Вопросы для подготовки к экзамену по предмету «Теория ГПСЧ»

1 Структура генератора ПСЧ

1.1 Основные понятия
1.2 Виды генераторов случайных чисел
1.3 Стандарты и нормативные документы
1.4 Структура генератора псевдослучайных чисел
1.5 Аппаратные генераторы случайных чисел

2 Алгоритмы генерации псевдослучайных чисел

2.1 Метод срединных квадратов
2.2 Линейный конгруэнтный метод
2.3 Аддитивный ГПСЧ
2.4 Метод М-последовательности. Регистр сдвига с обратной линейной связью
2.5 Нелинейная комбинация РСЛОС. Генератор Геффа
2.6 Генератор «стоп-пошёл»
2.7 Пороговый генератор
2.8 Многоскоростной генератор с внутренним произведением
2.9 Суммирующий генератор случайных чисел
2.10 Динамический генератор случайной последовательности
2.11 Каскад Голлмана
2.12 Прореживаемый генератор
2.13 Самопрореживаемый генератор
2.14 Алгоритм A5
2.15 Hughes XPD/KPD
2.16 Алгоритм Fish
2.17 Алгоритм Pike
2.18 Алгоритм Mush
2.19 ГПСЧ на базе клеточного автомата
2.20 Вихрь Мерсенна
2.21 Рэндомизация перемешиванием

3 Криптографически стойкие генераторы псевдослучайных чисел

3.1 Требования к КСГПСЧ
3.2 Безопасный блочный шифр
3.3 ANSI X9.17
3.4 FIPS 186. Алгоритм генерации секретного ключа для ЭЦП.
3.5 FIPS 186. Алгоритм генерации секретного числа сообщения для ЭЦП
3.6 Криптографически стойкая хэш-функция
3.7 ГПСЧ использующие алгоритмы потокового шифра
3.8 ГПСЧ на основе вычислительно сложных математических задачах

4 Тестирование статистических свойств случайных чисел

4.1 Виды тестов
4.2 Критерий хи-квадрат (χ2-критерий)
4.3 Критерий Колмогорова-Смирнова
4.4 Критерий равномерности
4.5 Критерий серий
4.6 Критерий интервалов
4.7 Критерий разбиений
4.8 Критерий перестановок
4.9 Критерий монотонности
4.10 Критерий конфликтов
4.11 Критерий промежутков между днями рождений
4.12 Универсальный статистический тест Маурера
4.13 Статистические критерии NIST

5 Генерация случайных чисел соответствующих различным распределениям

5.1 Стандартное равномерное распределение
5.2 Общий случай равномерного распределения
5.3 Треугольное распределение
5.4 Общее экспоненциальное распределение с параметрами положения и масштаба
5.5 Нормальное распределение (распределение Гаусса)
5.6 Гамма-распределение
5.7 Распределение Вейбулла-Гнеденко
5.8 Логнормальное распределение
5.9 Логистическое распределение
5.10 Многомерное нормальное распределение
5.11 Биномиальное распределение