Программный комплекс «Энтропийный анализ дискретных последовательностей» (ЭАДП)

Программный комплекс предназначен для анализа выходных последовательностей криптографических генераторов на основе энтропии Шеннона, Реньи и Тсаллиса. Позволяет получить как числовые данные – значения оценок энтропии при различных значениях длины фрагмента, задающего размерность алфавита, *p*-значения тестов, так и их визуализацию в зависимости от длины фрагмента (энтропийный профиль).

В начале работы необходимо выбрать файл с последовательностью, порядок бит (прямой Big Endian или обратный Little Endian), диапазон длин фрагмента *s* и функционалы энтропии. Вычисляемые значения добавляются на экран в режиме реального времени. Имеется возможность изменять уровень значимости α без пересчёта оценок энтропии и переключаться на различные режимы отображения: непосредственно оценки энтропии, удельная энтропия, нормированные значения, *p*-значения.

В отличие от известных батарей тестов, основанных на классической асимптотике, при которой отношение длины последовательности и числа параметров стремится к бесконечности, статистические тесты в программе основаны на специальной асимптотике, при которой указанное отношение стремится к конечному числу, что более адекватно описывает примеры, возникающие на практике. Также имеется возможность проверки сложной нулевой гипотезы, позволяющей учитывать незначительные отклонения распределения вероятностей тестируемой последовательности от *s*-мерной равномерности, с помощью оценок энтропии Тсаллиса.