**Вопросы для подготовки к экзамену по дисциплине «Теория генераторов псевдослучайных чисел»**

1. **Основные понятия. Структура генератора псевдослучайных чисел**
   1. Виды генераторов случайных чисел
      1. Случайное, псевдослучайное, физическое случайное число, детерминированный алгоритм, ГПСБ-ГПСЧ, тест на следующий бит, универсальность ТСБ.
   2. Стандарты и нормативные документы
      1. Виды генераторов, стандарты: российские (28147-89, 34.11-2012, ИСО 28640-2012), американские (SP 800-38A,B, SP 800-90A, SP 800-22, ANSI X9.82, ANSI X9.17)
   3. Структура генератора псевдослучайных чисел
      1. строка персонализации, код сеанса, источник энтропии, функция инициализации, реинициализации, деинициализации, генерации значения)
   4. Аппаратные генераторы случайных чисел
      1. источники энтропии, преобразование сигнала, проблемы.
2. **Алгоритмы генерации псевдослучайных чисел**
   1. Метод срединных квадратов
   2. Линейный конгруэнтный метод
      1. максимальная длина периода ЛКГ, условия максимальности периода, потенциал.
      2. полиномиальный КГ.
   3. Аддитивный ГПСЧ
      1. максимальная длина периода, условие максимальности периода.
   4. Инверсный конгруэнтный генератор
   5. Метод М-последовательности. Регистр сдвига с обратной линейной связью
      1. ассоциированный многочлен, максимальный период, условие максимальности периода, свойства ПСБ зависящие от ассоц. многочлена.
   6. Нелинейная комбинация РСЛОС. Генератор Геффа
      1. Метод Таусворта, условие максимальности периода
      2. Генератор с обратной связью по переносу, условия макс. периода.
      3. Длина периода генератора Геффа.
   7. Генератор «стоп-пошёл», модификации
   8. Пороговый генератор
      1. условия на длины периодов и многочлены обратной связи
   9. Многоскоростной генератор с внутренним произведением
   10. Суммирующий генератор случайных чисел
   11. Динамический генератор случайной последовательности
   12. Каскад Голлмана
       1. Линейная сложность (словия)
   13. Прореживаемый генератор
   14. Самопрореживаемый генератор
   15. Алгоритм А5
   16. Hughes XPD/KPD
   17. Алгоритм Fish
   18. Алгоритм Pike
   19. Алгоритм Mush
   20. ГПСЧ на базе клеточного автомата
   21. Вихрь Мерсенна
       1. период
   22. Рэндомизация перемешиванием
       1. уязвимость
3. **Криптографически стойкие генераторы псевдослучайных чисел**
   1. Требования к КСГПСЧ
      1. Линейная сложность, свойства, линейная сложность РСЛОС
      2. виды КСГПСЧ
   2. Безопасный блочный шифр
      1. режим счетчика, уникальность значений счетчика, режим гаммирования
   3. ANSI X9.17
      1. длина ключа, инициализационного вектора.
   4. FIPS 186. Алгоритм генерации секретного ключа для ЭЦП
      1. длина ключа
   5. FIPS 186. Алгоритм генерации секретного числа сообщения для ЭЦП
   6. Криптографически стойкая хэш-функция
      1. требования к КСХФ,CRC,MD4 – 512/128 (этапы),
      2. 34.11-94 (256/256/256)
      3. 34.11-2012 (512/512)
   7. ГПСЧ использующие алгоритмы потокового шифра
   8. ГПСЧ на основе вычислительно сложных математических задачах
4. **Тестирование статистических свойств случайных чисел**
   1. Виды тестов
   2. Критерий хи-квадрат (χ2-критерий)
      1. квантиль
   3. Критерий Колмогорова-Смирнова
   4. Критерий равномерности
   5. Критерий серий
   6. Критерий интервалов
   7. Критерий разбиений
   8. Критерий перестановок
   9. Критерий монотонности
   10. Критерий конфликтов
   11. Критерий промежутков между днями рождений
   12. Универсальный статистический тест Маурера
   13. Статистические критерии NIST