переходов к логическим следствиям; - анализировать и синтезировать информацию, полученную из любых источников; - составлять расписания с помощью раскраски графа; - решить задачу о назначениях; - доказать планарность графа; <u>Владеть:</u> - способностью проводить научные исследования и получать новые научные результаты; - умением самостоятельно увидеть следствия сформулированного результата; - знанием корректных постановок классических задач; - пониманием корректности постановок задач; - пониманием того, что фундаментальное знание является основой компьютерных наук; - выделением главных смысловых аспектов в доказательствах; - владением методами математического и алгоритмического моделирования при анализе и решении прикладных и инженерно-технических проблем;	ПК-3 способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
- алгоритмами построения различных задач профессиональной направленности в области информационных технологий.	

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
<u>Знать:</u> - основные понятия теории групп, колец, полей, используемые в теории псевдослучайных генераторов; <u>Уметь:</u> - решать математические задачи теории псевдослучайных генераторов; <u>Владеть:</u> - алгоритмами теории псевдослучайных генераторов, используемыми в задачах кодирования и защиты информации.	ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности
<u>Знать:</u> - формулировки классических задач математики, используемых в теории псевдослучайных генераторов; <u>Уметь:</u> - адаптировать постановки классических задач математики для приложений теории псевдослучайных генераторов; <u>Владеть:</u> - навыками постановки прикладных задач на основе аппарата теории псевдослучайных генераторов.	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики
<u>Знать:</u> - формулировки утверждений теории псевдослучайных генераторов; <u>Уметь:</u> - доказывать утверждения, связанные с прикладными аспектами теории псевдослучайных генераторов; <u>Владеть:</u> - различными методами вывода основных результатов теории псевдослучайных генераторов.	ПК-3 способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	180	180
Контактная работа:	52,25	52,25
Лекции (Л)	18	18
Практические занятия (ПЗ)	34	34
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа:	127,75	127,75
- выполнение индивидуального творческого задания (ИТЗ);	56	56
- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;	34	34
- подготовка к практическим занятиям;	34	34
- подготовка к рубежному контролю и т.п.)	3,75	3,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	зачет	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в предмет	14	4	0		10
2	Классификация генераторов псевдослучайных последовательностей	66	6	16		44
3	Генераторы псевдослучайных последовательностей, функционирующие в конечных полях	44	4	8		32
4	Оценка качества генераторов псевдослучайных последовательностей	56	4	10		42
	Итого:	180	18	34		128
	Всего:	180	18	34		128

4.2 Содержание разделов дисциплины

№ 1 Введение в предмет

Понятие генератора псевдослучайной последовательности. Области применения генераторов псевдослучайных последовательностей. Функции генераторов псевдослучайных последовательностей в системах защиты информации. Принципы построения генераторов псевдослучайных последовательностей. Требования к генераторам псевдослучайных последовательностей в криптографии. Структурная схема генераторов случайных последовательностей.

№ 2 Классификация генераторов псевдослучайных последовательностей

Понятие криптографических и некриптографических генераторов псевдослучайных последовательностей.

Конгруэнтные генераторы. Линейный конгруэнтный генератор. Линейная конгруэнтная последовательность и её потенциал. Усеченный конгруэнтный генератор. Полиномиальный конгруэнтный генератор. Аддитивные и мультипликативные генераторы Фибоначчи. Инверсивный конгруэнтный генератор.

Генераторы на регистрах сдвига с линейными обратными связями. Достоинства и недостатки генераторов на регистрах сдвига с линейными обратными связями. Примеры и сферы приложения генераторов на регистрах сдвига с линейными обратными связями. Математические основы генераторов на регистрах сдвига с линейными обратными связями: понятия образующего многочлена, сопровождающей матрицы, примитивного многочлена, показателя многочлена, M -последовательности. Генераторы M -последовательностей. Другие схемы генераторов: генератор двоичных последовательностей произвольной длины, генератор Джиффи, генератор Д. Голлмана, схема У. Дж. Чамберса.

Генераторы с использованием функций шифрования поточных и блочных шифров. Особенности режимов шифрования в поточных и блочных шифрах. Примеры генераторов стандартов RC4, ГОСТ 28147-89, AES.

Генераторы на основе использования односторонних функций. BBS-генератор. Генератор RSA.

№ 3 Генераторы псевдослучайных последовательностей, функционирующие в конечных полях

Основы теории конечных полей. Определения поля, конечного поля. Свойства полей. Простые поля Галуа. Число элементов конечного поля. Минимальные многочлены. Понятие примитивного многочлена. Неприводимые многочлены. Существование конечного поля. Различные представления элементов поля Галуа. Генератор ненулевых элементов. Сложение, умножение и деление в поле Галуа.

Устройства, функционирующие в простых полях Галуа.

Свойства генераторов M -последовательностей. Структурные особенности последовательностей максимальной длины. Автокорреляционная функция M -последовательности.

№ 4 Оценка качества генераторов псевдослучайных последовательностей

Графические тесты. Гистограмма распределения элементов последовательности. Распределение на плоскости. Проверка серий. Проверка на монотонность. Автокорреляционная функция. Профиль линейной сложности. Графический спектральный тест.

Оценочные тесты. Тесты Д. Кнута. Система оценки Дж. Марсалья. Система оценки NIST.

Другие тесты: посимвольная проверка и проверка частот.

Этапы исследования статистических свойств генератора псевдослучайной последовательностей: генерация последовательностей для тестирования, исполнение набора статистических тестов, анализ прохождения статистических тестов, принятие решения о свойствах генератора.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1, 2	2	Конгруэнтные генераторы.	4
3, 4	2	Генераторы на регистрах сдвига с линейными обратными связями.	4
5, 6	2	Генераторы с использованием функций шифрования поточных и блочных шифров.	4
7, 8	2	Генераторы на основе использования односторонних функций.	4
9, 10	3	Построение конечных полей.	4
11, 12	3	Устройства, функционирующие в простых полях Галуа.	4
13, 14	4	Графические тесты качества генераторов псевдослучайных последовательностей.	4
15, 16, 17	4	Оценочные тесты качества генераторов псевдослучайных	6

№ занятия	№ раздела	Тема	Кол-во часов
		последовательностей.	
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Винберг, Э.Б. Алгебра [Электронный ресурс] / Э.Б. Винберг. – НЦНМО, 2011. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=63299
2. Курош, А. Г. Курс высшей алгебры: учеб. для вузов / А. Г. Курош. – 17-е изд., стер. – СПб.: Лань, 2008. – 432 с.
3. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие [Электронный ресурс] / М.А. Иванов, И.В. Чугунков. – М.: МИФИ, 2012. – 400 с. Режим доступа: <http://biblioclub.ru/index.php?page=book&id=231673>
4. Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс] /Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 511с. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=428998

5.2 Дополнительная литература

1. Основы криптографии [Текст]: учеб. пособие для вузов / А. П. Алферов [и др.]. – М.: Гелиос АРВ, 2005. – 480 с.
2. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. – Москва: Солон-Пресс, 2002. – 256 с.
3. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

5.3 Периодические издания

1. Журнал «Дискретная математика».
2. Журнал «Дискретный анализ и исследование операций».
3. Журнал «Математические вопросы криптографии».
4. Журнал «Обозрение прикладной и промышленной математики».
5. Журнал «Прикладная дискретная математика».
6. Журнал «Фундаментальная и прикладная математика».

5.4 Интернет-ресурсы

1. http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал Math-Net.Ru — это современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России)
2. <http://intuit.ru/> (сайт института дистанционного обучения "ИНТУИТ")
3. <http://cryptography.ru/about/> (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий)

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

Для выполнения ИТЗ используется любая из доступных на момент выполнения заданий сред программирования, имеющихся в распоряжении лаборатории кафедры. Среда и язык программирования выбираются студентами самостоятельно в соответствии с их индивидуальными учебными возможностями и предпочтениями.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных и практических занятий.

Для чтения лекций при необходимости используется переносной мультимедийный комплект: ноутбук, проектор, экран.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.

Методические указания для обучающихся по освоению дисциплины (модуля) могут быть представлены в виде изданных печатным и (или) электронным способом методических разработок со ссылкой на адрес электронного ресурса, а при отсутствии таковых, в виде рекомендаций обучающимся по изучению разделов и тем дисциплины (модуля) с постраничным указанием глав, разделов, параграфов, задач, заданий, тестов и т.п. из рекомендованного списка литературы.

ЛИСТ

согласования рабочей программы

Направление подготовки: 02.03.01 Математика и компьютерные науки
код и наименование

Профиль: Алгоритмы и приложения компьютерной математики

Дисциплина: Б.1.В.ДВ.7.1 Теория псевдослучайных генераторов

Форма обучения: очная

(очная, очно-заочная, заочная)

Год набора 2015

РЕКОМЕНДОВАНА заседанием кафедры

Кафедра алгебры и дискретной математики

наименование кафедры

протокол № 2 от "26" 09 2015г.

Ответственный исполнитель, заведующий кафедрой

Кафедра алгебры и дискретной математики

наименование кафедры

подпись

О.А. Пихтилькова

расшифровка подписи

Исполнители:

старший преподаватель

должность

Д.В.

подпись

Богачева В.С.

расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

02.03.01 Математика и компьютерные науки

код и наименование

личная подпись

расшифровка подписи

Заведующий отделом комплектования научной библиотеки

Истомин

личная подпись

Т.В. Истомин

расшифровка подписи

Уполномоченный по качеству факультета

Кропачев

личная подпись

Кропачев В.С.

расшифровка подписи

Рабочая программа зарегистрирована в ОИОТ ЦИТ

Начальник отдела информационных образовательных технологий ЦИТ

личная подпись

Е.В. Дырдина

расшифровка подписи

Дополнения и изменения в рабочей программе на 2016 год набора

Направление подготовки: 02.03.01 Математика и компьютерные науки (программа академического бакалавриата)

Профиль: Алгоритмы и приложения компьютерной математики (бакалавр)

Дисциплина: Б.1.В.ДВ.7.1 Теория псевдослучайных генераторов

Форма обучения: очная

Внесенные изменения на 2016 год набора

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий _____ С.А. Герасименко
(подпись, расшифровка подписи)
"26" декабря 2016 г.

В рабочую программу вносятся следующие изменения:

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

- ✓ 1. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс] / П. Н. Башлы, А. В. Бабаши, Е. К. Баранова. – РИОР, 2013. – Режим доступа: <http://znanium.com/bookread2.php?book=405000>
- ✓ 2. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности «Информационные системы и технологии» / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – Москва: Академия, 2012. – 332 с.
- ✓ 3. Инструментальный контроль и защита информации [Электронный ресурс] / Н.А. Свиарев, О.В. Ланкин, А.П. Данилкин и др.; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». – Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 192 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=255905>

5.4 Интернет-ресурсы

1. <http://eqworld.ipmnet.ru/indexr.htm> (международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).
2. <http://intuit.ru/> (сайт института дистанционного обучения "ИНТУИТ").
3. <http://cryptography.ru/about/> (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий).
4. http://www.mathnet.ru/index.php?option_lang=rus (общероссийский математический портал, современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России).

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Windows;
2. Офисный пакет Microsoft Office (Word, Excel, Power Point);
3. Среда разработки Visual Studio.

6 Материально-техническое обеспечение дисциплины

Для выполнения заданий предназначен компьютерный класс (ауд. № 1605), подключенный к локальной сети ОГУ и сети Интернет, оснащенный всем необходимым оборудованием.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

Рабочая программа пересмотрена и одобрена на заседании кафедры алгебры и дискретной математики 19.02.16, протокол № 2 С.В. Грицай / С.А. Рихтерманова
(дата, номер протокола заседания кафедры, подпись лиц кафедры)

СОГЛАСОВАНО:

Заведующий отделом комплектования научной библиотеки

С.В. Грицай
личная подпись

Н.Н. Грицай

расшифровка подписи

Уполномоченный по качеству факультета

И.В. Крючкова
личная подпись

И.В. Крючкова

расшифровка подписи

Дополнения и изменения в рабочей программе на 2017 год набора

Направление подготовки: 02.03.01 Математика и компьютерные науки (программа академического бакалавриата)

Профиль: Алгоритмы и приложения компьютерной математики (бакалавр)

Дисциплина: Б.1.В.ДВ.7.1 Теория псевдослучайных генераторов

Форма обучения: очная

Внесенные изменения на 2017 год набора

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий С.А. Герасименко
(подпись, расшифровка подписи)

"28" декабря 2017г.

В рабочую программу вносятся следующие изменения:

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

- ✓ 1. Басалова, Г.В. Основы криптографии: курс лекций [Электронный ресурс] / Г.В. Басалова; Национальный Открытый Университет «ИНТУИТ». – Москва: Интернет-Университет Информационных Технологий, 2011. – 253с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=233689>
- ✓ 2. Биркгоф, Г. Современная прикладная алгебра = Modern Applied Algebra [Текст]: пер. с англ. / Г. Биркгоф, Т. К. Барти. – 2-е изд., стер. – СПб.: Лань, 2005. – 400 с.
- ✓ 3. Кострикин, А.И. Введение в алгебру: учебник [Электронный ресурс] / А.И. Кострикин. – Москва: МЦНМО, 2009. – Ч. 1. Основы алгебры. – 273 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=63140>
- ✓ 4. Кострикин, А.И. Введение в алгебру: учебник / А.И. Кострикин. – Москва: МЦНМО, 2009. – Ч. 3. Основные структуры алгебры. – 272 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=62951>
- ✓ 5. Панкратьев, Е.В. Элементы компьютерной алгебры: учебник [Электронный ресурс] / Е.В. Панкратьев; Национальный Открытый Университет «ИНТУИТ». – Москва: Интернет-Университет Информационных Технологий, 2007. – 247 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=233322>

5.2 Дополнительная литература

- 1. Алферов А.П. Основы криптографии: учеб. пособие для вузов / А. П. Алферов [и др.]. – М.: Гелиос АРВ, 2005. – 480с.
- 2. Лапониная, О.Р. Криптографические основы безопасности [Электронный ресурс] / О.Р. Лапониная. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=429092>
- 3. Пихтильков, С. А. Фундаментальная и компьютерная алгебра [Электронный ресурс]: учебное пособие для студентов, обучающихся по программе высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки / С. А. Пихтильков, О. А. Пихтилькова, Л. Б. Усова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования «Оренбург. гос. ун-т». – Электрон. текстовые дан. (1 файл: 0.58 Мб). – Оренбург: ОГУ, 2016. – 116 с.

4. Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс]/Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016, 511с. Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=428998

5. Алгебраические структуры и их приложения: учебное пособие [Электронный ресурс] / Л.В. Зяблицева, С.Ю. Корабельщикова, И.В. Кузнецова, С.А. Тихомиров; Министерство образования и науки Российской Федерации, Северный (Арктический) федеральный университет имени М.В. Ломоносова. – Архангельск: САФУ, 2015. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=436142>

5.4 Интернет-ресурсы

1. <http://eqworld.ipmnet.ru/indexr.htm> (международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).

2. <http://intuit.ru/> (сайт института дистанционного обучения "ИНТУИТ").

3. <http://cryptography.ru/about/> (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий).

4. http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал, современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России).

5. <https://arxiv.org/> (крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии).

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Windows.

2. Офисный пакет Microsoft Office (Word, Excel, Power Point).

3. Для выполнения ИТЗ используется любая из доступных на момент написания работ сред программирования, имеющихся в распоряжении лаборатории кафедры. Среда и язык программирования выбираются студентами самостоятельно в соответствии с их индивидуальными учебными возможностями и предпочтениями.

6 Материально-техническое обеспечение дисциплины

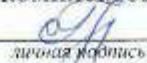
Для выполнения заданий предназначен компьютерный класс (ауд. № 1605), подключенный к локальной сети ОГУ и сети Интернет, оснащенный всем необходимым оборудованием.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

Рабочая программа пересмотрена и одобрена на заседании кафедры алгебры и дискретной математики 21.02.17, протокол № 1 С.А. Тихомирова
(дата, номер протокола заседания кафедры, подпись зав. кафедрой).

СОГЛАСОВАНО:

Заведующий отделом комплексования научной библиотеки


личная подпись

Н.Н. Грицай

расшифровка подписи

Уполномоченный по качеству факультета


личная подпись

И.В. Крючкова

расшифровка подписи