ГПСЧ – алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному).

**Криптостойкость**

Тест на следующий бит - тест, служащий для проверки генераторов псевдослучайных чисел на криптостойкость. Тест гласит, что *не должно существовать полиномиального алгоритма, который, зная первые k битов случайной последовательности, сможет предсказать k+1 бит с вероятностью, неравной ½.*

Пример: генератор, основанный на числе Пи, который начинает выводит числа с неизвестной точки. Однако этот подход не является критографически надежным — если криптоаналитик определит, какой бит числа Пи используется в данный момент, он сможет вычислить и все предшествующие и последующие биты.

Данный пример накладывает ещё одно ограничение на генераторы случайных чисел. Криптоаналитик *не должен иметь возможности предсказать работу генератора случайных чисел.*

Хабр [https://habr.com/post/151187/]

**Отличие генератора псевдослучайных чисел (ГПСЧ) от генератора случайных чисел (ГСЧ)**

Источники энтропии используются для накопления энтропии с последующим получением из неё начального значения (initial value, seed), необходимого генераторам случайных чисел (ГСЧ) для формирования случайных чисел. ГПСЧ использует единственное начальное значение, откуда и следует его псевдослучайность, а ГСЧ всегда формирует случайное число, имея в начале высококачественную случайную величину, предоставленную различными источниками энтропии.

Энтропия – это мера беспорядка. Информационная энтропия — мера неопределённости или непредсказуемости информации.

Можно сказать, что ГСЧ = ГПСЧ + источник энтропии.