Реализация криптографических алгоритмов в ИС

Лекция 3
Генерация случайных и псевдослучайных чисел (CSPRNG). Важность энтропии.

Содержание лекции

1. Генерация случайных и псевдослучайных чисел
2. Важность энтропии

Лекция 3
Генерация случайных и псевдослучайных чисел (CSPRNG). Важность энтропии.

1. Генерация случайных и псевдослучайных чисел

1. Генерация псевдослучайных чисел

Ключевой вопрос: Если мы шифруем данные с помощью идеального алгоритма (например, AES), но используем слабый ключ, сгенерированный плохим ГПСЧ, насколько безопасна наша система?

Ответ: **Абсолютно небезопасна.**

Генераторы псевдослучайных чисел (ГПСЧ) – это фундамент почти всех криптографических систем. Они используются для:

- Генерации ключей шифрования.
- Создания векторов инициализации (IV) и nonce.
- Выработки случайных значений для протоколов (например, в RSA, DSA, ECDSA).
- Создания "соли" (salt) для хеширования паролей.

1. Генерация псевдослучайных чисел

Определение: Генератор псевдослучайных чисел – алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению (обычно дискретному равномерному).

1. Генерация псевдослучайных чисел

Современная информатика широко использует псевдослучайные числа в самых разных приложениях – от метода Монте-Карло и имитационного моделирования до криптографии.

При этом от качества используемых ГПСЧ напрямую зависит качество получаемых результатов. Это обстоятельство подчёркивает известный афоризм математика ORNL Роберта Кавью: «***генерация случайных чисел слишком важна, чтобы оставлять её на волю случая***».

1. Генерация псевдослучайных чисел

Генерация случайных чисел – процесс, который с помощью устройства генерирует последовательность чисел или символов, которая может быть предсказана разумным образом только на основании случайности.

Генераторы случайных чисел:

1) «аппаратные генераторы случайных чисел» (HRNGS), которые генерируют случайные числа в зависимости от текущего значения какого-либо атрибута физической среды, который практически невозможно смоделировать при текущем уровне знаний,

2) генераторы псевдослучайных чисел (PRNGS), которые генерируют числа, которые выглядят случайными, но на самом деле являются детерминированными и могут быть воспроизведены, если известна модель (шаблон), на основании которой работает генератор псевдослучайных чисел.

1. Генерация псевдослучайных чисел

Существует множество методов генерации случайных данных, некоторые из которых существуют с древних времён.

Хорошо известные классические примеры – бросание игральной кости, подбрасывание монеты, тасование игральных карт, использование стеблей тысячелистника (для гадания) в «И Цзин» и др.

Из-за механического характера этих методов генерация большого количества достаточно случайных чисел (что важно в статистике) требовала много труда и времени, поэтому такие числа иногда собирались в **таблицы случайных чисел**.

В наше время на смену таблицам пришли генераторы случайных чисел.

1. Генерация псевдослучайных чисел

Вычислительные методы генерации псевдослучайных чисел не достигают цели истинной случайности, хотя они могут с переменным успехом соответствовать некоторым тестам на статистическую случайность, предназначенным для измерения непредсказуемости их результатов (то есть, в какой степени распознаваемы их шаблоны).

Обычно это делают вычислительные методы непригодными для таких областей применения, как криптография. Однако существуют также тщательно разработанные «криптографически стойкие генераторы псевдослучайных чисел» (**CSPRNGS**) со специальными функциями, специально разработанными для использования в криптографии.

1. Генерация псевдослучайных чисел

- **CSPRNG** – (Cryptographically Secure Pseudorandom Number Generator)
  - C - Cryptographically
  - S - Secure
  - P - Pseudo (random)
  - R - random
  - N - Number
  - G - Generator

1. Генерация псевдослучайных чисел

В июне 2025 года учёные из Университета Колорадо в Боулдере представили прорывную технологию генерации случайных чисел, устойчивых к подделке. Система **CURBy (Colorado University Randomness Beacon)** объединяет квантовую запутанность и блокчейн-подобные цепочки хешей, обеспечивая беспрецедентную защиту от манипуляций.

1. Генерация псевдослучайных чисел

В Python работа с генераторами случайных и псевдослучайных чисел организована через несколько модулей, каждый из которых имеет свою специфику и область применения:

1. Модуль random – основной для псевдослучайных чисел

2. Модуль secrets – для криптографических задач

3. Модуль os – низкоуровневый доступ к энтропии

4. Модуль numpy.random – для научных вычислений

Лекция 3
Генерация случайных и псевдослучайных чисел (CSPRNG). Важность энтропии.

2. Важность энтропии

2. Важность энтропии

Энтропия – мера неопределённости (случайности) в системе. В криптографии она отражает степень непредсказуемости данных, используемых при генерации ключей, векторов инициализации и соли.

2. Важность энтропии

- Качество ключей напрямую зависит от источника случайности.
- Без достаточной энтропии злоумышленник может предсказать генерацию ключей.
- CSPRNG требует высокоэнтропийного начального зерна (seed).
- Низкая энтропия делает систему уязвимой к атакам восстановления состояния генератора.

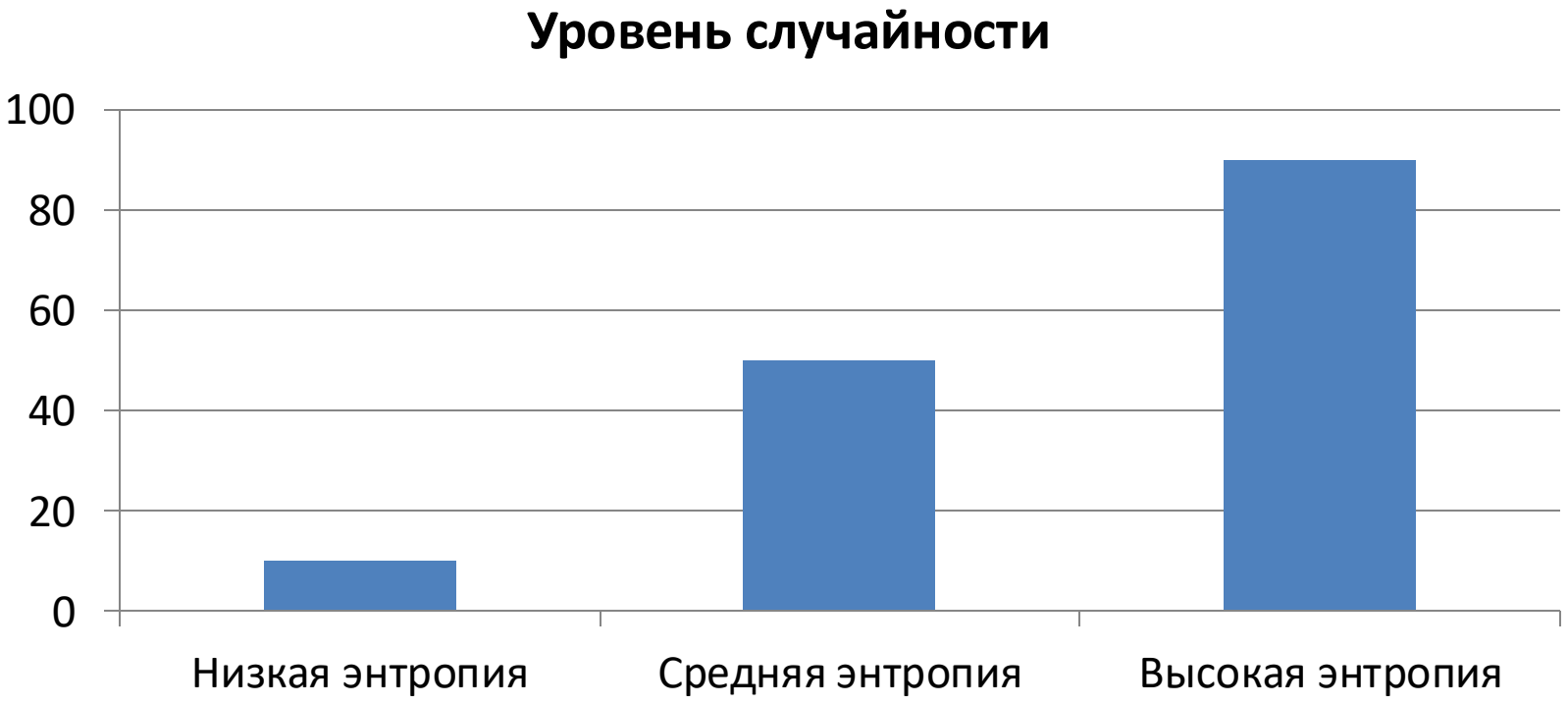
2. Важность энтропии

Примеры физических источников энтропии:

- Интервалы между нажатиями клавиш
- Движения мыши
- Тепловой шум, квантовые флуктуации
- Сетевые задержки

Операционные системы используют эти данные для наполнения энтропийного пула (например, /dev/random в Linux).

2. Важность энтропии



2. Важность энтропии

Даже самый надёжный криптоалгоритм уязвим при низкой энтропии.

- Проверяйте наличие достаточного источника случайности при генерации ключей.
- Используйте криптографически стойкие генераторы (например, secrets, os.urandom).
- Контролируйте качество энтропийного пула в виртуальных средах.

Энтропия – фундамент доверия к криптосистеме.