УДК 519.233.3

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ОЦЕНИВАНИЯ МИНИМАЛЬНОЙ ЭНТРОПИИ

И. К. Пирштук, Д. Е. Бородина

Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь, pirshtuk@bsu.by, borodinad313@gmail.com

Рассматривается задача сравнительного анализа алгоритмов оценивания минимальной энтропии источников случайности по сложности реализации, точности оценивания и быстродействию. Для вычисления гарантированной оценки минимальной энтропии используются верхние границы доверительных интервалов 10 алгоритмов, по которым вычисляется оценка минимальной энтропии, и далее выбирается наименьшая энтропия из всех алгоритмов. Приведены результаты численных экспериментов на реальных данных.

Ключевые слова: верхняя граница доверительного интервала; источник случайности; минимальная энтропия; статистический тест; генератор случайных числовых последовательностей.

RESEARCH ON THE EFFECTIVENESS OF ALGORITHMS MINIMUM ENTROPY ESTIMATES

I. K. Pirshtuk, D. E. Borodina

Belarusian State University, Nezavisimosti ave., 4, 220030, Minsk, Belarus, pirshtuk@bsu.by, borodinad313@gmail.com

The problem of comparative analysis of algorithms for estimating the minimum entropy of randomness sources in terms of implementation complexity, estimation accuracy and performance is considered. To calculate the guaranteed estimate of the minimum entropy, the upper bounds of the confidence intervals of 10 algorithms are used, according to which the estimate of the minimum entropy is calculated, and then the smallest entropy of all algorithms is selected. The results of numerical experiments on real data are presented.

Keywords: upper bound of the confidence interval; source of randomness; minimum entropy; statistical test; generator of random numerical sequences.

Введение

Генераторы случайных числовых последовательностей (ГСЧП) являются неотъемлемыми элементами современных систем криптографической защиты информации для решения следующих основных задач [1]: генерация сеансовых и других объектов в криптосистемах; генерация

случайных значений параметров для систем электронной цифровой подписи; формирование случайных запросов при реализации существующих криптографических протоколов выработки общего секретного ключа и аутентификации. Если последовательность случайных чисел окажется предсказуемой, то даже стойкий алгоритм шифрования при использовании этих чисел может оказаться уязвимым.

Лучшими источниками энтропии являются физические источники случайности. На практике используют и другие источники. Например, системные часы, системные буферы или буферы ввода-вывода; серийные номера или адреса пользователя, системы, оборудования, сети; пользовательский ввод с клавиатуры и мыши. Однако каждый из этих источников может произвести лишь ограниченное или предсказуемое количество случайных величин при некоторых обстоятельствах.

Для проверки случайного характера формируемых последовательностей случайных чисел на практике проводятся статистические тесты: сначала для первичных случайных данных, а потом для итоговых, как правило, бинарных данных. Цель проверки – определить является ли последовательность независимой и равномерно распределенной случайной последовательностью. Что позволяет выявить приемлемые источники случайности для решения криптографических задач.

Существует два варианта вычисления оценки энтропии выходной последовательности. Предполагается, что выходная последовательность является независимой и одинаково распределенной (далее – последовательности *idd*). Такое предположение в случае подтверждения значительно упрощает процесс оценки энтропии. Выходная последовательность *idd* тестируется с использованием перестановочных статистических тестов и статистических тестов хи-квадрат. Если в результате тестирования предположение о независимой и одинаково распределенной последовательности не подтверждается (далее – последовательности *non-idd*), то оценка энтропии более сложна и формируется как наихудшая из оценок минимальной энтропии.

Национальный институт стандартов и технологий США [2] (NIST) публикует в открытом доступе стандарты и специальные рекомендации в области информационной безопасности. В данной работе мы проанализируем алгоритмы, внесенные в финишную редакцию документа NIST.SP.800-90B (январь 2018) [3], а также программное обеспечение к нему.

Целями исследования являются:

– проведение сравнительного анализа алгоритмов оценивания минимальной энтропии по сложности реализации, точности и быстродействию [3];

– разработка инструкций и рекомендаций по установке стандартных программных средств по оценке минимальной энтропии данных с использованием пакетов NIST;

– разработка собственной реализации алгоритмов;

– проведение численных экспериментов на данных различной природы (физический ГСЧП, системные файлы, музыкальные файлы и т.п.).

1. Алгоритмы оценивания минимальной энтропии

В [3] приведено описание 10 алгоритмов (тестов) оценивания минимальной энтропии: 1)частотный тест; 2) тест коллизий; 3) тест Маркова; 4) тест сжатия; 5) тест t-набора; 6) тест наибольшей повторяющейся подстроки; 7) тест множественного прогнозирования наиболее частого значения в окне (MultiMCW); 8) тест прогнозирования задержки; 9) тест множественного прогнозирования моделей Маркова с подсчетом (MultiMMC); 10) тест прогнозирования LZ78Y (в оригинале стандарта NIST: 1. The Most Common Value Estimate; 2. The Collision Estimate; 3. The Markov Estimate; 4. The Compression Estimate; 5. *t*-Tuple Estimate; 6. Longest Repeated Substring (LRS) Estimate; 7. Multi Most Common in Window Prediction Estimate; 8. The Lag Prediction Estimate; 9. The MultiMMC Prediction Estimate; 10. The LZ78Y Prediction Estimate).

Ниже кратко опишем основную идею каждого из алгоритмов и их линейную сложность.

1. Частотный тест. Основная идея состоит в вычислении оценки вероятности наиболее часто встречаемого значения в выборке. Линейная сложность данного алгоритма O(n).

2. Тест коллизий. Линейная сложность O(n). Основная идея: измерение среднего времени (количества элементов) до первого совпадения в массиве наблюдений. Такое совпадение называется коллизией. Данный тест даёт низкую оценку энтропии для источников случайности, которые имеют значительное смещение частоты нескольких значений в отличие от остальных, что приводит к более быстрому появлению коллизий.

3. Тест марковской зависимости. Сложность O(n). В данном тесте строится оценка энтропии на основе зависимостей между соседними наблюдениями выходной последовательности. В качестве модели зависимости используется однородная цепь Маркова первого порядка (ОЦМ), в которой значение следующего наблюдения зависит только от значения текущего наблюдения. По исследуемой выходной последовательности оценивается матрица вероятностей переходов и вектор вероятностей начальных состояний.

Данный тест применяется только к бинарным последовательностям.

4. Тест сжатия. Сложность O(n). Основная идея: оценка энтропии на основе меры того, насколько сильно может быть сжата выходная последовательность без потери информации.

Данный тест также применяется только к бинарным последовательностям.

5. Тест частичных коллекций. Сложность $O(n^2)$. Данный тест основан на частоте частичных коллекций или t -наборов (пар, троек и т.д.), которые появляются во входном наборе данных, и производит оценку энтропии выборки на основе частоты этих t – наборов.

6. Тест наибольшей повторяющейся подстроки. Сложность $O(n^2)$. Данный тест основан на оценке энтропии коллизий источника, основываясь на количестве повторений подстрок (наборов) внутри набора данных, в частности на нахождении наиболее длинной повторяющейся подстроки.

7. Тест множественного прогнозирования наиболее частого значения в окне (MultiMCW) имеет сложность - O(n). MultiMCW-прогноз содержит несколько подпрогнозов, каждый из которых ставит целью угадать следующее выходное значение, основываясь на последних *w* выходных значениях. Каждый подпрогноз предсказывает значение, которое происходит чаще всего в этом окне из *w* предыдущих выходных значений. MultiMCW-прогноз содержит таблицу, хранящую количество раз, которое каждый из подпрогнозов был правильным, и использует подпрогноз с наиболее правильными предсказаниями для предсказывания следующего значения. MultiMCW-прогноз показывает низкую оценку энтропии, когда наиболее частое значение меняется с течением времени, но по-прежнему остается относительно постоянным.

8. Тест прогнозирования задержки имеет сложность O(n). Прогноз задержки содержит несколько подпрогнозов, каждый из которых предсказывает следующий выход, основываясь на заданной для данного подпрогноза задержке. Прогноз задержки содержит таблицу, хранящую количество раз, когда каждый из подпрогнозов был правильным, и использует подпрогноз с наиболее правильными предсказаниями для предсказывания следующего значения.

9. Тест множественного прогнозирования моделей Маркова с подсчетом. Сложность O(n). MultiMMC-прогноз состоит из множества подпрогнозов моделей Маркова с подсчетом. Каждый MMC-прогноз записывает наблюдаемые частоты для переходов от одного выходного значения к последующему выходному значению и делает прогноз, основываясь на наиболее частом наблюдаемом переходе из текущего выходного значения. Каждый подпрогноз имеет свою глубину и создает модель цепи Маркова порядка равного этой глубине, так с глубиной 1 создает мо-

дель первого порядка, в то время как MMC с глубиной D создает модель порядка D. MultiMMC содержит таблицу, хранящую количество раз, которое каждый из MMC-подпрогнозов был правильным, и использует подпрогноз с наиболее правильными предсказаниями для предсказывания следующего значения.

10. Тест прогнозирования LZ78Y. Сложность O(n). Прогноз содержит словарь строк, которые были добавлены в словарь к текущему моменту, и продолжает добавление новых строк в словарь до тех пор, пока словарь не достигнет своей максимальной емкости. Каждый раз, когда обрабатывается выборка, каждая подстрока из последних выборок обновляет словарь или добавляется в словарь. Для каждой подстроки и значения сохраняется количество раз, когда предсказание было успешным и далее для предсказания значения по строке выбирается значения с наиболее правильными предсказаниями.

Выделим основные особенности финишной редакции документа [3]:

1. Три алгоритма рекомендовано применять только к бинарным последовательностям, это тесты коллизий, Маркова и сжатия.
2. В описании алгоритмов при построении верхней границы вероятности используется квантили для доверительной вероятности 99% (в первой редакции документа доверительная вероятность равнялась 95%).
3. Уточнены формулы для расчета моментов, в частности, уточнен нормировочный коэффициент для вычисления моментов 2-го порядка, что, в принципе, не является значимым, однако теперь соответствует состоятельной оценке параметра.
4. Тест Маркова изменен существенно по сравнению с предыдущими версиями. В [3] алгоритм теста Маркова приведен только для однородной цепи Маркова первого порядка, что привело к значительному его упрощению: на основании выборочных статистических оценок начальных и переходных вероятностей строятся оценки вероятности получения шести фиксированных 128-битных строк, далее из них выбирается строка с наибольшей вероятностью, на основании которой строится оценка минимальной энтропии для данного теста. Тест можно применять *только* к бинарным последовательностям и практически любой длительности. Тем не менее, рекомендуется использовать выборки с более чем 1 000 000 отсчетов.
5. В алгоритме сжатия доопределен поправочный коэффициент с целью понижения среднеквадратического отклонения для зависимых данных (c=0.5907). При этом значение поправочного коэффициента указано явно. Отмечено, что в случае зависимых наблюдений значения поправочного коэффициента принадлежат интервалу [0.5; 07].

6. Все описанные тесты рекомендуется применять к последовательностям длительностью не менее 1 000 000 отсчетов и желательно проводить тестирование полным набором (батареей) тестов оценивания. Однако заметим, что в [3] смягчены требования к минимальному объему анализируемых данных для вычисления минимальной энтропии.

7. Для получения гарантированной оценки минимальной энтропии случайных данных источника случайности следует проводить оценивание минимальной энтропии для нескольких выборок (мы рекомендуем тестировать не менее 5 выборок по 1 Мб каждая с одного источника случайности).

Описание тестов приведено в [3] (на английском языке), а также в документе «Методика оценки энтропии источников случайности» (МИ.190159829.22.02 6].

Уменьшение объема исследуемой выборки может привести к завышенному значению оценки энтропии, увеличение объема исследуемой выборки ведет к более точному значению оценки энтропии.

Для получения гарантированной оценки энтропии рекомендуется использовать батарею тестов и проводить тестирование как можно большего количества последовательностей, полученных из рассматриваемого источника случайности.

Ниже приведем требования к выходным последовательностям источников случайности, примеры работы с программным обеспечением и численные результаты оценивания минимальной энтропии.

2. Требования к выходным последовательностям для оценивания минимальной энтропии

В криптографических приложениях рекомендуется использовать ГСЧП, выходные последовательности которых соответствуют требованиям тестов с высокими значениями оценок энтропии (≥ 0.997) [4].

Тестируемая последовательность в рассматриваемых тестах рассматривается как строка бит. Основным общим требованием для проведения любого из тестов является предоставление не менее 1 000 000 последовательных данных (в случае бинарных данных – бит) в исследуемой выборке, полученной из источника случайности. Значения после первых 1 000 000 данных могут игнорироваться. Заметим, что увеличение объема исследуемой выборки ведет к более точному значению оценки энтропии.

Если генерация последовательности размером в 1 000 000 значений невозможна, то допускается конкатенация (склеивание) нескольких последовательностей при условии, что они получены из одного и того же источника случайности и каждая из них содержит не менее 1 000 значений.

Оценка энтропии на основании тестирования одиночной последовательности может оказаться завышенной, поэтому рекомендуется проводить серию повторных запусков с использованием нескольких последовательностей, полученных из одного источника случайности.

Источники случайности могут иметь зависимости, выходящие за рамки возможностей одного отдельного теста. Поэтому для получения наиболее точного значения оценки целесообразно производить оценку источника случайности с использованием целого набора (батареи) тестов.

В качестве окончательного (или гарантированного) значения оценки энтропии источника случайности принимается минимальная из всех оценок минимальной энтропии, полученных при тестировании последовательности.

3. Примеры работы со стандартныими пакетами программ оценивания минимальной энтропии

В данном разделе приводится **методика работы с готовым программным обеспечением (ПО) [5].**

Для установки пакета SP800-90B_EntropyAssessment необходимо установить на компьютер программный код, который располагается на ресурсе Github (https://github.com/usnistgov/SP800-90B_EntropyAssessment). Для запуска кода требуется компилятор C++11, а также установленные библиотеки bzlib, divsufsort, jsoncpp, GMP MP и GNU MPFR. Для операционной системы Linux (Ubuntu) их можно установить с помощью команды “apt-get install libbz2-dev libdivsufsort-dev libjsoncpp-dev libssl-dev libmpfr-dev“.

В качестве входных данных пакет использует бинарные файлы, которые рекомендуется размещать в папке “bin“ внутри проекта.

Программный пакет состоит из двух основный отдельных разделов:

• тесты iid, подтверждающие, что набор данных является iid-последовательностью;

• тесты non-iid оценивания минимальной энтропии для любых предоставленных данных.

Для компиляции исходных файлов C++ в исполняемые файлы для обоих разделов пакета используется команда “make“. Также пакет предоставляет возможность раздельной компиляции для файлов первого и второго раздела с помощью команд “make iid“ и “make non_iid“ соответственно. После компиляции исходных файлов становятся доступными 2 команды: “./ea_iid “ и “./ea_non_iid “. Рассмотрим подробнее каждую из них.

Для работы с iid-последовательностями используется команда “./ea_iid“. В качестве обязательных входных параметров она принимает имя бинарного файла, данные из которого будут тестироваться. Данные

из бинарного файла интерпретируются двумя способами: как последовательность битов и как 30 последовательность из наборов по n бит каждый, по умолчанию n = 8. Число n можно задавать с помощью дополнительного опционального параметра. Для вывода полных результатов работы программы к команде можно добавить опциональный параметр “-v“. Таким образом, синтаксис команды можно представить в виде “ ./ea_iid [-v] [n]“.

Результатом выполнения команды являются два значения оценки энтропии (по битам и по наборам из n символов), посчитанные с помощью частотного метода, и выбор минимального из них, а также результаты прохождения последовательности тестов на независимость и одинаковую распределенность. При добавлении к команде флага “-v“ вместе с результатами программа также отобразит размер входных данных, количество n-символьных наборов в данных, вычисленное среднее значение, медиану, являются ли данные бинарными. Для теста оценки энтропии будут отображены промежуточные вычисляемые параметры (p(p-hat), pu(p_u), nmax(mode)). Также отображаются детали прохождения тестов последовательности на независимость и одинакокую распределенность.

Для работы с non-iid-последовательностями используется команда “./ea_non_iid“. Синтаксис ее аналогичен вышеописанной команде “./ea_iid“. Результатом выполнения команды “./ea_non_iid“ являются два значения оценки энтропии(по битам и по наборам из n символов) и выбор минимального из них. Данные итоговые оценки значения энтропии получены путем выбора минимального значения из всех оценок энтропии, полученных каждым тестом, описанным выше.

Также как и команда “./ea_iid“,команда “./ea_non_iid“, введенная с флагом “-v“, кроме описанных выше результатов отобразит дополнительную информацию: размер входных данных, количество n-символьных наборов в данных, а также значения оценки энтропии и промежуточные вычисляемые параметры для из каждого из десяти тестов.

4. Результаты численных экспериментов

Для проведения численных экспериментов использовались выходные последовательности физического генератора случайных чисел с источником случайности на основе шумового диода ND 102L. Данный генератор формирует выходную бинарную последовательность необходимого размера на основе первичных дискретных данных компаратора.

Для эксперимента были сформированы 5 бинарных последовательностей случайных чисел размером 1 МБ каждая. Эти последовательности были записаны в бинарный файл для дальнейшей работы. Для исследо-

вания зависимости времени работы тестов от длительности выборки использовались объединенные выборки (конкатенация файлов).

Для проверки корректности работы готового ПО было разработано собственное ПО на языке Pyton, которое по быстродействию проигрывает NIST, а по точности оценивания совпадает. Собственное ПО размещено на ресурсе Github (https://github.com/DEBorodina/SP800-90_Entropy Assesment).

Также проводились эксперименты с выходными последовательностями других источников случайности, в частности с музыкальными файлами и системными данными персонального компьютера.

Далее, с помощью пакета прикладных программ SP800-90B_EntropyAssessment для каждой последовательности были вычислены оценки минимальной энтропии с помощью каждого теста и выбраны минимальные из них. Последовательность интерпретировалась двумя способами: как последовательность бит (бинарная последовательность) и как последовательность байт (не бинарная последовательность). Тесты, предназначенные только для бинарной последовательности, для не бинарной последовательности пропускались. Результаты эксперимента для первого случая приведены в табл. 1, для второго случая в табл. 2.

Во время эксперимента также измерялось время выполнения каждого теста и всего набора тестов в целом. Результаты измерений для последовательности бит представлены в табл. 3, результаты измерений для последовательности байт в табл. 4. В таблицах также приведены средние значения времени выполнения каждого теста и всего набора.

*Таблиц*а 1

Оценки минимальной энтропии для последовательности бит

Название теста \ номер файла	**1**	**2**	**3**	**4**	**5**
Частотный тест	0.998372	0.998109	0.998383	0.998668	0.998409
Тест коллизий	0.943146	0.944420	0.953271	0.976680	0.940531
Тест марковской зависимости	0.999741	0.998980	0.999825	0.999507	0.999391
Тест сжатия	**0.892780**	**0.905933**	**0.917015**	0.947797	**0.885673**
Тест частичных коллекций	0.931125	0.935118	0.931125	**0.935118**	0.933095
Тест наибольшей повторяющейся подстроки	0.996381	0.991059	0.998460	0.997518	0.997033
Тест MultiMCW	0.998793	0.998975	0.998035	0.999387	0.998699
Тест прогнозирования задержки	0.999029	0.997471	0.998041	0.998681	0.999836
Тест множественного прогнозирования моделей Маркова с подсчетом	0.998484	0.998449	0.998890	0.998964	0.998787
Тест прогнозирования LZ78Y	0.998826	0.999424	0.998989	0.998765	0.998856
Минимальное значение	**0.892780**	**0.905933**	**0.917015**	**0.935118**	**0.885673**

Как видно из табл. 1 четыре минимальных значения энтропии обеспечивает тест сжатия.

Таблица 2

Оценки минимальной энтропии для последовательности байт

Название теста \ номер файла	**1**	**2**	**3**	**4**	**5**
Частотный тест	7.881996	7.876381	7.882327	7.880673	7.893625
Тест частичных коллекций	**7.368524**	**7.388520**	**7.349074**	**7.349074**	7.388520
Тест наибольшей повторяющейся подстроки	7.746931	7.550441	7.938298	7.942519	7.942662
Тест (MultiMCW)	7.944132	7.972408	7.970294	7.952452	7.976998
Тест прогнозирования задержки	7.933886	7.966863	7.955692	7.938698	7.933200
Тест множественного прогнозирования моделей Маркова с подсчетом	7.903666	7.925672	7.957760	7.938008	6.655556
Тест прогнозирования LZ78Y	7.902973	7.923606	7.958787	7.936956	**6.655551**
Минимальное значение	**7.368524**	**7.388520**	**7.349074**	**7.349074**	**6.655551**

Как видно из табл. 2 четыре минимальных значения энтропии обеспечивает тест частичных коллекций.

Таблица 3

Время прохождения тестов для последовательности бит, сек

Название теста \ номер файла	**1**	**2**	**3**	**4**	**5**	Среднее
Частотный тест	0.023	0.023	0.022	0.023	0.023	0.0228
Тест коллизий	0.038	0.039	0.039	0.039	0.041	0.0392
Тест марковской зависимости	0.078	0.078	0.079	0.078	0.079	0.1826
Тест сжатия	0.717	0.732	0.745	0.756	0.689	0.0784
Тест частичных коллекций	2.329	2.340	2.439	2.401	2.372	0.7278
Тест наибольшей повторяющейся подстроки	2.329	2.340	2.439	2.401	2.372	2.3762
Тест MultiMCW	1.101	1.100	1.109	1.168	1.105	1.1166
Тест прогнозирования задержки	1.895	1.879	1.923	1.896	1.891	1.8968
Тест множественного прогнозирования моделей Маркова с подсчетом	3.037	2.268	2.268	2.675	2.386	**2.5250**
Тест прогнозирования LZ78Y	2.171	2.009	2.009	2.288	2.101	2.1636

Как видно из табл. 3 быстродействие тестов достаточно высокое, а самый медленный тест выполняется в среднем за 2.525 сек.

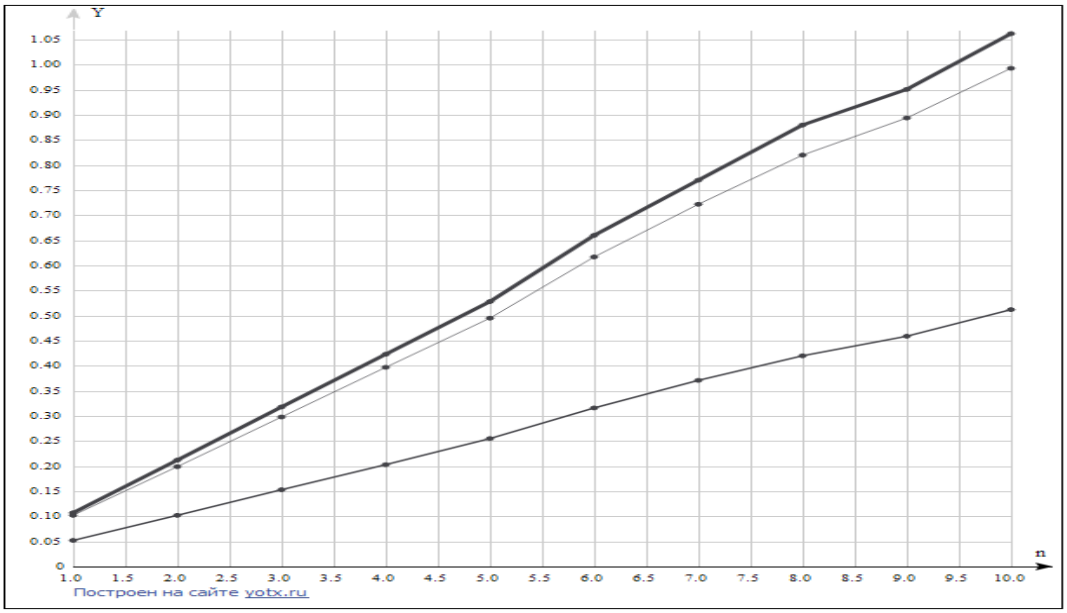
Таблица 4

Время прохождения тестов для последовательности байт, сек

Название теста \ номер файла	**1**	**2**	**3**	**4**	**5**	Среднее
Частотный тест	0.001	0.001	0.001	0.001	0.001	0.001
Тест частичных коллекций	0.130	0.131	0.129	0.139	0.130	0.132
Тест наибольшей повторяющейся подстроки	0.130	0.131	0.129	0.139	0.130	0.132
Тест MultiMCW	0.070	0.072	0.074	0.078	0.078	0.074
Тест прогнозирования задержки	0.028	0.029	0.028	0.034	0.029	0.030
Тест множественного прогнозирования моделей Маркова с подсчетом	9.133	9.345	9.228	9.058	9.066	9.166
Тест прогнозирования LZ78Y	14.492	15.874	14.981	14.275	14.309	14.786
Общее время оценки энтропии	**24.853**	**26.451**	**25.440**	**24.557**	**24.612**	**25.183**

Как видно из табл. 4, среднее время обработки одного файла составляет около 25 сек. Отметим также быстродействие частотного теста: около 0.001 сек обрабатывался файл длительностью 1 МБ.

В качестве иллюстрации на рисунке приведены графики зависимостей времени работы алгоритмов от объема тестируемой последовательности для трех тестов: тест Маркова, верхний график; частотный тест, средний график; тест коллизий, нижний график.



Графики зависимостей времени работы тестов от объема выборки

Из рисунка видно, что продолжительность работы тестов практически линейно (со скидкой на помехи и отклонения в работе ЭВМ) зависит от объема тестируемой выборки.

Заключение

1. Проанализированы методы и алгоритмы тестирования выходных последовательностей (iid и no-iid) источников случайности на основе документа NIST SP 800-90B (2018). Выработаны рекомендации по выбору тестов и их параметров для оценки минимальной энтропии. В качестве гарантированной итоговой оценки минимальной энтропии следует выбирать наихудшую из рассмотренных оценок.

2. Описана методика установки и работы с пакетом прикладных программ SP800-90B_EntropyAssessment (ППП), который предоставляет реализацию описанных алгоритмов на языке программирования C++.

3. С помощью пакета проведены численные эксперименты с 5 выходными бинарными последовательностями длительностью 1 МБ физического генератора случайных чисел на основе шумового диода ND 102L. Для каждой последовательности были вычислены оценки минимальной энтропии для всех 10 тестов. В качестве итоговой оценки минимальной энтропии выбиралась минимальная из всех полученных для данной последовательности. Также во время эксперимента было измерено время прохождения каждого теста и всего набора целиком.

4. Разработано, описано и размещено на ресурсе Github (https://github.com/DEBorodina/SP800-90_EntropyAssesment) собственное программное обеспечение на языке программирования python, включающее в себя приведенные в статье алгоритмы.

5. Проведены эксперименты для сравнения результатов работы собственного программного пакета с результатами, полученным с помощью готового программного обеспечения. В результате чего подтверждена корректность работы разработанной программы.

Библиографические ссылки

1. *Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В.* Криптология. Мн: БГУ, 2013. 512 с.
2. Computer Security Resource Center. URL: csrc.nist.gov.
3. Barker E. Recommendation for the Entropy Sources Used for Random Bit Generation / M. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, M. Boyle// This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-90B. – 2018. – 84 p.
4. A proposal for: Functionality classes for random number generators / Wolfgang Killmann, Werner Schindler // Режим доступа: https://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/15ss/15ss-taoc/01_AIS31_Functionality_classes_for_random_number_generators.pdf – Дата доступа: 15.10.2020
5. Dynamic-Link Libraries. https://msdn.microsoft.com/en-us/library/ windows/ desktop/ms682589(v=vs.85).aspx.
6. Методика оценки энтропии источников случайности (МИ.190159829.22.02). Минск, 2022.