Минобрнауки России

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

Кафедра алгебры и дискретной математики

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

Год набора 2017

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 7 от "21" февраля 2017 г.

Заведующий кафедрой
Кафедра алгебры и дискретной математики _____ О.А. Пихтилькова
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
старший преподаватель _____ А.Н. Благовисная
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.01 Математика и компьютерные науки _____ О.А. Пихтилькова
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
_____ Н.Н. Грицай
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
_____ И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____ ___

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*

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
Знать: - *основные понятия теории групп, колец, полей, используемые в теории псевдослучайных генераторов;* **Уметь:** - *решать математические задачи теории псевдослучайных генераторов;* **Владеть:** - *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
Знать: - *формулировки классических задач математики, используемых в теории псевдослучайных генераторов;* **Уметь:**	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- *адаптировать постановки классических задач математики для приложений теории псевдослучайных генераторов;* **Владеть:** - *навыками постановки прикладных задач на основе аппарата теории псевдослучайных генераторов.*	классических задач математики
Знать: - *формулировки утверждений теории псевдослучайных генераторов;* **Уметь:** - *доказывать утверждения, связанные с прикладными аспектами теории псевдослучайных генераторов;* **Владеть:** - *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: - *самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* - *подготовка к практическим занятиям;* - *подготовка к рубежному контролю)*	**127,75**	**127,75**
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	12	2	0		10
2	Математические основы псевдослучайных последовательностей	60	6	10		44
3	Генераторы псевдослучайных последовательностей	54	6	16		32
4	Оценка качества генераторов псевдослучайных последовательностей	54	4	8		42
	Итого:	180	18	34		128
	Всего:	180	18	34		128

4.2 Содержание разделов дисциплины

№ 1 Введение в предмет

Понятие псевдослучайной последовательности. Области применения генераторов псевдослучайных последовательностей. Виды генераторов псевдослучайных последовательностей. Принципы построения генераторов псевдослучайных последовательностей. Требования к генераторам псевдослучайных последовательностей в системах защиты информации.

№ 2 Математические основы псевдослучайных последовательностей

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. Сложение, умножение и деление в поле Галуа.

Алгебра последовательностей. Определяющие периодические свойства последовательностей. Линейные рекуррентные последовательности. Усложнение последовательностей. Последовательности максимального периода.

№ 3 Генераторы 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, М-последовательности. Генераторы М-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.

№ 4 Оценка качества генераторов псевдослучайных последовательностей

Подходы к анализу псевдослучайных последовательностей.

Линейная сложность последовательностей. Рекуррентная сложность последовательностей.

Графические тесты последовательностей.

Статистические требования к последовательностям. Постулаты Голомба. Статистические тесты. Характеристика тестов Д. Кнута, Дж. Марсалья. Система оценки NIST. Этапы исследования статистических свойств генератора псевдослучайной последовательностей.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1, 2	2	Построение конечных полей.	4
3	2	Алгебра последовательностей.	2
4, 5	2	Линейные рекуррентные последовательности.	4
6, 7	3	Конгруэнтные генераторы.	4

№ занятия	№ раздела	Тема	Кол-во часов
8, 9	3	Генераторы на регистрах сдвига с линейными обратными связями.	4
10	3	Фильтрующие генераторы.	2
11	3	Комбинирующие генераторы.	2
12	3	Генераторы гаммы с неравномерным движением	2
13	3	BBS-генератор.	2
14, 15	4	Графические тесты качества генераторов псевдослучайных последовательностей.	4
16, 17	4	Оценочные тесты качества генераторов псевдослучайных последовательностей.	4
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Фомичев, В.М. Методы дискретной математики в криптологии [Электронный ресурс] / В.М. Фомичев. – Москва: Диалог-МИФИ, 2010. – 436 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=447668

2. Смарт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

5.2 Дополнительная литература

1. Гультяева, Т.А. Основы теории информации и криптографии: конспект лекций [Электронный ресурс] / Т.А. Гультяева; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск: НГТУ, 2010. – 88 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=228963

2. Нечаев, В. И. Элементы криптографии. Основы теории защиты информации [Текст]: учеб. пособие / В. И. Нечаев. – М.: Высш. шк., 1999. – 109 с.

5.3 Периодические издания

1. Прикладная математика и механика: журнал. - М.: Агентство «Роспечать», 2016.

2. Вычислительные технологии: журнал. - М.: Агентство «Роспечать», 2016.

3. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017.

4. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017.

5.4 Интернет-ресурсы

1. 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.

2. 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).

3. https://arxiv.org/ – крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии.

4. https://www.gost.ru/portal/gost/ – портал Федерального агентства по техническому регулированию и метрологии.

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

1. Операционная система Microsoft Windows.
2. OpenOffice/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Бесплатное средство просмотра файлов PDF Adobe Reader.
4. SCOPUS [Электронный ресурс]: реферативная база данных / компания Elsevier. – Режим доступа: https://www.scopus.com/, в локальной сети ОГУ.
5. Springer [Электронный ресурс]: база данных научных книг, журналов, справочных материалов / компания Springer Customer Service Center GmbH . – Режим доступа: https://link.springer.com/, в локальной сети ОГУ.
6. Общероссийский математический портал Math-Net.Ru [Электронный ресурс]: профессиональная база данных для математиков – Режим доступа: http://www.mathnet.ru/index.phtml/?option_lang=rus

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой подключенной к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

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