РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Генераторы псевдослучайных чисел и их применение в криптографии (на англ. яз)

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в магистратуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 01.04.02 «Прикладная математика и информатика». Направленность (профиль) «Дискретные структуры и алгоритмы». Образовательная программа «Информационная безопасность компьютерных систем».

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть магистерской образовательной программы «Информационная безопасность компьютерных систем», изучается в 4-м семестре.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
Способность и умение использовать принципы построения и сравнени надежности базовых криптографических алгоритмов; владение навыка ми, обеспечивающими критическую оценку криптографических алго- ритмов, примитивов, стандартов; представление о современных метод криптографической защиты информации и государственных стандарта на криптографические алгоритмы (СПК-56); способность использовать терминологию в области математического аппарата криптологии, основные утверждения в области алгебры, тео- рии чисел, теории эллиптических кривых, основные базовые алгоритм	З1 (СПК-56,СПК-57) Знать: основные методы синтеза и анализа криптографических генераторов псев- дослучайных чисел У1 (СПК-56,СПК-57) Уметь определять и оценивать критические криптографические характери- стики генераторов псевдослучайных чисел В1 (СПК-56, СПК-57) Владеть навыками применения современного математического аппарата (в частности, неархимедовой динамикой) для синтеза и анализа крипто-

используемые в криптологии; владение навыками решения основных задач в области алгебры, теории чисел, теории эллиптических кривых; знать основные алгебраические и теоретико-числовые понятия и утверждения, используемые в криптологии (СПК-57);	графических генераторов псевдослучайных чисел

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 2 зачетные единицы, всего 72 часа.

28 часов составляет контактная работа с преподавателем – 26 часов занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 2 часа экзамен.

44 часа составляет самостоятельная работа учащегося.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по математическому анализу, линейной алгебре, функциональному анализу, теории вероятностей в объеме, соответствующем основным образовательным программам бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения используются компьютерные презентации лекций, электронные учебные пособия.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе изучаются генераторы псевдослучайных чисел, представляющие собой автономные автоматы, методы синтеза и анализа таких автоматов, а также различные (существенные для криптографии) свойства последовательностей, генерируемых этими автоматами. Отличительной особенностью курса является использование методов неархимедовой эргодической теории: выходные последовательности автоматов рассматриваются как орбиты динамических систем в соответствующих фазовых пространствах, снабженных неархимедовой метрикой и естественной вероятностной мерой (нормированной мерой Хаара); при этом статистические свойства последовательностей определяются эргодическими свойствами систем.

The course focuses on analysis and design of cryptographic pseudorandom number generators; various properties of sequences produced by the generators are studied as well. During the course, the generators are considered as autonomous automata, whereas the automata are treated as dynamical systems in the non-Archimedean metric space. Thus the sequences generated by the automata are considered as orbits in the non-Archimedean metric space endowed with a natural probability measure, the normalized Haar measure. Crucial cryptographic properties of the sequences are then derived from the ergodic properties of corresponding non-Archimedean dynamical systems.

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	**Всего (часы)**	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						**Самостоятельная работа учащегося, часы** из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости: коллоквиумы, практические контрольные занятия и др.	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п..	**Всего**
Тема 1. Генераторы псевдослучайных чисел как динамические системы в неархимедовом пространстве. Понятие генератора псевдослучайных чисел (ГПСЧ). ГПСЧ как автоматы. Криптографическим ГПСЧ и поточные шифраторы. Классиче-	**4**	4	-	-	-	-	**4**	2	-	**2**

ские ГПСЧ. Автоматы с бинарным входом/выходом и Т-функции как криптопримитивы для ГПСЧ.Функции, задаваемые автоматами (детерминированные функции) как функции на бесконечных словах. Пространства всех бесконечных слов над конечным алфавитом как неархимедово метрическое пространство, детерминированные функции как 1-липшицевы функции на нем. Автоматы как неархимедовы динамические системы. Понятие р-адического числа. Элементы р-адического анализа, в частности, анализа Т-функций.										
Тема 2. Неархимедова эргодическая теория и ее применение к синтезу и анализу ГПСЧ. Понятия р-адической эргодической теории. Эргодичность как условие равномерности распреде-	**10**	10	-	-	-	-	**10**	2	-	**2**

ления выходной последовательности ГПСЧ. Основная теорема р-адической эргодической теории для детерминированных функций. Условия и критерии эргодичности для детерминированных функций. Специальные классы функций и основанные на них ГПСЧ Неархимедова эргодическая теория для функций нескольких переменных и основанных на них ГПСЧ. Латинские квадраты и их применение в совершенных шифрах. Построение латинских квадратов на основе неархимедовой эргодической теории.										
Тема 3. Свойства выходных последовательностей ГПСЧ, построенных на основе Т-функций. Периоды координатных последовательностей, линейный ранг, 2-адический ранг, распределение k-грамм. Свойства полупе-	**6**	6	-	-	-	-	**6**	2	-	**2**

риодов координатных последовательностей. Линейные зависимости между координатными последовательностями. Распределение в единичном квадрате, закон 0-1 для автоматов. Т-функции меры 1. .										
Тема 4. ГПСЧ с динамически изменяющимся законом рекурсии. Сплетения автоматов как неавтономные динамические системы на неархимедовом пространстве. Построение ГПСЧ и поточных шифраторов с динамически изменяющимся законом на основе сплетений. Свойства выходных последовательностей таких ГПСЧ.	**6**	6	-	-	-	-	**6**	2	-	**2**
Промежуточная аттестация – экзамен: индивидуальное практическое контрольное задание + индивидуальное	**2**	-	-	-	-	2	**2**	36	-	**36**

собеседование										
Итого	**28**						**28**			**44**

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовке к практическим заданиям и итоговой аттестации.

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная учебно-методическая литература

1) V.Anashin, A. Khrennikov. Applied algebraic dynamics. — Berlin: Walter de Gruyter, 2009. — 557 c.

2) V.Anashin. Non-Archimedean analysis, T-functions and cryptography — M.: Макс Пресс Москва, 2006. — 56 c

3) V.Anashin. The p-adic ergodic theory and applications. — 216 c. Available from http://istina.msu.ru/media/courses/course/979/622/8722971/CHINABOOK-FIN.PDF)

Дополнительная учебно-методическая литература

1) V.Anashin. Psedorandom number generators: applications to cryptography. Lecture course presentation, available from http://istina.msu.ru/media/courses/course/d87/fb0/34028165/Lectures-2017.PDF

2) V. Anashin. Lecture notes of Int'l Summer School. — 53 c. Available from http://istina.msu.ru/media/courses/course/979/622/8722971/LECTURE_NOTES_V_2.PDF

3) V.Anashin. Stream ciphers. Lecture course presentations. Available from http://istina.msu.ru/courses/8722971/

4) Коблиц Н. *p-адические числа, p-адический анализ и дзета-функции*. - М., Мир, 1982.

5) Хренников А.Ю. *Неархимедов анализ и его приложения*. Физматлит, Москва, 2003

6) Каток С.Б. *p-адический анализ в сравнении с вещественным*. МЦНМО, Москва, 2004

7) Кнут Д. *Искусство программирования для ЭВМ*. т. 2. Получисленные алгоритмы. Вильямс, Москва–СПб–Киев, 2000

Ресурсы информационно-телекоммуникационной сети «Интернет»

1) https://www.researchgate.net/profile/Vladimir_Anashin/contributions

Информационные технологии, используемые в процессе обучения

В процессе обучения используются компьютерные презентации, а также пакет прикладных программ Vorg для визуализации выходных последовательностей генераторов псевдослучайных чисел.

Материально-техническая база

Для преподавания дисциплины требуется компьютерный класс, оборудованный маркерной доской, проектором и экраном.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Английский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

д.ф.- м.н., профессор Анашин Владимир Сергеевич (anashin@iisi.msu.ru)

Приложение

Оценочные средства для промежуточной аттестации по дисциплине «Генераторы псевдослучайных чисел и их применение в криптографии»

Промежуточная аттестация состоит из выполнения практического контрольного задания, проверяющего приобретенные учащимся умения и навыки, и индивидуального собеседования, проверяющего приобретенные знания.

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ	**КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ из соответствующих карт компетенций**					**ОЦЕНОЧНЫЕ СРЕДСТВА**
	1	2	3	4	5	
	Неудовлетворительно	**Неудовлетворительно**	**Удовлетворительно**	**Хорошо**	**Отлично**	
З1 (СПК-56,СПК-57) Знать: основные методы синтеза и анализа криптографических генераторов псевдослучайных чисел	Отсутствие знаний	Фрагментарные представления об основных методах синтеза и анализа криптографических генераторов псевдослучайных чисел	В целом сформированные, но неполные знания обосновных методах синтеза и анализа криптографических генераторов псевдослучайных чисел	Сформированные, но содержащие отдельные пробелы знания об основных методах синтеза и анализа криптографических генераторов псевдослучайных чисел	Сформированные систематические знания об основных методах синтеза и анализа криптографических генераторов псевдослучайных чисел	индивидуальное собеседование
У1 (СПК-56,СПК-57) Уметь определять и оценивать	Отсутствие умений	Фрагментарные умения в области решения базовых задач по определению и оценке критических крипто-	В целом сформированное, но не систематическое умение решать базовые задачи по определению и	Сформированное, но содержащее отдельные пробелы умение решать базовые задачи по определе-	Сформированное систематическое умение решать базовые задачи по определению и оценке	практическое контрольное задание, индивидуальное собеседование

критические криптографические характеристики генераторов псевдослучайных чисел		графических характеристик генераторов псевдослучайных чисел	оценке критических криптографических характеристик генераторов псевдослучайных чисел	нию и оценке критических криптографических характеристик генераторов псевдослучайных чисел	критических криптографических характеристик генераторов псевдослучайных чисел	
В1 (СПК-56, СПК-57) Владеть навыками применения современного математического аппарата (в частности, неархимедовой динамикой) для синтеза и анализа криптографических генераторов псевдослучайных чисел	Отсутствие навыков	Фрагментарное владение навыками применения современного математического аппарата (в частности, неархимедовой динамикой) для синтеза и анализа криптографических генераторов псевдослучайных чисел	В целом сформированное, но не систематическое владение навыками применения современного математического аппарата (в частности, неархимедовой динамикой) для синтеза и анализа криптографических генераторов псевдослучайных чисел	Сформированное, но содержащее отдельные пробелы владение навыками применения современного математического аппарата (в частности, неархимедовой динамикой) для синтеза и анализа криптографических генераторов псевдослучайных чисел	Сформированное систематическое владение навыками применения современного математического аппарата (в частности, неархимедовой динамикой) для синтеза и анализа криптографических генераторов псевдослучайных чисел	практическое контрольное задание, индивидуальное собеседование

Фонды оценочных средств

Примерные практические самостоятельные работы для текущего контроля успеваемости.

ПСР ТК1. 2-адический анализ и Т-функции

Примерные варианты заданий:

1. Вывести тождества, связывающие продолжения на все пространство целых 2 адических чисел функций, представляющих основные арифметические и поразрядные логические команды процессора (+, NOT,AND,OR,XOR).
2. Доказать равномерную непрерывность вышеуказанных функций.
3. Найти частные производные (и производные по модулю 2^n) вышеуказанных функций во всех тех случаях, когда эти производные существуют.

ПСР ТК2. Генераторы псевдослучайных чисел на основе Т-функций

Примерные варианты заданий:

1. Найти длину периода инверсивного генератора с законом рекурсии $f(x) = 1 + x + \frac{p^2}{1 + px}$.
2. Показать, что функция inv (взятие обобщенного обратного) детерминирована, дифференцируема везде кроме 0: и найти общий вид ее производной i-го порядка в точке, отличной от 0.
3. Доказать, что функция $\frac{(x^p - x)^2}{p}$ является A-функцией, но не является B-функцией.

Список вопросов для индивидуального собеседования на промежуточной аттестации.

Билет 1
1. Архимедова и неархимедова метрика. Предел в неархимедовом пространстве (в частности, в пространстве целых p-адических чисел Z_p).
2. Транзитивно ли отображение f(x) по модулю 256?
f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 1))

Билет 2
1. Детерминированные функции как непрерывные неархимедовы функции. ГПСЧ как автоматы.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge}2$ + 2))

Билет 3
1. Каноническая форма представления p-адического числа. Представление рациональных чисел в p-адической форме.
2. Сохраняет ли T-функция F(x, y, z) = (x + xy(xy XOR x XOR y XOR 1), x + y, xy + z) меру?

Билет 4
1. Команды процессора как функции в пространстве целых p-адических чисел. Тождества.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge}2$ + 3))

Билет 5
1. Теорема Островского.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge}2$ + 31))

Билет 6
1. Арифметика p-адических чисел.
2. Сбалансирована ли T-функция F(x, y, z) = (x + (y_2 XOR y)(z_2 XOR z), 1 + x + y, y + xy + z) по модулю $2^{\wedge}512$?

Билет 7
1. Топология неархимедова пространства (в частности, пространства целых p-адических чисел Z_p).
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge}2$ + 30))

Билет 8
1. Лемма Гензеля (классическая и общая).

2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge}2$ + 29))

Билет 9

1. Непрерывность и равномерная непрерывность в неархимедовом пространстве (в частности, в пространстве целых p-адических чисел Z_p).
2. Сохраняет ли T-функция F(x, y, z) = (x + yz(yz XOR y XOR z XOR 1), 1 + x + y, x + xy + z) меру?

Билет 10

1. T-функции. Продолжение стандартной команды процессора до непрерывной функции целого 2-адического аргумента.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge}2$ + 28))

Билет 11

1. Детерминированные функции как функции, удовлетворяющие p-адическому условию условию Липшица с константой 1. Детерминированные команды процессора.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge}2$ + 27))

Билет 12

1. Дифференцируемые функции в пространстве целых p-адических чисел. Дифференцируемость по модулю p^k. Производная, дифференциал и якобиан по модулю p^k.
2. Сбалансирована ли T-функция F(x, y, z) = (x + xz(xz XOR x XOR z XOR 1), x + y, 1 + x + y + xy + z) по модулю $2^{\wedge}1024$?

Билет 13

1. p-адические ряды и критерий их сходимости.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge}2$ + 26))

Билет 14

1. Интерполяционные ряды Малера. Критерий детерминиро-

ванности функции на языке рядов Малера.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 25))

Билет 15
1. Интерполяционные ряды ван дер Пута. Критерий детерминированности функции на языке рядов ван дер Пута.
2. Сохраняет ли T-функция F(x, y, z) = (x+(x2XORx)(y2XORy)(z^2XOR z), x + y, x + z) меру?

Билет 16
1. Мера Хаара и естественная вероятностная мера на пространстве целых p-адических чисел. Основная эргодическая теорема для детерминированных функций.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 24))

Билет 17
1. Критерии и достаточные условия сохранения меры детерминированной функцией, равномерно дифференцируемой по модулю p. Построение латинских квадратов и пар ортогональных латинских квадратов.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 23))

Билет 18 1. Критерий сохранения меры T-функцией в терминах координатных функций.
2. Сбалансирована ли T-функция F(x, y, z) = (x + xy(x XOR 1)(y XOR 1), x + y, 1 + xy + z) по модулю 2^2048?

Билет 19
1. Критерий сохранения меры T-функцией в терминах рядов Малера.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 22))

Билет 20

1. Критерий сохранения меры Т-функцией в терминах рядов ван дер Пута.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 21))

Билет 21
1. Критерий эргодичности Т-функции в терминах координатных функций.
2. Сохраняет ли Т-функция F(x, y, z) = (x+xyz(xXOR1)(yXOR1)(zXOR 1), 1 + x + y, 1 + xy + x + y + z) меру?

Билет 22
1. Критерий эргодичности Т-функции в терминах рядов Малера.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 20))

Билет 23
1. Критерий эргодичности Т-функции в терминах рядов ван дер Пута.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 19))

Билет 24
1. Критерий эргодичности детерминированных функций, равномерно дифференцируемых по модулю p_2.
2. Сбалансирована ли Т-функция F(x, y, z) = (1+x+x(xXOR1)(z^2XOR z), 1 + y, 1 + xy + z) по модулю 2^{4096}?

Билет 25
1. Критерий сохранения меры Т-функцией из класса B.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4(x^2 + 18))

Билет 26
1. Критерий эргодичности Т-функций из класса B.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR

1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge 2}$ + 13))

Билет 27
1. Свойства координатных последовательностей эргодических Т-функций (периоды, строение).
2. Сохраняет ли Т-функция F(x, y, z) = (1 + x + xy(x XOR 1)(y XOR 1)(z_2 XOR z), x + y, y + z) меру?

Билет 28
1. Классические ГПСЧ на основе эргодических и сохраняющих меру функций.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge 2}$ + 17))

Билет 29
1. Сплетения и ГПСЧ с динамически изменяющимся законом.
2. Транзитивно ли отображение f(x) по модулю 256? f(x) = (x XOR 1) XOR (2(x AND (1 + 2x) AND (3 + 4x) AND (7 + 8x) AND (15 + 16x) AND (31 + 32x) AND (63 + 64x))) XOR (4($x^{\wedge 2}$ + 14))

Билет 30 1. Структура ГПСЧ с динамически изменяющимся законом, построенных на основе сплетений.
2. Сбалансирована ли Т-функция F(x, y, z) = (1 XOR x XOR ((y_2 XOR y)(z_2 XOR z)), x + y, x + y + z) по модулю $2^{\wedge 256}$?

Примерное практическое контрольное задание для промежуточной аттестации.

ПКЗ ПА. Нахождение длины периода ГПСЧ

В качестве закона рекурсии ГПСЧ берется некоторая Т-функция, требуется определить область, на которой эта Т-функция эргодична и на основании этого найти дину периода соответствующего ГПСЧ.

Методические материалы для проведения процедур оценивания результатов обучения

Практическое контрольное задание для промежуточной аттестации является довольно объемным, поэтому частично выполняется в качестве домашней контрольной работы для текущего контроля успеваемости. Выполнение каждой практической самостоятельной работы текущего контроля успеваемости может принести максимум 25 баллов, в итоге по результатам работы в семестре учащийся может набрать максимум 50 баллов. На промежуточной аттестации можно набрать 150 баллов – 100 баллов максимум по итогам индивидуального собеседования (50 баллов максимум за первый вопрос билета и 50 баллов максимум за второй вопрос билета), плюс 50 баллов максимум за выполнение практического контрольного задания. Итоговая сумма, не меньшая 170, соответствует оценке «отлично», от 135 до 169 – оценке «хорошо», от 90 до 134 – оценке «удовлетворительно», меньшая 90 – оценке «неудовлетворительно».