САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 1

1. Определение генератора случайных чисел. Генератор псевдослучайных чисел.
2. Ограничения применимости критерия Колмогорова-Смирнова.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 2

1. Применение псевдослучайных чисел.
2. В чем суть критерия интервалов (без формул).

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 3

1. Что называется ГСЧ с источником энтропии?
2. Описание побитового теста.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 4

1. Формула генерации ПСЧ методом средин квадратов.
2. Описание частотного блочного теста.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 5

1. Какое число следует за 1010101010 в методе средин квадратов.
2. Описание теста на периодичность.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 6

1. ГПСЧ на основе трансцендентных иррациональных чисел.
2. Описание теста кумулятивных сумм.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 7

1. Какой ГПСЧ называется криптостойким?
2. Описание критерия серий.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 8

1. Линейный конгруэнтный метод.
2. Что проверяется в критерии перестановок?

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 9

1. Критерий выбора модуля линейного конгруэнтного алгоритма
2. Формулировка критерия монотонности.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 10

1. Критерий выбора множителя линейного конгруэнтного алгоритма.
2. Формулировка критерия промежутков между днями рождений.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 11

1. Критерий выбора потенциала линейного конгруэнтного метода.
2. Формулировка критерия сериальной корреляции.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 12

1. Почему конгруэнтная ПСЧ имеет недостатки, если a и m из формулы $X_{n+1}=(aX_n+c) \bmod m$ не взаимно простые?
2. Формулировка критерия подпоследовательностей.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 13

1. В хорошем источнике случайных чисел неравенства $X_{n-1}<X_{n+1}<X_n$ примерно один раз из шести, так как каждое из шести возможных отношений порядка должно иметь одну и ту же вероятность появления. Покажите, что приведенный выше порядок никогда не возникает, если использовать для генерации метод Фибоначчи: $X_{n+1} = (X_n+X_{n-1}) \bmod m$.
2. Спектральный критерий.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 14

1. У вас есть 2 шестигранных игральных кости, все грани которых пронумерованы от 1 до 6. Бросая две кости сразу, Вы получаете число от 1 до 12. Сколько всего вариантов последовательностей при 144-х бросаниях этих костей?
2. Как можно использовать дискретное преобразование Фурье для тестирования случайности ПСЧ.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 15

1. Какие криптографические алгоритмы можно использовать для генерации ПСЧ?
2. Как из ПСЧ с равномерным распределением получить ПСЧ другого непрерывного распределения?

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 16

1. Аддитивный генератор ПСЧ.
2. Получение последовательности ПСЧ с биноминальным распределением.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 17

1. Рэндомизация перемешиванием.

2. Получение последовательности ПСЧ с пуассоновским распределением со средним мю.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 18

1. Модификации линейного конгруэнтного алгоритма генерации ПСЧ.
2. Получение последовательности ПСЧ с геометрическим распределением.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 19

1. Формулировка критерия монотонности.
2. Получение последовательности ПСЧ с нормальным распределением.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 20

1. Структура генератора ПСЧ.
2. Получение последовательности ПСЧ с показательным распределением.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 21

1. Получение последовательности ПСЧ с гамма-распределением порядка a>0.

2. Нелинейная комбинация РСЛОС.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 22

1. Получение последовательности ПСЧ с бета-распределением.
2. Генератор «стоп-пошёл».

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 23

1. Получение последовательности ПСЧ с Хи-квадрат-распределением.

2. ГПСЧ «Каскад Голлмана».

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 24

1. Получение последовательности ПСЧ с F-распределением

2. Прореживаемый ГПСЧ.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 25

1. Получение последовательности ПСЧ с Т-распределением.

2. ГПСЧ на базе клеточного автомата.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 26

1. ГПСЧ «Вихрь Мерсенна».

2. Требования к криптографически стойкому ГПСЧ.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 27

1. Аппаратные генераторы ПСЧ.

2. ГПСЧ ANSI X9.17.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 28

1. ГПСЧ Шамира и RSA.

2. Критерий равномерности.

Зав. кафедрой _____ В.Н. Салий

САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра *теоретических основ компьютерной безопасности и криптографии*

Специальность «*Компьютерная безопасность*»

Дисциплина «*Теория псевдослучайных генераторов*»

Экзаменационный билет № 29

1. ГПСЧ Блюма-Микали.

2. Критерий конфликтов.

Зав. кафедрой _____ В.Н. Салий