Оригинальная статья / Original article

https://doi.org/10.21869/2223-1536-2025-15-4-8-21

УДК 519.24; 53; 57.017

Длина когнитивного пути итерационного снижения энтропии бинарных кодовых последовательностей от первоначального хаоса (идеального «белого» шума) до детерминизма монотонности

А. И. Иванов[1] ✉

[1] Пензенский научно-исследовательский электротехнический институт
ул. Советская, д. 9, г. Пенза 440000, Российская Федерация

✉ e-mail: bio.ivan.penza@mail.ru

Резюме

Целью *исследования является показ возможности оценки уровня когнитивности через снижение энтропии кодовой последовательности. При полном хаосе нет порядка, однако эволюция, естественный интеллект и искусственный интеллект способны противодействовать беспорядку, постепенно его уменьшая.*
Методы. *Энтропия Шеннона канонизирована и описана во всех учебниках, однако как инструмент практического применения она ущербна из-за огромной вычислительной сложности ее оценок. Тем не менее в этом веке стали активно разрабатываться альтернативные подходы, существенно упрощающие вычисления. В частности, энтропия в пространстве расстояний Хэмминга должна иметь линейную вычислительную сложность, а энтропия корреляционной сцепленности разрядов кода должна иметь квадратичную вычислительную сложность. Проблема состоит лишь в том, что энтропия Хэмминга и энтропия корреляционной сцепленности разрядов имеют собственные шкалы, не совпадающие со шкалой энтропии Шеннона.*
Результаты. *Метрик энтропии должно быть множество, одной из таких метрик является длина когнитивного пути от хаоса «белого» шума до полного детерминизма и монотонности. В статье приведена программная реализация оценки подобной метрики. Показано, что длина когнитивного пути сводится как к расстояниям Хэмминга, так и к коэффициентам корреляции между возникающими кодовыми последовательностями.*
Заключение. *Предложенная метрика длины когнитивного пути, видимо, должна иметь свою собственную энтропийную шкалу, не совпадающую со шкалой энтропии Шеннона. Все это следует рассматривать как удобный для практического применения частный случай некоторой упрощенной оценки сложной в вычислительном отношении задачи. По крайней мере, приведенную в статье программу можно рассматривать как еще одну систему тестов качества криптографического ключа, имеющую полиномиальную вычислительную сложность.*

Ключевые слова: *энтропия Шеннона; энтропия Хэмминга; энтропия корреляционных связей; энтропия когнитивного упрощения.*

Конфликт интересов: *Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Иванов А. И. Длина когнитивного пути итерационного снижения энтропии бинарных кодовых последовательностей от первоначального хаоса (идеального «белого» шума) до детерминизма монотонности // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2025. Т. 15, № 4. С. 8–21. https://doi.org/10.21869/ 2223-1536-2025-15-4-8-21

Поступила в редакцию 17.10.2025 *Подписана в печать 15.11.2025* *Опубликована 26.12.2025*

Length of the cognitive path of iterative reduction of the entropy of binary code sequences from the initial chaos (ideal "white" noise) to the determinism of monotonicity

Alexander I. Ivanov[1] ✉

[1] Penza Research Institute of Electrical Engineering
9 Sovetskaya Str., Penza 440000, Russian Federation

✉ e-mail: bio.ivan.penza@mail.ru

Abstract

The purpose of the research *is to demonstrate the possibility of assessing the level of cognition by reducing the entropy of the code sequence. In complete chaos there is no order, but evolution, natural intelligence and artificial intelligence are able to counteract disorder, gradually reducing it.*

Methods*. Shannon entropy is canonized and described in all textbooks, but as a tool for practical application it is flawed due to the enormous computational complexity of its estimates. However, in this century, alternative approaches have been actively developed that significantly simplify calculations. In particular, the entropy in the space of Hamming distances should have a linear computational complexity, and the entropy of the correlation entanglement of code bits should have a quadratic computational complexity. The only problem is that the Hamming entropy and the entropy of the correlation entanglement of bits have their own scales that do not coincide with the Shannon entropy scale.*

Results*. There should be many entropy metrics, one of such metrics is the length of the cognitive path from the chaos of "white" noise to complete determinism and monotony. The article provides a software implementation of the assessment of such a metric. It is shown that the length of the cognitive path is reduced to both the Hamming distances and the correlation coefficients between the resulting code sequences.*

Conclusion*. The proposed cognitive path length metric should apparently have its own entropy scale, which does not coincide with the Shannon entropy scale. All this should be considered as a convenient for practical use special case of some simplified evaluation of a computationally complex problem. At least, the program given in the article can be considered as another system of cryptographic key quality tests, which has polynomial computational complexity.*

Keywords: *Shannon entropy; Hamming entropy; entropy of correlation links; entropy of cognitive simplification.*

Conflict of interest: *The Authors declares the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Ivanov A.I. Length of the cognitive path of iterative reduction of the entropy of binary code sequences from the initial chaos (ideal "white" noise) to the determinism of monotonicity. *Izvestiya Yugo-Zapadnogo*

gosudarstvennogo universiteta. Serija: Upravlenie, vychislitel'naja tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering. 2025;15(4):8–21. (In Russ.) https://doi.org/10.21869/2223-1536-2025-15-4-8-21

Received 17.10.2025 *Accepted 15.11.2025* *Published 26.12.2025*

***

Введение

В середине прошлого века Клод Шеннон создал формулу для оценки информационной энтропии. Теоретическая значимость формулы Шеннона неоспорима, и сегодня она присутствует во всех учебниках. С практической точки зрения подобная оценка энтропии затруднительна для больших размерностей длины криптографического ключа:

$$H("x_1, x_2, ..., x_{256}") = -\sum_{i=1}^{N} P_i \cdot \log(P_i), \quad (1)$$

где $N \approx 2^{256}$ из-за того, что вероятность появления каждого i-го кодового состояния P_i мала. Чем выше число переменных в (1), тем больше нужна выборка для корректной оценки доверительной вероятности.

К сожалению, попытки оценки энтропии, по Шеннону, имеют экспоненциальную вычислительную сложность. В связи с этим качество криптографических ключей оценивается с использованием гораздо более простых в вычислительном отношении тестов [1].

Таким образом, научно-техническая общественность вынужденно двигается по пути замены сложной в вычислительном отношении оценки (1) к использованию группы более простых в вычислительном отношении тестов Национального института стандартов США. При этом этих тестов недостаточно [2], в общем случае базовой величиной остается энтропия [3].

Материалы и методы

Переход от анализа статистик обычных кодов в пространство расстояний Хэмминга

Одним из перспективных направлений исследований в контексте упрощения оценок энтропии является переход от статистического анализа обычных кодов к статистическому анализу в пространстве расстояний Хэмминга. То, что этот технический прием создан исследователями биометрических технологий, не случайно подтверждается использованием этой метрики в протоколах «биометрико-криптографического рукопожания» [4]. Кроме того, расстояния Хемминга и коэффициенты корреляции между кодами применимы и в других схемах аутентификации [5]. При этом попытки стандартизации «нечетких экстракторов» [6] оказались неудачными из-за многообразия их вариантов и низкой длины эквивалентного криптографического ключа аутентификации. Тем не менее расстояние Хэмминга оказалось полезным при оценках энтропии Шеннона для ключей биометрической аутентификации [7].

«Нечеткие экстракторы», активно создаваемые зарубежными исследователями в конце прошлого века, построены на том, что выполняется квантование «сырых» биометрических данных, при этом выполняется сравнение с порогом, совпадающим с математическим ожиданием предъявленной выборки биометри-

ческих данных. В итоге наиболее качественные биометрические параметры анализа рисунка радужной оболочки глаза позволяют получить код из 2096 бит после квантования «сырых» биометрических параметров. При этом ошибочных бит после квантования «сырых» данных оказывается много (наблюдается порядка 30% ошибочных бит). Технология «нечетких экстракторов» построена на том, что для обнаружения и устранения ошибок используются классические математические конструкции избыточных бинарных кодов.

Из теории известно, бинарные коды могут привить до 50% кодов. Однако таким конструкциям потребуется бесконечно большая избыточность. Естественно, что этот предельный режим на практике реализован быть не может. Для правки большого числа ошибок приходится использовать самокорректирующиеся коды с очень высокой избыточностью. Так, по данным Даугмана [8], после использования классического самокорректирующихся кодов реальная длина ключа аутентификации личности составляет 114 бит, т. е. при реализации своего «нечеткого экстрактора» Даугман использовал самокорректирующийся код с 2046/114≈18-кратной избыточностью.

Для нас принципиально важно то, что при обосновании ожидаемой длины ключа «нечеткого экстрактора» в 114 бит был использован переход в пространство расстояний Хэмминга:

$$h = \sum_{i=1}^{2046} ("x_i") \oplus ("c_i"), \qquad (2)$$

где "x_i" – один из разрядов проверяемого входного кода «нечеткого экстрактора» Даугмана; "c_i" – один из разрядов «нечеткого контейнера», используемого для обнаружения и устранения ошибок в «сыром» коде.

Принципиальным шагом по упрощению вычислений является то, что в место анализа огромного числа состояний системы $N \approx 2^{2046}$ по формуле Шеннона (1) переход в пространство расстояний Хэмминга (2) экспоненциально снижает число, анализируемых состояний до величины $N = 2047$.

Следует обратить особое внимание на то, что технология «нечетких экстракторов» на текущий момент не получила широкого распространения. Проблема состоит в том, что она ориентирована на применение классических самокорректирующихся кодов с огромной 18-кратной избыточностью. Это приводит к снижению длины криптографического ключа в 18 раз по отношению к числу анализируемых биометрических параметров.

Так общедоступное приложение «БиоНейроАвтограф», анализирующее рукописный почерк, позволяет получать всего 416 биометрических параметров. Если применить технологию «нечетких экстракторов», то мы получим длину ключа 416/18≈23 бит. Еще хуже складывается ситуация при анализе «нечеткими экстракторами» голоса [9] и рисунков отпечатков пальца.

Нейросетевое обогащение биометрических данных перед их квантованием

Установлено, что технология «нечетких экстракторов» эффективно работает, когда биометрические данные «хорошего» качества и их много. Когда данных мало и они «среднего» качества,

требуется слишком большая кодовая избыточность, а стабильно повторяющиеся ключи оказываются короткими.

Выходом из этого тупика является предварительное нейросетевое обогащение сырых биометрических данных до уровня приемлемого подавления в них хаоса. При этом, какая технология нейросетевого обогащения данных используется, не имеет значения. Типов искусственных нейронов множество, они могут быть объединены в нейросети с различными архитектурами. Каждая нейросетевая архитектура применима, если она позволяет обогащать данные до приемлемого качества и обеспечить необходимый объем. Это могут быть как простейшие однослойные или двухслойные нейросети, автоматически обученные по ГОСТ Р 52633.5-2011, либо это могут быть заранее предобученные многослойные нейросети глубокого обучения [10], ориентированные на распознавание лиц людей или перевода их голосового запроса в текстовый запрос [11].

Принципиально важным моментом является то, что в России введен стандарт по их тестированию на малых выборках ГОСТ Р 52633.3-2011. Он использует то, что в пространстве расстояний Хэмминга коды-отклики нейросети на образы «Чужой» имеют нормальное распределение. Это позволяет не ждать появления редких событий, как требует формула Шеннона (1), а предсказывать вероятности появления редких событий [12] в пространстве расстояний Хемминга. То же самое выполняется и в пространстве коэффициентов корреляции двух сравниваемых между собой кодов [13].

В итоге удается экспоненциально сократить объем тестовых выборок при оценке энтропии криптографических ключей, например, длиной 256 бит. При этом шкала энтропии Хэмминга не совпадает со шкалой энтропии Шеннона (рис. 1).

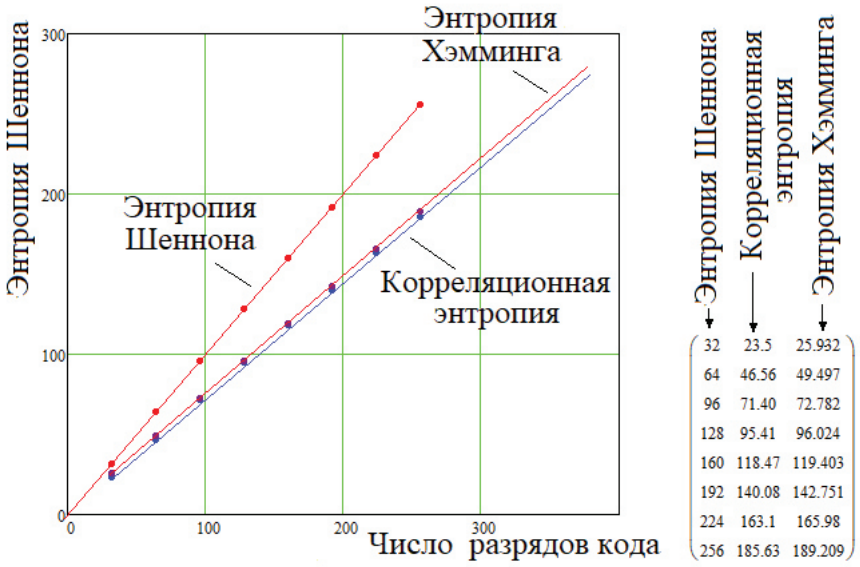

Рис. 1. Методические ошибки оценки энтропии по шкале Шеннона при ее оценках в пространстве расстояний Хэмминга и в пространстве корреляционной энтропии

Fig. 1. Methodological errors in estimating entropy on the Shannon scale when estimating it in the space of Hamming distances and in the space of correlation entropy

Очевидно, что более простые в вычислительном отношении оценки энтропии Хэмминга могут быть пересчитаны в значения энтропии Шеннона [14] путем следующего преобразования:

$$H("x_1, x_2, ..., x_N") \approx -0,41 + \\ + 1,377 \cdot X("x_1, x_2, ..., x_N"), \quad (3)$$

где $X("x_1, ..., x_N")$ – энтропия Хэмминга, вычисленная в рамках гипотезы нормального распределения расстояний Хэмминга для 32 случайно, выбранных из тестовой базы примеров биометрических образов «Чужой» по рекомендациям ГОСТ Р 52633.3-2011.

Параллельно с расстоянием Хэмминга энтропию можно оценивать через вычисление коэффициентов корреляции между кодами-откликами нейросети на образы «Чужой» [15]:

$$r \approx corr("\overline{x}","\overline{c}") \approx \\ \approx \frac{1}{N}\sum_{i=1}^{N}\frac{("x_i" - E("\overline{x}")) \cdot ("\overline{c}_i" - E("\overline{c}"))}{\sigma("\overline{x}") \cdot \sigma("\overline{c}")}, \quad (3)$$

где $E(.)$ – математическое ожидание анализируемых бинарных векторов; $\sigma(.)$ – стандартное отклонение анализируемых бинарных векторов.

В первом приближении можно рассматривать энтропию Хэмминга и корреляционную энтропию как два эквивалента классический энтропии Шеннона (1) с полиномиальной вычислительной сложностью оценок.

Заметим, что для идеального генератора бинарного «белого» шума последовательности одинаковой длины N при вычислении функционала (4) всегда дают случайные блуждания вокруг нулевого значения коэффициентов корреляции.

Коэффициенты корреляции, так же как расстояния Хэмминга, имеют нормальное распределение, т. е. оценить энтропию вполне возможно через предсказывание вероятности появления редких событий по данным распределения разных значений коэффициентов корреляции случайно выбранных 32 образов «Чужой». Шкала энтропии Шеннона и шкала корреляционной энтропии связаны линейно:

$$H("x_1, x_2, ..., x_N") \approx -0,334 + 1,377 \times \\ \times R("x_1, x_2, ..., x_N"), \quad (5)$$

где $R("x_1, \ldots, x_N")$ – корреляционная оценка энтропии.

При этом значения расстояний Хэмминга хорошо описываются законом биномиального распределения Бернулли, если стандартное отклонение расстояний Хэмминга интерпритировать как «среднегрупповую» неопределенного Гейзенберга для нескольких молекул (нескольких опытов малой выборки) [16]. Корреляционные расстояния появляются, если перейти от подбрасывания одной монеты по схеме Бернулли к подбрасыванию монет горстью [17].

Для корреляционных предсказаний вероятностей ошибок пока нет рекомендаций в форме национального стандарта по типу ГОСТ Р 52633.3-2011, будем надеяться, что он может появиться в силу линейной связи шкалы энтропии Шеннона со шкалой энтропии коэффициентов корреляции (4) (рис. 1).

Устранение случайности циклическими упорядочивающими перестановками состояний разрядов

Если мы хотим получить ключ длиной 256 бит, то нам потребуется обратиться к генератору псевдослучайных чисел. Далее необходимо выполнить квантование, присвоив состояние «0» отрицательным числам и состояние «1» положительным числам. При этом мы получим случайную бинарную последовательность. В первом приближении ее можно считать «белым» шумом.

Можно попытаться постепенно устранять из последовательности присутствие хаоса «белого» шума. Например, этого можно добиться, перегоняя нулевые состояния в начало последовательности, а единичные состояния в конец последовательности [18]. На рисунке 2 отображены первые три шага циклической перестановки состояний из начала последовательности в ее окончание.

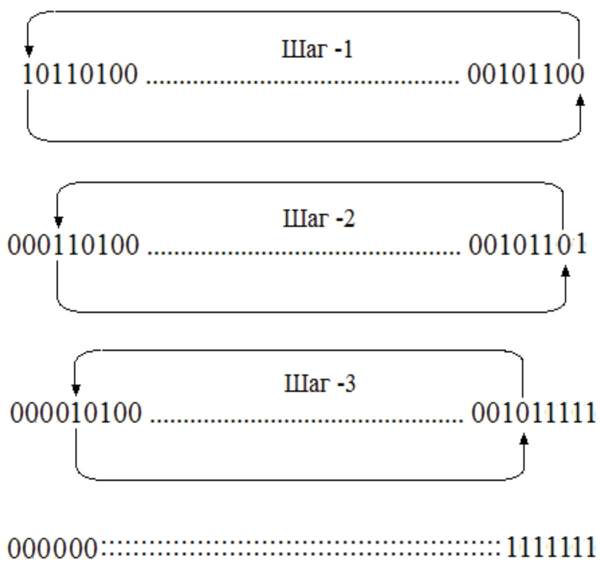

Рис. 2. Три первых шага циклических перестановок состояний «0» из начала в конец и последовательности с замещением их состояниями «1», первоначально расположенными в конце последовательности

Fig. 2. The first three steps of cyclic permutations of states "0" from the beginning to the end and the sequence with their replacement by states "1", initially located at the end of the sequence

На рисунке 2 видно, что начало последовательности состоит только из нулей «00000…», а конец последовательности состоит только из единиц «……111111». При этом длина монотонных входных и выходных состояний увеличиваются на каждом шаге алгоритма. На рисунке 3 представлена программа, реализованная на языке MathCAD, воспроизводящая соответствующий численный эксперимент, а также отражены его результаты.

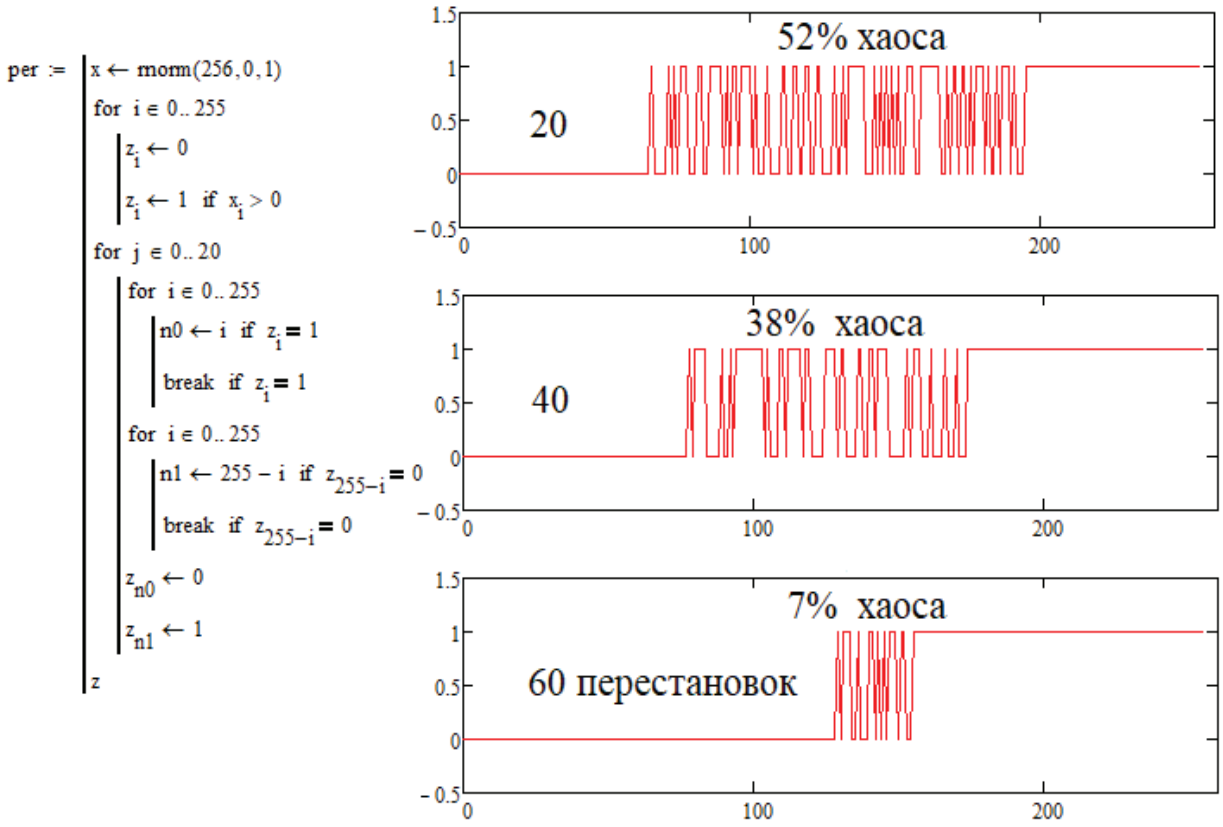

Рис. 3. Постепенное устранение хаоса из псевдослучайной бинарной последовательности через использование 20, 40, 60 кольцевых перестановок состояний «1»↔«0»

Fig. 3. Gradual elimination of chaos from a pseudo-random binary sequence through the use of 20, 40, 60 ring permutations of states "1"↔"0"

Из рисунка 3 видно, что по мере увеличения числа перестановок сжимается центральный интервал остаточного хаоса. Формально для любой бинарной последовательности можно вычислить, сколько потребуется перестановок для устранения некоторой изначально заданной части хаоса.

В нашем случае остаточная часть хаоса составляют 52%, 38%, 7% от его начального 100%-ного значения до запуска процедур упорядочивания. Предположительно число перестановок, требующееся для полного устранения хаоса, можно рассматривать как некоторую метрику когнитивного пути нейросетевого противодействия хаосу. По крайней мере, такая интерпретация хорошо ложится на технологии биометрико-нейросетевой идентификации и аутентификации.

Результаты и их обсуждение

Рассмотренная выше метрика длины когнитивного пути дополняет ранее уже известные три метрики. Это хорошо иллюстрирует связь числа понижающих энтропию перестановок. Связь числа перестановок с метрикой расстояний Хэмминга отображена ниже (рис. 4).

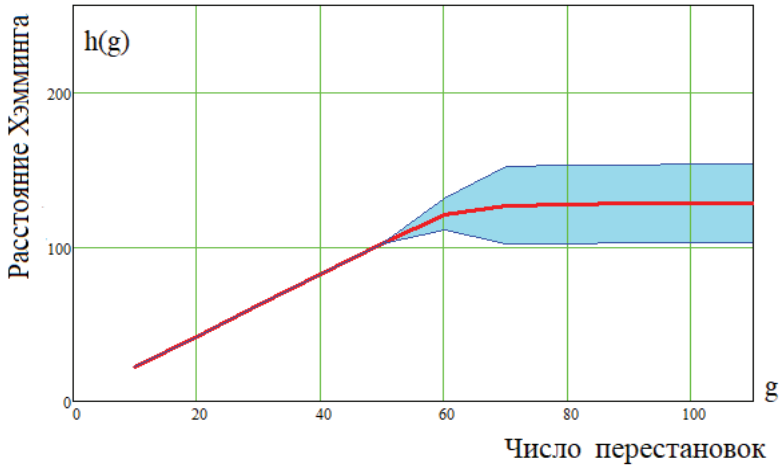

Рис. 4. Статистико-детерминированная связь метрики перестановок и метрики расстояний Хэмминга

Fig. 4. Statistically deterministic relationship between the permutation metric and the Hamming distance metric

Представленные на рисунке 4 данные получены в результате численного моделирования, построенного на программе, отображенной в левой части рисунка 3. Из рисунка 4 видно, что при применении до 50 перестановок новая метрика *–g* линейно связана с метрикой расстояний Хэмминга. При большем числе перестановок связь с расстоянием Хэмминга становится статистической. При этом математическое ожидание расстояний Хэмминга становится равным 128 бит, его стандартное отклонение монотонно увеличивается до значения в 8 бит.

Похожим соотношением метрика перестановок понижения энтропии *–g* связана с метрикой корреляционных связей (рис. 5).

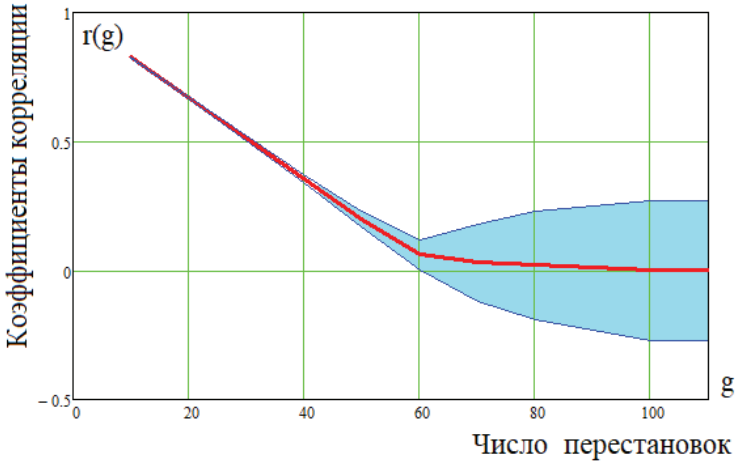

Рис. 5. Связь значений коэффициентов корреляции с числом перестановок -g, понижающих энтропию

Fig. 5. Relationship between the values of the correlation coefficients and the number of permutations -g that reduce entropy

В интервале до 40 перестановок –g их связь с коэффициентом корреляции является линейной и практически детерминированной. С ростом числа перестановок математическое ожидание значений коэффициентов корреляции приближается к нулевому значению. Стандартное отклонение монотонно увеличивается до значения $\sigma(r) \approx 0{,}0934$. Отмеченная затемненной заливкой площадь в правой части рисунка 5 соответствует режиму блужданий значений коэффициентов корреляции вокруг нулевого значения.

Скорее всего, может быть формализована связь, описывающая взаимное влияние метрики перестановок с метрикой Хэмминга и метрикой корреляционных связей. После формализации должна получиться система их двух уравнений. Появляется перспектива найти решение этой системы, дающее связи метрики перестановок с энтропией Шеннона. Тогда мы получим еще один эффективный алгоритм упрощенной оценки энтропии Шеннона, имеющий полиномиальную вычислительную сложность. Еще одним способом получить связь шкалы энтропии Шеннона с энтропией перестановок является имитационное моделирование. По крайней мере, это направление исследований технически реализуемо для коротких случайных последовательностей длинной до 32 бит.

Тем не менее вполне возможны простые процедуры связывания шкалы энтропии перестановок и шкалы энтропии Шеннона для кода длиной 256 бит. Промежуточные частные энтропии Шеннона, полученные для резных значений метрики –g, могут быть оценены в первом приближении следующим соотношением:

$$H(g) \approx \frac{n_{\text{хаос}}}{n_0 + n_{\text{хаос}} + n_1} \approx \frac{n_{\text{хаос}}}{256}, \qquad (6)$$

где $n_{\text{хаос}}$ – число изменяющихся разрядов остаточного хаоса, возникающих после применения g-шагов упорядочивания (рис. 3) в центре частично упорядоченной последовательности; n_0 – длина начального фрагмента монотонной последовательности, состоящего только из состояний «0»; n_1 – длина заключительной монотонной последовательности, состоящей только из «1».

Последнее означает, что для любой бинарной последовательности мы можем задать сетку числа перестановок $\{g_1, g_2,\ldots,g_k\}$ и получить вектор-откликов оценок энтропии Шеннона $H(g_1)$, $H(g_2),\ldots,H(g_k)$ по формуле (6). Далее следует воспользоваться данным численных экспериментов, например, через обучение нейросети связывающей шкалу энтропии перестановок и классическую шкалу энтропии Шеннона.

Энтропия Хэмминга и энтропия корреляционных связей сами по себе дают для одной бинарной последовательности только два значения показателя: $\{X(\text{«.»}), R(\text{«.»})\}$. Когнитивная метрика в тех же условиях дает возможность получить вектор показателей $\{H(g_1), H(g_2),\ldots,H(g_k)\}$ монотонно

понижающейся энтропии. Более того, опираясь на концепцию постепенного снижения уровня энтропии или повышения уровня когнетивности для сетки перестановок $\{g_1, g_2,\ldots,g_k\}$, мы можем получить вектор откликов расстояний Хэмминга $\{h(g_1), h(g_2),\ldots,h(g_k)\}$ и вектор откликов показателей корреляционной сцепленности $\{r(g_1), r(g_2),\ldots,r(g_k)\}$. Формально привлечением двух когнитивной метрики удается увеличить число анализируемых параметров в $2k$ раз. Такое повышения длины вектора учитываемых данных должно приводить к повышению точность оценки энтропии. Однако такое повышение достоверности должно присутствовать.

Видимо, снижение энтропии данных – это объективное свойство естественных нейронных сетей живых существ и всех нейросетевых приложений искусственного интеллекта. Уровень когнитивности, скорее всего, является дополнением ее противоположности – энтропии или уровня хаоса. Основное свойство нейронных сетей (естественных и искусственных), видимо, связано с их потенциальной возможностью за счет своих собственных когнитивных свойств снижать уровень хаоса (уровень энтропии «белого» шума) на фоне легко формализуемых классической математикой детерминированных компонент.

Выводы

Предложенная метрика длины когнитивного пути, видимо, должна иметь свою собственную энтропийную шкалу, не совпадающую со шкалой энтропии Шеннона. Все это следует рассматривать как удобный для практического применения частный случай некоторой упрощенной оценки сложной в вычислительном отношении задачи. По крайней мере, приведенную в статье программу можно рассматривать как еще одну систему тестов качества криптографического ключа, имеющую полиномиальную вычислительную сложность.

Список литературы

1. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Special Publication (NIST SP) / L. Bassham, A. Rukhin, J. Soto [et al.]. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762 (дата обращения: 11.09.2025).

2. Zubkov A. M., Serov A. A. Testing the NIST Statistical Test Suite on artificial pseudorandom sequences // Математические вопросы криптографии. 2019. № 10(2). С. 89–96.

3. Зубков А. М. Энтропия как характеристика качества случайных последовательностей // Математические вопросы криптографии. 2021. № 12(3). С. 31–48.

4. Иванов А. И., Чернов П. А. Протоколы биометрико-криптографического рукопожатия: защита распределенного искусственного интеллекта Интернет вещей нейросетевыми методами // Системы безопасности. 2018. № 6 (144). С. 54–59.

5. Bogdanov D. S., Mironkin V. O. Data recovering for a neural network-based biometric authentication scheme // Математические вопросы криптографии. 2019. № 10(2). С. 61–74.

6. Rane S. Standardization of Biometric Template Protection // IEEE MultiMedia. 2014. Vol. 21, N 4. P. 94–99.

7. Иванов А. И., Иванов А. П., Юнин А. П. Устранение методической погрешности оценки энтропии в пространстве расстояний Хэмминга // Защита информации. Инсайд. 2023. № 6(114). С. 55–59.

8. Feng Hao, Anderson R., Daugman J. Combining crypto with biometrics effectively // IEEE Transactions on Computers. 2006. Vol. 55, N 9. P. 1084–1088.

9. Nandakumar K., Jain A. K. Biometric Template Protection: Bridging the performance gap between theory and practice // IEEE Signal Processing Magazine. 2015. Vol. 32, is. 5. P. 88–100. https://doi.org/10.1109/MSP.2015.2427849

10. Николенко С., Кудрин А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. СПб.: Питер, 2018. 480 с.

11. Мэн Цзянь, Яо Лусин. DeepSeek на практике / перевод с китайского И. А. Шевкуна. М.: ДМК Пресс, 2025. 206 с.

12. Волчихин В. И., Иванов А. И., Иванов А. П. Алгоритмы быстрого вычисления энтропии Шеннона на малых выборках для длинных кодов с существенно зависимыми разрядами // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2024. № 4. С. 27–34. https://doi.org/10.24143/2072-9502-2024-4-27-34

13. Иванов А. И. Корреляционная энтропия как метрика абсолютного хаоса либо его противоположности в форме абсолютного порядка // Системы безопасности. 2025. № 4. С. 130–133.

14. Иванов А. И., Иванов А. П., Горбунов К. А. Нейросетевое преобразование биометрии в код аутентификации: дополнение энтропии Хэмминга энтропией корреляционных связей между разрядами // Надежность и качество сложных систем. 2023. № 1(41). С. 91–98.

15. Нейросетевой анализ малых выборок с использованием большого числа статистических критериев для проверки последовательности гипотез о значении математических ожиданий коэффициентов корреляции / А. И. Иванов, А. И. Годунов, Е. А. Малыгина, Н. А. Папуша, А. И. Ермакова // Известия высших учебных заведений. Поволжский регион. Технические науки. 2024. № 3. С. 37–46. https://doi.org/10.21685/2072-3059-2024-3-4

16. Иванов А. И. Квантовая неопределенность Гейзенберга для «средне-групповой» скорости математических молекул // Защита информации. Инсайд. 2024. № 6(120). С. 58–92.

17. Иванов А. И. Появление взаимной корреляции состояний 256 монет Бернулли при их параллельном подбрасывании горстью // Защита информации. Инсайд. 2025. № 4. С. 82–86.

18. Иванов А. И. Энтропия как оценка числа модификации кода от исходного хаоса к максимальному порядку: быстрый алгоритм приближенной оценки качества случайных последовательностей // Защита информации. Инсайд. 2024. № 4(118). С. 56–59.

References

1. Bassham L., Rukhin A., Soto J., et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Special Publication (NIST SP). Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762 (accessed 11.09.2025).

2. Zubkov A.M., Serov A.A. Testing the NIST Statistical Test Suite on artificial pseudorandom sequences. *Matematicheskie voprosy kriptografii = Mathematical Issues of Cryptography*. 2019;(10):89–96. (In Russ.)

3. Zubkov A.M. Entropy as a characteristic of the quality of random sequences. *Matematicheskie voprosy kriptografii = Mathematical Issues of Cryptography*. 2021;(12):31–48.

4. Ivanov A.I., Chernov P.A. Protocols of biometric and cryptographic handshake: protection of distributed artificial intelligence of the Internet of Things by neural network methods. *Sistemy bezopasnosti = Security Systems*. 2018;(6):54–59. (In Russ.)

5. Bogdanov D.S., Mironkin V.O. Data recovery for a neural network-based bio-metric authentication scheme. *Matematicheskie voprosy kriptografii = Mathematical Issues of Cryptography*. 2019;(10):61–74.

6. Rane S. Standardization of Biometric Template Protection. *IEEE MultiMedia*. 2014;21(4):94–99.

7. Ivanov A.I., Ivanov A.P., Yunin A.P. Elimination of methodological errors in estimating entropy in the space of Hamming distances. *Zashchita informatsii. Insaid = Information Protection. Inside*. 2023;(6):55–59. (In Russ.)

8. Feng Hao, Anderson R., Daugman J. Combining crypto with biometrics effectively. *IEEE Transactions on Computers*. 2006;55(9):1084–1088.

9. Nandakumar K., Jain A. K. Biometric Template Protection: Bridging the perfor-mance gap between theory and practice. *IEEE Signal Processing Magazine*. 2015;32:88–100. https://doi.org/10.1109/MSP.2015.2427849

10. Nikolenko S., Kudrin A., Arkhangelskaya E. Deep learning. Immersion in the world of neural networks. Saint Petersburg: Piter; 2018. 480 p. (In Russ.)

11. Meng Jian, Yao Luxing. DeepSeek in practice. Moscow: DMK Press; 2025. 206 p. (In Russ.)

12. Volchikhin V.I., Ivanov A.I., Ivanov A.P. Algorithms for fast calculation of Shannon entropy on small samples for long codes with significantly different digits. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika = Bulletin of the Astrakhan State Technical*

University. Series: Management, Computer Engineering and Computer Science. 2024:(4):27–34. (In Russ.) https://doi.org/10.24143/2072-9502-2024-4-27-34

13. Ivanov A.I. Correlation entropy as a metric of absolute chaos or its opposite in the form of absolute order. *Sistemy bezopasnosti = Security Systems*. 2025;(4):130–133. (In Russ.)

14. Ivanov A.I., Ivanov A.P., Gorbunov K.A. Neural network transformation of biometrics into an authentication code: addition of Hamming entropy by entropy of relational connections between bits. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and Quality of Complex Systems*. 2023;(1):91–98. (In Russ.)

15. Ivanov A.I., Godonov A.I., Malygina E.A., Papusha N.A., Ermakova A.I. Neural network analysis of small samples using a large number of statistical criteria to test the sequence of hypotheses about the value of mathematical expectations of correlation coefficients. *Izvestiya vysshikh uchebnykh zavedenii. Povolzhskii region. Tekhnicheskie nauki = Proceedings of Higher Educational Institutions. The Volga Region. Technical Sciences*. 2024;(3):37–46. (In Russ.) https://doi.org/10.21685/2072-3059-2024-3-4

16. Ivanov A.I. Heisenberg's quantum uncertainty for the "medium-group" velocity of mathematical molecules. *Zashchita informatsii Insaid = Information Protection. The Inside View.* 2024;(6):58–92. (In Russ.)

17. Ivanov A.I. The appearance of a mutual correlation of the states of 256 Ber-zero coins when they are tossed in parallel by a handful. *Zashchita informatsii Insaid = Information Protection. The Inside View.* 2025;(4):82–86. (In Russ.)

18. Ivanov A.I. Entropy as an estimate of the number of code modifications from initial chaos to maximum order: a fast algorithm for approximate estimation of the quality of random sequences. *Zashchita informatsii Insaid = Information Protection. The Inside View*. 2024;(4):56–59. (In Russ.)

Информация об авторе / Information about the Author

Иванов Александр Иванович,
доктор технических наук, профессор,
научный консультант, Пензенский
научно-исследовательский
электротехнический институт,
г. Пенза, Российская Федерация,
e-mail: bio.ivan.penza@mail.ru
SPIN: 2277-7744,
ORCID: 0000-0003-3475-2182,
Author ID: 744989

Alexander I. Ivanov, Doctor of Sciences
(Engineering), Professor, Scientific Consultant,
Penza Research Institute of Electrical
Engineering, Penza, Russian Federation,
e-mail: bio.ivan.penza@mail.ru,
SPIN: 2277-7744,
ORCID: 0000-0003-3475-2182,
Author ID: 744989