УДК 519.218+004.056.5 DOI 10.17223/20710410/65/4

О ВЛИЯНИИ ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ДИСКРЕТНЫХ ИСТОЧНИКОВ, ФОРМИРУЮЩИХ КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ, НА ПРАКТИЧЕСКУЮ СЕКРЕТНОСТЬ КЛЮЧА

А. С. Логачев*, В. О. Миронкин**

*Лаборатория ТВП, г. Москва, Россия

**МИРЭА — Российский технологический университет, г. Москва, Россия

E-mail: mironkin.v@mail.ru

Предложена математическая модель двоичного дискретного источника, приближенная к практическим условиям функционирования устройств генерации криптографических ключей. Модель допускает нестационарность таких устройств, а также наличие статистических зависимостей между их выходными битами. В рамках модели получена достижимая и легко вычислимая оценка снизу практической секретности ключа. Показано, что при определённых параметрах модели оценка позволяет делать содержательные выводы о криптографическом качестве ключей, в то время как другие известные оценки не справляются с этим.

Ключевые слова: *практическая секретность ключа, алгоритм опробования до успеха, усечённый алгоритм опробования.*

ON THE INFLUENCE OF PROBABILISTIC CHARACTERISTICS OF DISCRETE SOURCES FORMING CRYPTOGRAPHIC KEYS ON THE PRACTICAL SECRECY OF THE KEY

A. S. Logachev*, V. O. Mironkin**

*TVP Laboratory, Moscow, Russia

**MIREA — Russian Technological University, Moscow, Russia

The mathematical model of a binary discrete source is proposed, which is close to the practical conditions for the operation of cryptographic key generation devices. The model takes into account the non-stationarity of such devices, as well as the presence of statistical dependencies between their output bits. Within the framework of the model, an achievable and easily computable lower estimate of the practical secrecy of the key is obtained. It is shown that with certain parameters of the model, the assessment allows us to draw meaningful conclusions about the cryptographic quality of keys, while other well-known estimates do not cope with this.

Keywords: *the practical secrecy of the key, algorithm of testing to success, truncated algorithm of testing.*

Введение

В соответствии с принципом Керкгоффса [1, 2] защищённость информационных систем держится на секретности используемых в них криптографических ключей. Поэтому совершенно не удивительно, что оценка практической секретности ключа

является не только неотъемлемой составляющей анализа широкого класса алгоритмических методов защиты информации (далее — АМЗИ), в том числе имеющих квантовую природу [3], но и синтеза ряда аппаратно-программных средств, используемых для генерации случайных последовательностей [4], на основе которых формируются ключи шифрования, ключи электронной подписи, пароли, пин-коды и т. д.

Криптографический смысл практической секретности ключа, а также результаты её теоретико-вероятностного исследования достаточно полно изложены в работах [5, 6]. Публикацию И. М. Арбекова [5], без сомнения, можно считать основополагающей работой по анализу практической секретности ключа, положившей начало дальнейшим исследованиям в этой области [3, 6].

Напомним, что в соответствии с [5] для произвольных фиксированных $n \in \mathbb{N}$ и π, $0 < \pi \leqslant 1$, практическая секретность ключа $Q_n^{(\pi)}$ равна минимальному среди средних значений трудоёмкостей $R_{A_n(\tilde{\pi})}$ всех возможных усечённых алгоритмов $A_n(\tilde{\pi})$ опробования ключа из $\{0,1\}^n$ с вероятностями успеха $\tilde{\pi}$, $\tilde{\pi} \geqslant \pi$:

$$Q_n^{(\pi)} = \min_{A(\tilde{\pi})\colon\, \tilde{\pi} \geqslant \pi} \left(R_{A_n(\tilde{\pi})}\right).$$

В работе [6] указанная величина изучается в рамках математической модели, в которой ключ представляет собой реализацию дискретного источника без памяти (далее — ДИБП) [7], функционирующего в соответствии с некоторой полиномиальной схемой:

$$\mathcal{A} \sim \begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_{2^n} \\ p_1 & p_2 & \dots & p_{2^n} \end{pmatrix}, \tag{1}$$

где $\omega_i \in \{0,1\}^n$, $n \in \mathbb{N}$, $i = 1, 2, \dots, 2^n$, а компоненты вектора распределения $\overline{p} = (p_1, p_2, \dots, p_{2^n})$ удовлетворяют соотношениям

$$p_1 + p_2 + \ldots + p_{2^n} = 1 \quad \text{и} \quad 1 > p_1 \geqslant p_2 \geqslant \ldots \geqslant p_{2^n} > 0. \tag{2}$$

Для этой модели автором [6] получена следующая оценка снизу практической секретности ключа:

$$Q_n^{(\pi)}(\delta) \geqslant \left(1 - \frac{2\delta}{\pi}\right) \frac{2^n\,(1 - 8\delta) + 1}{2}, \tag{3}$$

где $\delta = \dfrac{1}{2} \displaystyle\sum_{j=1}^{2^n} |p_j - 2^{-n}|$ — расстояние по вариации между распределениями $(p_1, p_2, \dots, p_{2^n})$ и $(2^{-n}, 2^{-n}, \dots, 2^{-n})$.

Замечание 1. Оценка (3) получена для алгоритма оптимального опробования ключей, заключающегося в переборе элементов ключевого множества в порядке невозрастания их вероятностей (2), начиная с наиболее вероятного. При произвольном фиксированном распределении (1) такой алгоритм, очевидно, минимизирует среднюю трудоёмкость опробования.

Отметим один из недостатков оценки (3) — для её вычисления необходимо суммирование 2^n достаточно малых слагаемых, что требует существенных вычислительных мощностей, а также высокой точности расчётов. Кроме того, в соответствии с [6] оценка (3) является содержательной лишь при справедливости неравенства

$$\delta < \min\left(1/8, \pi/2\right). \tag{4}$$

Формула (3) активно используется на практике. В частности, в классических условиях анализа АМЗИ [6, с. 32], когда элементы ключевого множества имеют равновероятное распределение

$$p_1 = p_2 = \ldots = p_{2^n} = 2^{-n} \tag{5}$$

и, как следствие, $\delta = 0$, выполняется известное равенство [5, с. 46]

$$Q_n^{(1)}(0) = (2^n + 1)/2.$$

Таким образом, в «рафинированных» условиях, соответствующих (5), оценка (3) практической секретности ключа является достижимой и её использование в связи с этим не вызывает никаких сомнений. Вместе с тем при синтезе АМЗИ могут возникать достаточно естественные вопросы: возможно ли на практике обеспечить выполнение модельных предположений вида (1), характерных лишь для стационарных источников [7]? И если их нельзя обеспечить, то что использовать в качестве аналога оценки (3)? Или никакие аналоги не требуются и её использование является допустимым?

Отвечая на первый вопрос, к сожалению, мы получим отрицательный ответ. Действительно, в общем случае учесть влияние всех возможных внешних факторов на процесс формирования криптографических ключей некоторым, вообще говоря, физическим источником достаточно проблематично. Кроме того, сама элементная база реального источника подвержена естественной деградации, влияющей на вероятностные свойства и характеристики формируемых последовательностей.

В таком случае становятся актуальными пока ещё открытые второй и третий вопросы, которые мы рассмотрим в рамках настоящей работы, попутно предлагая некоторые способы построения оценки снизу практической секретности ключа в более общих модельных предположениях, характерных для практики.

Исследование будем проводить в три этапа. На первом этапе построим оценку снизу для средней трудоёмкости алгоритма опробования ключа до успеха, на втором этапе — оценку снизу для средней трудоёмкости процедуры опробования ключа на основе усечённых алгоритмов с некоторыми фиксированными вероятностями успеха и, наконец, на третьем — искомую оценку для практической секретности ключа.

Для решения указанных задач построим теоретико-вероятностную модель источника формирования криптографических ключей.

1. Модель источника формирования криптографических ключей

Рассмотрим невырожденный двоичный дискретный источник — вероятностное пространство $(\{0,1\}^\infty, \mathcal{F}, \Pr)$, где $\mathcal{F}$ — наименьшая по включению σ-алгебра на $\{0,1\}^\infty$, содержащая все цилиндрические множества [7] общего вида, а вероятность $\Pr$ такова, что для её конечномерных распределений $P_{t_1,t_2,\ldots,t_k}$, $1 \leqslant t_1 < t_2 < \ldots < t_k$, $k = 1, 2, \ldots$, выполняется соотношение

$$\left(\frac{1}{2} - \varepsilon\right)^k \leqslant P_{t_1,t_2,\ldots,t_k}(x_1, x_2, \ldots, x_k) \leqslant \left(\frac{1}{2} + \varepsilon\right)^k \tag{6}$$

для произвольных $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$, где $0 \leqslant \varepsilon \leqslant 1/2$.

Здесь последовательность элементов $t_1, t_2, \ldots, t_k$ определяет моменты времени формирования источником $(\{0,1\}^\infty, \mathcal{F}, \Pr)$ значений $x_1, x_2, \ldots, x_k$, в нашем случае представляющих биты ключа.

Замечание 2. Ограничение вида (6) на вероятностные свойства источника является достаточно слабым по сравнению с (1), допускающим, в частности, его нестационарность или даже зависимость формируемых им битов ключа. Более того, при $\varepsilon \to 1/2$ это ограничение в принципе вырождается.

Подобная математическая модель источника использовалась в [8] при обосновании качества криптографических преобразований.

В частном случае, когда $\varepsilon = 0$, неравенство (6) принимает вид

$$2^{-k} \leqslant P_{t_1,t_2\ldots,t_k}(x_1, x_2, \ldots, x_k) \leqslant 2^{-k},$$

что при $k = n$ соответствует ДИБП с распределением (5).

Итак, мы построили модель дискретного источника формирования криптографических ключей. В рамках этой модели перейдём к оценке средней трудоёмкости алгоритма опробования ключа до успеха.

2. Оценка снизу средней трудоёмкости алгоритма опробования ключа до успеха

Согласно (6), для произвольного фиксированного ε, $0 \leqslant \varepsilon \leqslant 1/2$, уместно говорить о формировании ключей из $\{0,1\}^n$ в соответствии с полиномиальной схемой, зависящей от вектора $\bar{t} = (t_1, t_2, \ldots, t_n)$:

$$\mathcal{A}_\varepsilon(\bar{t}) \sim \begin{pmatrix} \omega_1 & \omega_2 & \ldots & \omega_{2^n} \\ p_1(\bar{t}) & p_2(\bar{t}) & \ldots & p_{2^n}(\bar{t}) \end{pmatrix}, \tag{7}$$

где $\omega_i \in \{0,1\}^n$, $i = 1, 2, \ldots, 2^n$, а компоненты вектора распределения $\overline{p}(\bar{t}) = \big(p_1(\bar{t}), p_2(\bar{t}), \ldots, p_{2^n}(\bar{t})\big)$ удовлетворяют системе соотношений

$$\begin{cases} p_1(\bar{t}) + p_2(\bar{t}) + \ldots + p_{2^n}(\bar{t}) = 1, \\ 1 > p_1(\bar{t}) \geqslant p_2(\bar{t}) \geqslant \ldots \geqslant p_{2^n}(\bar{t}) > 0, \\ (1/2 - \varepsilon)^n \leqslant p_j(\bar{t}) \leqslant (1/2 + \varepsilon)^n, \ j = 1, 2, \ldots, 2^n. \end{cases} \tag{8}$$

Общая теория [5] позволяет выписать формулу для средней трудоёмкости $\mathbf{E}T_{\mathcal{A}_\varepsilon(\bar{t})}$ алгоритма опробования ключа, сформированного источником в соответствии с вероятностной схемой $\mathcal{A}_\varepsilon(\bar{t})$, до успеха:

$$\mathbf{E}T_{\mathcal{A}_\varepsilon(\bar{t})} = \sum_{j=1}^{2^n} j p_j(\bar{t}). \tag{9}$$

Для произвольных $n \in \mathbb{N}$ и ε, $0 \leqslant \varepsilon \leqslant 1/2$, введём обозначение

$$T_n^{(1)}(\varepsilon) = \min_{\bar{t}} \left(\min_{p_1(\bar{t}),\ldots,p_{2^n}(\bar{t})} \big(\mathbf{E}T_{\mathcal{A}_\varepsilon(\bar{t})}\big) \right),$$

где $\bar{t} = (t_1, t_2, \ldots, t_n)$, $1 \leqslant t_1 < t_2 < \ldots < t_n$, а $\big(p_1(\bar{t}), p_2(\bar{t}), \ldots, p_{2^n}(\bar{t})\big)$ — векторы, удовлетворяющие (8).

Кроме того, через $[z]$ обозначим наибольшее целое число, меньшее или равное z. Тогда имеет место

Утверждение 1. Для произвольных $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$, справедливо равенство

$$T_n^{(1)}(\varepsilon) = s + 1 + \frac{(2^n - s - 1)(2^n - s)}{2}\left(\frac{1}{2} - \varepsilon\right)^n - \frac{s(s+1)}{2}\left(\frac{1}{2} + \varepsilon\right)^n, \qquad (10)$$

где $s = \left[2^n \dfrac{1 - (1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n}\right]$. При этом для $\varepsilon \in \{0, 1/2\}$

$$T_n^{(1)}(0) = (2^n + 1)/2, \quad T_n^{(1)}(1/2) = 1. \qquad (11)$$

Доказательство. Равенства в (11) очевидны. Перейдём к обоснованию соотношения (10). Зафиксировав произвольные ε, $0 < \varepsilon < 1/2$, и $\bar{t} = (t_1, t_2, \ldots, t_n)$, $1 \leqslant t_1 < t_2 < \ldots < t_n$, построим вероятностную схему

$$\hat{\mathcal{A}}_\varepsilon(\bar{t}) \sim \begin{pmatrix} \omega_1 & \omega_2 & \ldots & \omega_{2^n} \\ \hat{p}_1(\bar{t}) & \hat{p}_2(\bar{t}) & \ldots & \hat{p}_{2^n}(\bar{t}) \end{pmatrix}, \qquad (12)$$

минимизирующую величину (9). Очевидно, что количество значений $\hat{\mathcal{A}}_\varepsilon(\bar{t})$, имеющих максимальную вероятность $(1/2 + \varepsilon)^n$, совпадает с наибольшим натуральным $s < 2^n$, удовлетворяющим неравенству

$$s\,(1/2 + \varepsilon)^n + (2^n - s)\,(1/2 - \varepsilon)^n \leqslant 1, \qquad (13)$$

т. е. с величиной

$$s = \left[\frac{1 - 2^n\,(1/2 - \varepsilon)^n}{(1/2 + \varepsilon)^n - (1/2 - \varepsilon)^n}\right] = \left[2^n \frac{1 - (1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n}\right].$$

Таким образом,

$$\hat{p}_1(\bar{t}) = \ldots = \hat{p}_s(\bar{t}) = (1/2 + \varepsilon)^n. \qquad (14)$$

В свою очередь, количество значений $\hat{\mathcal{A}}_\varepsilon(\bar{t})$, имеющих минимальную вероятность $(1/2 - \varepsilon)^n$, больше либо равно $2^n - s - 1$. При этом

$$\hat{p}_{s+2}(\bar{t}) = \ldots = \hat{p}_{2^n}(\bar{t}) = (1/2 - \varepsilon)^n. \qquad (15)$$

Наконец, с учётом (13)

$$\hat{p}_{s+1}(\bar{t}) = 1 - \sum_{j=1}^{s} \hat{p}_i(\bar{t}) - \sum_{j=s+2}^{2^n} \hat{p}_i = 1 - s\,(1/2 + \varepsilon)^n - (2^n - s - 1)\,(1/2 - \varepsilon)^n \geqslant 0. \qquad (16)$$

По построению все значения $\hat{p}_1(\bar{t}), \ldots, \hat{p}_{2^n}(\bar{t})$ удовлетворяют (8). Для $j = 1, \ldots, s$, $s + 2, \ldots, 2^n$ это очевидный факт. Остаётся убедиться в справедливости неравенства $(1/2 - \varepsilon)^n \leqslant \hat{p}_{s+1}(\bar{t}) \leqslant (1/2 + \varepsilon)^n$. Действительно, в соответствии с определением величины s выполняются следующие цепочки соотношений:

$$\begin{gathered} \hat{p}_{s+1}(\bar{t}) = 1 - s(1/2 + \varepsilon)^n - (2^n - s)\,(1/2 - \varepsilon)^n + (1/2 - \varepsilon)^n \geqslant \\ \geqslant 1 - 1 + (1/2 - \varepsilon)^n = (1/2 - \varepsilon)^n, \\ \hat{p}_{s+1}(\bar{t}) = 1 - (s+1)(1/2 + \varepsilon)^n - (2^n - s - 1)\,(1/2 - \varepsilon)^n + (1/2 + \varepsilon)^n < \\ < 1 - 1 + (1/2 + \varepsilon)^n = (1/2 + \varepsilon)^n. \end{gathered}$$

Итак, распределение вероятностной схемы (12), удовлетворяющее (14)–(16), минимизирует (9). Таким образом,

$$\min_{p_1(\bar{t}),\ldots,p_{2^n}(\bar{t})} \left(\mathbf{E}T_{\mathcal{A}_\varepsilon(\bar{t})}\right) = \mathbf{E}T_{\hat{\mathcal{A}}_\varepsilon(\bar{t})} = \sum_{j=1}^{2^n} j\hat{p}_j(\bar{t}) = \sum_{j=1}^{s} i\hat{p}_j(\bar{t}) + (s+1)\hat{p}_{s+1}(\bar{t}) + \sum_{j=s+2}^{2^n} j\hat{p}_j(\bar{t}) =$$

$$= \sum_{j=1}^{s} j(1/2+\varepsilon)^n + (s+1)(1 - s(1/2+\varepsilon)^n - (2^n - s - 1)(1/2-\varepsilon)^n) + \sum_{j=s+2}^{2^n} j(1/2-\varepsilon)^n =$$

$$= s + 1 + \frac{(2^n - s - 1)\,(2^n - s)}{2}\left(\frac{1}{2} - \varepsilon\right)^n - \frac{s(s+1)}{2}\left(\frac{1}{2} + \varepsilon\right)^n.$$

Полученное выражение не зависит от $\bar{t}$ и поэтому представляет собой искомый результат (10). ■

Для $0 < \varepsilon < 1/2$ оценка (10) является достижимой, имеет достаточно простой аналитический вид и эффективно вычислима при больших значениях $n \in \mathbb{N}$. В качестве примера приведём значения величин $Q_n^{(1)}(\delta)$ и $T_n^{(1)}(\varepsilon)$, рассчитанные с использованием формул (3) и (10) для наиболее часто применяемых на практике значений $n \in \mathbb{N}$ с указанием соответствующих АМЗИ (табл. 1).

Таблица 1

Оценка	ε						
	10^{-4}	$5\cdot10^{-4}$	10^{-3}	$5\cdot10^{-3}$	10^{-2}	$5\cdot10^{-2}$	10^{-1}
$n = 56$ (DES)							
$Q_n^{(1)}(0)$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$
$T_n^{(1)}(\varepsilon)$	$3{,}58\cdot10^{16}$	$3{,}50\cdot10^{16}$	$3{,}40\cdot10^{16}$	$2{,}62\cdot10^{16}$	$1{,}78\cdot10^{16}$	$2{,}71\cdot10^{14}$	$1{,}46\cdot10^{12}$
$Q_n^{(1)}(\delta)$	$3{,}40\cdot10^{16}$	$2{,}64\cdot10^{16}$	$1{,}77\cdot10^{16}$	–	–	–	–
$n = 112$ (3DES)							
$Q_n^{(1)}(0)$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$
$T_n^{(1)}(\varepsilon)$	$2{,}57\cdot10^{33}$	$2{,}45\cdot10^{33}$	$2{,}31\cdot10^{33}$	$1{,}28\cdot10^{33}$	$5{,}00\cdot10^{32}$	$7{,}95\cdot10^{28}$	$3{,}55\cdot10^{24}$
$Q_n^{(1)}(\delta)$	$2{,}31\cdot10^{33}$	$1{,}27\cdot10^{33}$	$2{,}17\cdot10^{32}$	–	–	–	–
$n = 128$ (AES, DEAL, KASUMI, Present, SEED, Speck)							
$Q_n^{(1)}(0)$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$
$T_n^{(1)}(\varepsilon)$	$1{,}68\cdot10^{38}$	$1{,}59\cdot10^{38}$	$1{,}48\cdot10^{38}$	$7{,}40\cdot10^{37}$	$2{,}44\cdot10^{37}$	$1{,}10\cdot10^{33}$	$1{,}25\cdot10^{28}$
$Q_n^{(1)}(\delta)$	$1{,}49\cdot10^{38}$	$7{,}25\cdot10^{37}$	–	–	–	–	–
$n = 160$ (SEAL)							
$Q_n^{(1)}(0)$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$
$T_n^{(1)}(\varepsilon)$	$7{,}19\cdot10^{47}$	$6{,}72\cdot10^{47}$	$6{,}15\cdot10^{47}$	$2{,}46\cdot10^{47}$	$5{,}72\cdot10^{46}$	$2{,}10\cdot10^{41}$	$1{,}57\cdot10^{35}$
$Q_n^{(1)}(\delta)$	$6{,}17\cdot10^{47}$	$2{,}22\cdot10^{47}$	–	–	–	–	–
$n = 168$ (3DES)							
$Q_n^{(1)}(0)$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$
$T_n^{(1)}(\varepsilon)$	$1{,}84\cdot10^{50}$	$1{,}71\cdot10^{50}$	$1{,}56\cdot10^{50}$	$5{,}88\cdot10^{49}$	$1{,}26\cdot10^{49}$	$2{,}46\cdot10^{43}$	$9{,}33\cdot10^{36}$
$Q_n^{(1)}(\delta)$	$1{,}56\cdot10^{50}$	$5{,}13\cdot10^{49}$	–	–	–	–	–
$n = 192$ (AES, DEAL, Speck)							
$Q_n^{(1)}(0)$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$
$T_n^{(1)}(\varepsilon)$	$3{,}08\cdot10^{57}$	$2{,}84\cdot10^{57}$	$2{,}54\cdot10^{57}$	$8{,}03\cdot10^{56}$	$1{,}32\cdot10^{56}$	$4{,}06\cdot10^{49}$	$1{,}97\cdot10^{42}$
$Q_n^{(1)}(\delta)$	$2{,}55\cdot10^{57}$	$5{,}95\cdot10^{56}$	–	–	–	–	–
$n = 256$ («Кузнечик», «Магма», AES, DEAL, Speck, Threefish)							
$Q_n^{(1)}(0)$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$
$T_n^{(1)}(\varepsilon)$	$5{,}64\cdot10^{76}$	$5{,}05\cdot10^{76}$	$4{,}34\cdot10^{76}$	$8{,}31\cdot10^{75}$	$6{,}88\cdot10^{74}$	$1{,}58\cdot10^{66}$	$3{,}11\cdot10^{56}$
$Q_n^{(1)}(\delta)$	$4{,}37\cdot10^{76}$	–	–	–	–	–	–

Из табл. 1 видно, что результат утверждения 1 позволяет точнее оценить среднюю трудоёмкость опробования ключа до успеха по сравнению с формулой (3). Вместе с этим при малых значениях ε (например, меньших 10^{-4}) разность значений оценок $T_n^{(1)}(\varepsilon)$ и $Q_n^{(1)}(\delta)$ не столь велика и использование оценки (3), вообще говоря, допустимо. А вот в области больших отклонений ($\varepsilon \geqslant 5 \cdot 10^{-3}$) формула (3) в принципе не работает (в табл. 1 этот факт отмечен символом «–»).

Нетрудно понять, что причиной отсутствия данных в ячейках табл. 1, соответствующих значениям величины $Q_n^{(1)}(\delta)$, является невыполнение условия (4) для соответствующих значений параметров n и ε. Разберемся подробнее с этим вопросом.

Сначала определим область значений ε из (8), для которых возможно использование оценки (3) при фиксированном $n \in \mathbb{N}$.

Утверждение 2. Для любого $n \in \mathbb{N}$ и вероятностной схемы (12) оценка (3) корректна при выполнении неравенства

$$0 \leqslant \varepsilon < \frac{1}{2}\left(\sqrt[n]{1+\frac{1}{4+2^{3-n}}}-1\right). \tag{17}$$

Доказательство. Очевидно, для $\varepsilon = 0$ оценка (3) корректна. Зафиксируем произвольные значения $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$. Тогда для для расстояния по вариации δ между распределениями $\left(\hat{p}_1(\bar{t}), \ldots, \hat{p}_{2^n}(\bar{t})\right)$ и $(2^{-n}, \ldots, 2^{-n})$ справедливо равенство

$$\begin{gathered}\delta = \frac{1}{2}\sum_{j=1}^{2^n}\left|\hat{p}_j(\bar{t})-\frac{1}{2^n}\right| = \frac{s}{2}\left(\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right)+\\ +\frac{1}{2}\left|1-s\left(\frac{1}{2}+\varepsilon\right)^n-(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n-\frac{1}{2^n}\right|+\\ +\frac{(2^n-s-1)}{2}\left(\frac{1}{2^n}-\left(\frac{1}{2}-\varepsilon\right)^n\right).\end{gathered} \tag{18}$$

Используя вытекающее из (13) соотношение

$$(s+1)\,(1/2+\varepsilon)^n + (2^n-s-1)\,(1/2-\varepsilon)^n > 1,$$

оценим сверху второе слагаемое в правой части (18):

$$\begin{gathered}\frac{1}{2}\left|1-s\left(\frac{1}{2}+\varepsilon\right)^n-(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n-\frac{1}{2^n}\right| =\\ =\frac{1}{2}\left|1-(s+1)\left(\frac{1}{2}+\varepsilon\right)^n-(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n+\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right| \leqslant\\ \leqslant\frac{1}{2}\left|1-(s+1)\left(\frac{1}{2}+\varepsilon\right)^n-(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n\right|+\frac{1}{2}\left|\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right| =\\ =\frac{1}{2}\left((s+1)\left(\frac{1}{2}+\varepsilon\right)^n+(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n-1\right)+\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^{n+1}}.\end{gathered} \tag{19}$$

Подставив (19) в (18), получим следующую оценку для δ:

$$\delta \leqslant (s+1)\left((1/2+\varepsilon)^n - 2^{-n}\right).$$

В свою очередь, из (4) следует, что выполнение неравенства

$$\begin{gathered}(s+\omega+1)\left(\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right)= \\ =\left(2^n\frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}+1\right)\left(\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right)<\frac{1}{8},\end{gathered} \tag{20}$$

где $\omega=\left(2^n\dfrac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}-s\right)$ — дробная часть числа $2^n\dfrac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}$, является достаточным условием корректного использования оценки (3).

Рассмотрим (20) подробнее. Используя справедливое при $-1<x<1$, $k\in\mathbb{N}$ неравенство

$$1-kx\leqslant(1-x)^k,$$

обращающееся в равенство при $x=0$, а также разложение

$$(1+2\varepsilon)^n-(1-2\varepsilon)^n=2\sum_{k=1}^{]n/2[}\mathrm{C}_n^{2k-1}(2\varepsilon)^{2k-1}, \tag{21}$$

где $]z[$ — наименьшее целое число, большее или равное z, выпишем вспомогательное соотношение

$$\frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}<\frac{1-1+2n\varepsilon}{4n\varepsilon}=\frac{1}{2},$$

позволяющее записать достаточное условие выполнения (20):

$$\left(2^{n-1}+1\right)\left(\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right)<\frac{1}{8}\ \Leftrightarrow\ \varepsilon<\frac{1}{2}\left(\sqrt[n]{1+\frac{1}{4+2^{3-n}}}-1\right). \tag{22}$$

Утверждение доказано. ■

На рис. 1 представлена зависимость размера определённой в (17) области допустимых для корректного использования оценки (3) значений ε от величины $n\in\mathbb{N}$.

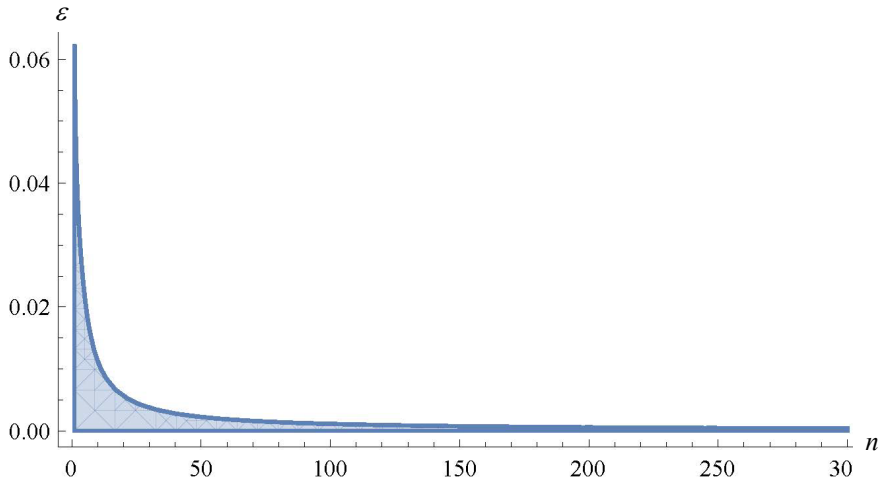

Рис. 1. Область значений ε, удовлетворяющих (17)

В табл. 2 приведены значения правых границ интервалов допустимых значений ε, рассчитанных для указанных в табл. 1 значений $n\in\mathbb{N}$.

Таблица 2

n	56	112	128	160	168	192	256
Макс. знач. ε	$2{,}00 \cdot 10^{-3}$	$9{,}97 \cdot 10^{-4}$	$8{,}72 \cdot 10^{-4}$	$6{,}98 \cdot 10^{-4}$	$6{,}65 \cdot 10^{-4}$	$5{,}81 \cdot 10^{-4}$	$4{,}36 \cdot 10^{-4}$

Замечание 3. Данные табл. 2 в достаточной мере соответствуют информации, приведённой в табл. 1. При необходимости интервал (17) допустимых значений ε может быть скорректирован за счёт более точного оценивания в (21).

Перейдём теперь к оценке длины криптографического ключа, для которой возможно использование оценки (3) при фиксированном значении ε, $0 < \varepsilon < 1/2$.

Утверждение 3. Для любого ε, $0 < \varepsilon < 5/16$, и вероятностной схемы (12) оценка (3) корректна при выполнении неравенства

$$1 \leqslant n < \log_{1+2\varepsilon}(5/4 - 4\varepsilon). \tag{23}$$

Доказательство. Рассмотрим левую часть первого из неравенств (22). Используя разложения [9]

$$(1+2\varepsilon)^n = \sum_{k=0}^{n} \mathrm{C}_n^k (2\varepsilon)^k, \quad \sum_{k=0}^{n} \mathrm{C}_n^k = 2^n$$

и учитывая, что $\varepsilon < 1/2$, выпишем цепочку соотношений

$$\begin{gathered}\left(2^{n-1}+1\right)\left(\left(\frac{1}{2}+\varepsilon\right)^n - \frac{1}{2^n}\right) = \frac{(1+2\varepsilon)^n - 1}{2} + \frac{(1+2\varepsilon)^n - 1}{2^n} = \\ = \frac{(1+2\varepsilon)^n - 1}{2} + \frac{1}{2^n}\left(2\varepsilon C_n^1 + C_n^2 (2\varepsilon)^2 + \ldots + C_n^n (2\varepsilon)^n\right) = \frac{(1+2\varepsilon)^n - 1}{2} + \\ + \frac{\varepsilon}{2^{n-1}}\left(C_n^1 + 2\varepsilon C_n^2 + \ldots + C_n^n (2\varepsilon)^{n-1}\right) < \frac{(1+2\varepsilon)^n - 1}{2} + \\ + \frac{\varepsilon}{2^{n-1}}\left(C_n^1 + C_n^2 + \ldots + C_n^n\right) < \frac{(1+2\varepsilon)^n - 1}{2} + 2\varepsilon,\end{gathered} \tag{24}$$

позволяющую записать достаточное условие выполнения (3):

$$\left((1+2\varepsilon)^n - 1\right)/2 + 2\varepsilon < 1/8 \;\Leftrightarrow\; n < \log_{1+2\varepsilon}(5/4 - 4\varepsilon).$$

Здесь $0 < \varepsilon < 5/16$. ■

На рис. 2 в логарифмической шкале представлена зависимость размера определённой в (23) области допустимых для корректного использования оценки (3) значений n от величины ε, $0 < \varepsilon < 5/16$.

Для значений ε, указанных в табл. 1, приведём результаты оценки правых границ интервалов допустимых значений n (табл. 3).

Таблица 3

ε	10^{-4}	$5 \cdot 10^{-4}$	10^{-3}	$5 \cdot 10^{-3}$	10^{-2}	$5 \cdot 10^{-2}$	10^{-1}
Макс. знач. n	1114	221	110	20	9	–	–

Замечание 4. Данные табл. 3 в целом соответствуют информации, приведённой в табл. 1. При необходимости интервал (23) может быть скорректирован за счёт более точного оценивания в (24).

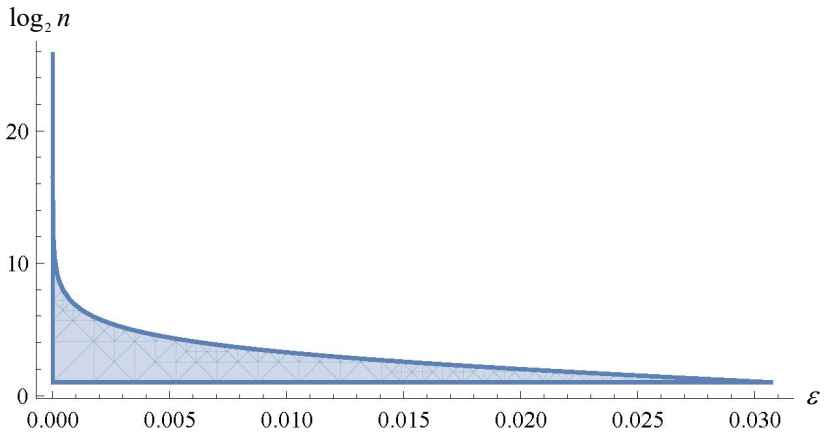

Рис. 2. Область значений n, удовлетворяющих (23)

Результаты утверждений 2 и 3 позволяют оценить связь параметров δ и n, ε, а также описывают ограничения, возникающие при использовании оценки (3) в случаях больших отклонений вероятностных характеристик источников формирования криптографических ключей от «идеальных».

Далее от модели применения одного алгоритма опробования, достоверно приводящего к успеху, перейдём к модели последовательного применения алгоритмов, завершающихся успехом с некоторыми фиксированными вероятностями, не меньшими π, где $0 < \pi \leqslant 1$.

3. Оценка снизу средней трудоёмкости процедуры опробования ключа на основе усечённых алгоритмов

В соответствии с [5] для определения истинного ключа в общем случае используется последовательность разнесённых по времени выполнения усечённых алгоритмов опробования, имеющих некоторые фиксированные вероятности успеха, не меньшие π, $0 < \pi \leqslant 1$. Так, в случае $\pi = 1$ указанная последовательность состоит из одного алгоритма опробования до успеха и, как следствие, средняя трудоёмкость такой процедуры опробования ключа совпадает со средней трудоёмкостью этого алгоритма. Её мы оценили в п. 2. Перейдём к рассмотрению случая $0 < \pi < 1$.

Согласно [5, 6, 10], для каждого такого усечённого алгоритма «успехом» считается событие, состоящее в определении истинного ключа (каждый раз нового, выбираемого в соответствии с распределением (1)). При этом в [5] для вычисления средней трудоёмкости процедуры определения ключа, заключающейся в последовательном применении усечённых алгоритмов опробования, используется модель независимых испытаний с фиксированной вероятностью успеха π. Число таких испытаний представляет собой случайную величину τ, имеющую геометрическое распределение с параметром π (далее будем обозначать $\tau \sim \mathrm{Geom}(\pi)$).

Замечание 5. Как и в п. 2, мы откажемся от жёстких условий стационарности источника и независимости битов формируемых им ключей, позволяющих применять для анализа классическую модель независимых испытаний.

Для источника, функционирующего в соответствии с вероятностной схемой (7), через ξ_i, $i = 1, 2, \ldots$, обозначим случайную величину, равную трудоёмкости определения истинного ключа при применении i-го усечённого алгоритма.

В силу возможной зависимости битов ключей, формируемых источником (6), в общем случае величины $\xi_1, \xi_2, \ldots$ являются зависимыми.

Для произвольного $i = 1, 2, \ldots$ через $\overline{p}_i(\bar{t}_i)$ обозначим распределение вероятностной схемы (7) в момент применения i-го усечённого алгоритма:

$$\overline{p}_i(\bar{t}_i) = \left(p_1(\bar{t}_i), p_2(\bar{t}_i), \ldots, p_{2^n}(\bar{t}_i)\right).$$

Здесь $\bar{t}_i = \left(t_1^{(i)}, t_2^{(i)}, \ldots, t_n^{(i)}\right)$ — вектор соответствующих моментов времени формирования битов ключа. Отметим, что для источника, не являющегося в общем случае стационарным, $\overline{p}_i(\bar{t}_i) \neq \overline{p}_j(\overline{t_j})$ и, как следствие, $\mathbf{E}\xi_i \neq \mathbf{E}\xi_j$, $i, j \geqslant 1$, $i \neq j$.

Для произвольного $i = 1, 2, \ldots$ и $k \in \{1, 2, \ldots, 2^n\}$ положим

$$\pi_k^{(i)} = \sum_{j=1}^{k} p_j(\bar{t}_i).$$

Тогда по формуле полной вероятности для отдельно взятого i-го усечённого алгоритма

$$\mathbf{E}\xi_i = \left(1 - \pi_{l_i}^{(i)}\right) l_i + \sum_{j=1}^{l_i} j p_j(\bar{t}_i), \tag{25}$$

где $l_i = \min\left\{k \in \{1, 2, \ldots, 2^n\} \colon \pi_k^{(i)} \geqslant \pi\right\}$.

Замечание 6. Поскольку в общем случае $\pi_{l_i}^{(i)} \neq \pi$, то фактически i-й усечённый алгоритм имеет вероятность успеха $\pi_{l_i}^{(i)} \geqslant \pi$.

Наконец, через τ обозначим случайную величину, равную порядковому номеру усечённого алгоритма опробования, при применении которого определяется истинный ключ.

С учётом изложенного, трудоёмкость процедуры определения ключа, сформированного в соответствии с (7), заключающейся в последовательном применении усечённых алгоритмов опробования с вероятностями успеха не меньшими π, представляется в следующем виде:

$$T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1), \ldots, \mathcal{A}_\varepsilon(\overline{t_\tau})} = \sum_{i=1}^{\tau} \xi_i.$$

Для произвольных параметров $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$, вероятностной схемы (7), а также для произвольного π, $0 < \pi \leqslant 1$, введём обозначение

$$T_n^{(\pi)}(\varepsilon) = \min_{\bar{t}_1, \ldots, \bar{t}_\tau} \left(\min_{\substack{p_1(\bar{t}_1), \ldots, p_{2^n}(\bar{t}_1) \\ \cdots \\ p_1(\bar{t}_\tau), \ldots, p_{2^n}(\bar{t}_\tau)}} \left(\mathbf{E} T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1), \ldots, \mathcal{A}_\varepsilon(\bar{t}_\tau)} \right) \right),$$

где $1 \leqslant t_1^{(i)} < t_2^{(i)} < \ldots < t_n^{(i)}$; $\left(p_1(\bar{t}_i), p_2(\bar{t}_i), \ldots, p_{2^n}(\bar{t}_i)\right)$ — векторы, удовлетворяющие (8), $i = 1, \ldots, \tau$. Тогда справедливо

Утверждение 4. Для произвольных $n \in \mathbb{N}$, ε, $0 < \varepsilon < 1/2$, и π, $0 < \pi \leqslant 1$, справедливы следующие равенства:

— если $0 < \pi \leqslant s\,(1/2 + \varepsilon)^n$, то

$$T_n^{(\pi)}(\varepsilon) = \frac{2^n}{(1+2\varepsilon)^n} - \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[+ \frac{(1+2\varepsilon)^n}{2^{n+1}} \left(\left(\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right)^2 + \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right); \tag{26}$$

— если $s(1/2+\varepsilon)^n < \pi \leqslant 1-(2^n-s-1)\,(1/2-\varepsilon)^n$, то

$$T_n^{(\pi)}(\varepsilon) = \frac{2^n(s+1)}{2^n-(2^n-s-1)\,(1-2\varepsilon)^n} - \\ -(s+1)\left(\frac{s}{2}\,(1/2+\varepsilon)^n + (2^n-s-1)\,(1/2-\varepsilon)^n\right); \tag{27}$$

— если $1-(2^n-s-1)\,(1/2-\varepsilon)^n < \pi \leqslant 1$, то

$$T_n^{(\pi)}(\varepsilon) = \left(\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right)\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right](1-2\varepsilon)^n\right) \Big/ \left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right](1-2\varepsilon)^n\right) + \\ +s+1-\frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n + \\ +\frac{1}{2}\left(2^{2n}-2^{n+1}s-2^n+\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]-2^{n+1}-1\right)+s^2+s\right)(1/2-\varepsilon)^n, \tag{28}$$

где $s = \left[2^n \dfrac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}\right]$. При этом для $\varepsilon \in \{0, 1/2\}$

$$T_n^{(\pi)}(0) = 2^n -]2^n\pi[+ \frac{(]2^n\pi[)^2 +]2^n\pi[}{2^{n+1}}, \quad T_n^{(\pi)}(1/2) = 1. \tag{29}$$

Доказательство. Зафиксируем произвольное значение π, $0 < \pi \leqslant 1$. Тогда по определению условного математического ожидания [11, с. 54]

$$\mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)} = \mathbf{E}\sum_{i=1}^{\tau}\xi_i = \sum_{j=1}^{\infty}\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau=j\right)\Pr\{\tau=j\},$$

где $\Pr\{\tau=j\} = \pi_{l_j}^{(j)}\prod\limits_{i=1}^{j-1}\left(1-\pi_{l_i}^{(i)}\right)$. При этом по построению процедуры опробования, а также с учётом соотношения (25)

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau=j\right) = \sum_{i=1}^{j-1}l_i + \sum_{i=1}^{l_j} i p_i(\bar{t}_j). \tag{30}$$

Выпишем (30) для минимизирующей его вероятностной схемы (12) с распределением (14)–(16). Рассмотрим сначала два граничных случая: $\varepsilon \in \{0, 1/2\}$.

Пусть $\varepsilon = 0$. Тогда для $i = 1, \ldots, j$ справедливы равенства $l_i =]2^n\pi[$ и $\pi_{l_i}^{(i)} = l_i/2^n$. Таким образом, (30) принимает следующий вид:

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau=j\right) = (j-1)\,]2^n\pi[+ \frac{1}{2^n}\sum_{i=1}^{]2^n\pi[} i = (j-1)\,]2^n\pi[+ \frac{]2^n\pi[+1}{2^{n+1}}\,]2^n\pi[.$$

При этом $\Pr\{\tau=j\} = \dfrac{]2^n\pi[}{2^n}\left(1-\dfrac{]2^n\pi[}{2^n}\right)^{j-1}$, т. е. $\tau \sim \mathrm{Geom}\left(\dfrac{]2^n\pi[}{2^n}\right)$. Тогда

$$\mathbf{E}\tau = \frac{2^n}{]2^n\pi[} \quad \text{и} \quad \mathbf{E}T^{(\pi)}_{\mathcal{A}_0(\bar{t}_1),\ldots,\mathcal{A}_0(\bar{t}_\tau)} =]2^n\pi[\underbrace{\sum_{j=1}^{\infty}(j-1)\frac{]2^n\pi[}{2^n}\left(1-\frac{]2^n\pi[}{2^n}\right)^{j-1}}_{\mathbf{E}(\tau-1)} + \\ +\frac{]2^n\pi[+1}{2^{n+1}}\,]2^n\pi[\underbrace{\sum_{j=1}^{\infty}\frac{]2^n\pi[}{2^n}\left(1-\frac{]2^n\pi[}{2^n}\right)^{j-1}}_{1} = 2^n -]2^n\pi[+ \frac{(]2^n\pi[)^2+]2^n\pi[}{2^{n+1}}.$$

С учётом отсутствия зависимости полученного выражения от $\bar{t}_1, \ldots, \bar{t}_\tau$ выполняется первое из равенств (29).

Пусть $\varepsilon = 1/2$. Тогда $l_i = 1$ и $\pi_{l_i}^{(i)} = 1$. Таким образом,

$$\Pr\{\tau = 1\} = 1 \quad \text{и} \quad \mathbf{E}T^{(\pi)}_{\mathcal{A}_{1/2}(\bar{t}_1),\ldots,\mathcal{A}_{1/2}(\bar{t}_\tau)} = 1,$$

откуда следует второе из равенств (29).

Пусть теперь $0 < \varepsilon < 1/2$. Рассмотрим отдельно три случая.

Если $\pi \leqslant s(1/2+\varepsilon)^n$, то $l_i = \left]\dfrac{2^n\pi}{(1+2\varepsilon)^n}\right[$ и $\pi_{l_i}^{(i)} = l_i(1/2+\varepsilon)^n$ для $i = 1, \ldots, j$. Таким образом, (30) принимает следующий вид:

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau = j\right) = (j-1)\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[+ (1/2+\varepsilon)^n \sum_{i=1}^{]2^n\pi/(1+2\varepsilon)^n[} i =$$
$$= (j-1)\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[+ \frac{(1+2\varepsilon)^n}{2^{n+1}}\left(\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[+ 1\right)\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[.$$

В рассматриваемом случае $\Pr\{\tau{=}j\}{=}(1/2{+}\varepsilon)^n\left]\dfrac{2^n\pi}{(1+2\varepsilon)^n}\right[\left(1{-}\left(\dfrac{1}{2}{+}\varepsilon\right)^n\right]\dfrac{2^n\pi}{(1{+}2\varepsilon)^n}\left[\right)^{j-1}$, т. е. $\tau \sim \mathrm{Geom}\left(\left(\dfrac{1}{2}+\varepsilon\right)^n\right]\dfrac{2^n\pi}{(1+2\varepsilon)^n}\left[\right)$, поэтому $\mathbf{E}\tau = 2^n\Big/\left((1+2\varepsilon)^n\right]\dfrac{2^n\pi}{(1+2\varepsilon)^n}\left[\right)$. В результате

$$\mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)} = \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\mathbf{E}(\tau-1) + \frac{(1+2\varepsilon)^n}{2^{n+1}}\left(\left(\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right)^2 + \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right) =$$
$$= \frac{2^n}{(1+2\varepsilon)^n} - \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\frac{(1+2\varepsilon)^n}{2^{n+1}}\left(\left(\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right)^2 + \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right),$$

откуда следует (26).

Если $s(1/2+\varepsilon)^n < \pi \leqslant 1 - (2^n - s - 1)\,(1/2-\varepsilon)^n$, то для $i = 1, \ldots, j$ получаем

$$l_i = s+1 \quad \text{и} \quad \pi_{l_i}^{(i)} = s(1/2+\varepsilon)^n + 1 - s(1/2+\varepsilon)^n - (2^n - s - 1)\,(1/2-\varepsilon)^n +$$
$$+(l_i - s - 1)(1/2-\varepsilon)^n = 1 - (2^n - s - 1)\,(1/2-\varepsilon)^n,$$

поэтому

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau = j\right) = (j-1)(s+1) + (1/2+\varepsilon)^n\sum_{i=1}^{s} i +$$
$$+(s+1)\left(1 - s\,(1/2+\varepsilon)^n - (2^n - s - 1)\,(1/2-\varepsilon)^n\right) =$$
$$= j(s+1) - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n - (s+1)\,(2^n - s - 1)\left(\frac{1}{2}-\varepsilon\right)^n.$$

При этом $\Pr\{\tau = j\} = \left(1 - (2^n - s - 1)\,(1/2-\varepsilon)^n\right)\left((2^n - s - 1)\,(1/2-\varepsilon)^n\right)^{j-1}$, т. е. $\tau \sim$ $\sim \mathrm{Geom}\left(1 - (2^n - s - 1)\,(1/2-\varepsilon)^n\right)$. Таким образом, $\mathbf{E}\tau = \dfrac{2^n}{2^n - (2^n - s - 1)\,(1-2\varepsilon)^n}$ и

$$\mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)} = (s+1)\mathbf{E}\tau - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n - (s+1)\,(2^n - s - 1)\left(\frac{1}{2}-\varepsilon\right)^n =$$

$$= (s+1)\left(\frac{2^n}{2^n-(2^n-s-1)(1-2\varepsilon)^n} - \frac{s}{2}\left(\frac{1}{2}+\varepsilon\right)^n - (2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n\right),$$

откуда получаем (27).

Наконец, если $1-(2^n-s-1)(1/2-\varepsilon)^n < \pi \leqslant 1$, то для $i=1,\ldots,j$ справедливы равенства $l_i = 2^n - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]$ и $\pi_{l_i}^{(i)} = 1 - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n$, поэтому

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau=j\right) = (j-1)\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right) + \left(\frac{1}{2}+\varepsilon\right)^n\sum_{i=1}^{s} i +$$

$$+(s+1)\left(1-s\left(\frac{1}{2}+\varepsilon\right)^n - (2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n\right) + \left(\frac{1}{2}-\varepsilon\right)^n \sum_{i=s+2}^{2^n-[2^n(1-\pi)/(1-2\varepsilon)^n]} i =$$

$$= (j-1)\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right) + s + 1 - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n - (s+1)(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n +$$

$$+\frac{1}{2}\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right] - s - 1\right)\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right] + s + 2\right)\left(\frac{1}{2}-\varepsilon\right)^n =$$

$$= (j-1)\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right) + s + 1 - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n +$$

$$+\frac{1}{2}\left(2^{2n} - 2^{n+1}s - 2^n + \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right] - 2^{n+1} - 1\right) + s^2 + s\right)\left(\frac{1}{2}-\varepsilon\right)^n.$$

При этом $\Pr\{\tau=j\} = \left(1 - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n\right)\left(\left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n\right)^{j-1}$, т. е. $\tau \sim \mathrm{Geom}\left(1-\left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n\right)$. Следовательно, $\mathbf{E}\tau = \left(1-\left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n\right)^{-1}$ и выполняется равенство

$$\mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)} = \frac{\left(2^n - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right)\left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right](1-2\varepsilon)^n}{2^n - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right](1-2\varepsilon)^n} + s + 1 - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n +$$

$$+\frac{1}{2}\left(2^{2n} - 2^{n+1}s - 2^n + \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right] - 2^{n+1} - 1\right) + s^2 + s\right)\left(\frac{1}{2}-\varepsilon\right)^n,$$

из которого следует (28). ■

Замечание 7. Верификация выражений (26)–(28) выполнена с использованием автоматизированной системы упрощения алгебраических выражений пакета Wolfram Mathematica 12.1.

Проиллюстрируем характер зависимости $T_n^{(\pi)}(\varepsilon)$ от величины π, $0 < \pi \leqslant 1$, при $n=7$ и некоторых фиксированных значениях параметра ε (рис. 3).

Из графиков на рис. 3 видно, что с увеличением значения ε эффективность (с точки зрения трудозатрат) последовательности разнесённых по времени выполнения усечённых алгоритмов опробования становится выше, чем у алгоритма опробования до успеха.

Приведённые результаты и примеры ещё раз подтверждают тезис о важности обоснования выбора модели опробования ключа — до успеха или на основе нескольких

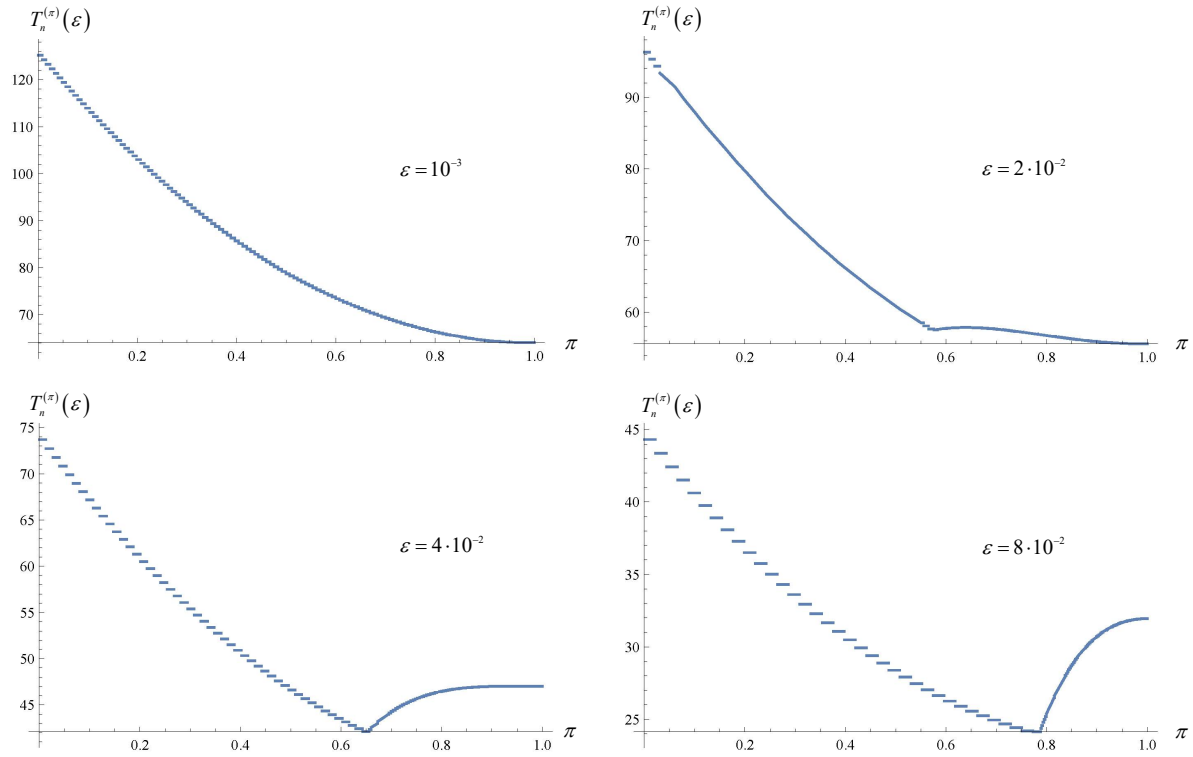

Рис. 3. Зависимость $T_n^{(\pi)}(\varepsilon)$ от π при $n = 7$ и некоторых значениях ε

усечённых алгоритмов. В отдельных случаях та или иная модель может давать существенный выигрыш по трудоёмкости.

Итак, мы получили точные и достижимые оценки снизу для средней трудоёмкости процедуры опробования ключа на основе усечённых алгоритмов с вероятностями успеха, не меньшими некоторой заданной границы π, $0 < \pi \leqslant 1$. Перейдём к финальному этапу исследования — оценке практической секретности ключа.

4. Оценка снизу практической секретности ключа

Для произвольных параметров $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$, вероятностной схемы (7) через $T_n(\varepsilon)$ обозначим практическую секретность ключа, сформированного источником (6).

Согласно общей теории [5, 6] и результатам предыдущих пунктов настоящей работы, справедливо равенство

$$T_n(\varepsilon) = \min_{0<\pi\leqslant 1}\left(\min_{\bar{t}_1,\ldots,\bar{t}_\tau}\left(\min_{\substack{p_1(\bar{t}_1),\ldots,p_{2^n}(\bar{t}_1)\\ \ldots\\ p_1(\bar{t}_\tau),\ldots,p_{2^n}(\bar{t}_\tau)}} \mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)}\right)\right), \tag{31}$$

где $\bar{t}_i = \left(t_1^{(i)}, t_2^{(i)}, \ldots, t_n^{(i)}\right)$, $1 \leqslant t_1^{(i)} < t_2^{(i)} < \ldots < t_n^{(i)}$, векторы $\left(p_1(\bar{t}_i), p_2(\bar{t}_i), \ldots, p_{2^n}(\bar{t}_i)\right)$ удовлетворяют (8), $i = 1, \ldots, \tau$, а π — нижняя граница вероятностей успеха усечённых алгоритмов опробования, $0 < \pi \leqslant 1$.

С учётом введённых в п. 3 обозначений выражение (31) может быть записано в компактном виде

$$T_n(\varepsilon) = \min_{0<\pi\leqslant 1} \left(T_n^{(\pi)}(\varepsilon)\right). \tag{32}$$

Таким образом, процесс вычисления $T_n(\varepsilon)$ сводится к определению минимума кусочно-постоянной функции, описанной в утверждении 4.

В табл. 4 приведены достижимые оценки снизу практической секретности ключа $T_n(\varepsilon)$, вычисленные с использованием формул (32) и (26)–(28) для значений $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$, указанных в табл. 1, и показано, на каких значениях π достигаются эти оценки.

Таблица 4

Оценка	ε						
	10^{-4}	$5\cdot 10^{-4}$	10^{-3}	$5\cdot 10^{-3}$	10^{-2}	$5\cdot 10^{-2}$	10^{-1}
$n = 56$							
$T_n(\varepsilon)$	$3{,}58\cdot 10^{16}$	$3{,}50\cdot 10^{16}$	$3{,}40\cdot 10^{16}$	$2{,}33\cdot 10^{16}$	$1{,}26\cdot 10^{16}$	$1{,}73\cdot 10^{14}$	$1{,}33\cdot 10^{12}$
π	1	1	1	0,639	0,758	0,997	0,999
$n = 112$							
$T_n(\varepsilon)$	$2{,}57\cdot 10^{33}$	$2{,}45\cdot 10^{33}$	$2{,}31\cdot 10^{33}$	$9{,}02\cdot 10^{32}$	$2{,}85\cdot 10^{32}$	$6{,}00\cdot 10^{28}$	$3{,}52\cdot 10^{24}$
π	1	1	1	0,756	0,906	0,999	0,999
$n = 128$							
$T_n(\varepsilon)$	$1{,}68\cdot 10^{38}$	$1{,}59\cdot 10^{38}$	$1{,}48\cdot 10^{38}$	$4{,}98\cdot 10^{37}$	$1{,}36\cdot 10^{37}$	$8{,}56\cdot 10^{32}$	$1{,}25\cdot 10^{28}$
π	1	1	1	0,784	0,930	0,999	1
$n = 160$							
$T_n(\varepsilon)$	$7{,}19\cdot 10^{47}$	$6{,}72\cdot 10^{47}$	$6{,}15\cdot 10^{47}$	$1{,}53\cdot 10^{47}$	$3{,}08\cdot 10^{46}$	$1{,}74\cdot 10^{41}$	$1{,}57\cdot 10^{35}$
π	1	1	1	0,834	0,962	0,999	1
$n = 168$							
$T_n(\varepsilon)$	$1{,}84\cdot 10^{50}$	$1{,}71\cdot 10^{50}$	$1{,}56\cdot 10^{50}$	$3{,}60\cdot 10^{49}$	$6{,}72\cdot 10^{48}$	$2{,}08\cdot 10^{43}$	$9{,}33\cdot 10^{36}$
π	1	1	1	0,845	0,968	0,999	1
$n = 192$							
$T_n(\varepsilon)$	$3{,}08\cdot 10^{57}$	$2{,}84\cdot 10^{57}$	$2{,}49\cdot 10^{57}$	$4{,}72\cdot 10^{56}$	$7{,}01\cdot 10^{55}$	$3{,}54\cdot 10^{49}$	$1{,}97\cdot 10^{42}$
π	1	1	0,595	0,874	0,980	0,999	1
$n = 256$							
$T_n(\varepsilon)$	$5{,}64\cdot 10^{76}$	$5{,}05\cdot 10^{76}$	$3{,}96\cdot 10^{76}$	$4{,}56\cdot 10^{75}$	$3{,}64\cdot 10^{74}$	$1{,}47\cdot 10^{66}$	$3{,}11\cdot 10^{56}$
π	1	1	0,626	0,929	0,994	0,999	1

Заключение

Для математической модели дискретного источника (6), приближённой к реальным условиям функционирования физических устройств, используемых для формирования криптографических ключей, в том числе допускающей нестационарность таких устройств, а также наличие зависимости между битами формируемых ключей, получены достижимые оценки снизу практической секретности ключа.

Результаты работы обобщают ранее известные оценки, выписанные в достаточно «рафинированных» модельных предположениях [5, 6].

ЛИТЕРАТУРА

1. *Kahn D.* The Codebreakers: the Story of Secret Writing. N.Y.: Scribner, 1996. 1181 p.
2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. М.: Триумф, 2002. 816 с.
3. *Арбеков И. М.* Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой. М.: URSS, 2022. 168 с.

4. *Turam M., Barker E., Kelsey J., and McKay K.* Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publ. 800-90B. 2018. 76 p.
5. *Арбеков И. М.* Критерии секретности ключа // Матем. вопр. криптогр. 2016. Т. 7. Вып. 1. С. 39–56.
6. *Arbekov I. M.* Lower bounds for the practical secrecy of a key // Матем. вопр. криптогр. 2017. Т. 8. Вып. 2. С. 29–38.
7. *Лось А. Б., Миронкин В. О.* Теоретико-информационные аспекты защиты информации. М.: URSS, 2023. 144 с.
8. *Лось А. Б., Нестеренко А. Ю., Рогачева О. А.* О влиянии неравновероятности выходной последовательности на качество криптографических преобразований // Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории. Материалы XXII Междунар. конф., посвящённой 120-летию со дня рождения академика А. Н. Колмогорова и 60-летию со дня открытия школы-интерната № 18 при Московском университете. Тула: ТГПУ им. Л. Н. Толстого, 2023. С. 151–157.
9. *Феллер В.* Введение в теорию вероятностей и ее приложения. Т. 1. 2-е изд. М.: Мир, 1963. 498 с.
10. *Карпов А. А., Миронкин В. О., Михайлов М. М.* Об энтропийных характеристиках последовательной процедуры опробования элементов полиномиальной схемы // Обозр. прикл. и промышл. матем. 2021. Т. 28. № 1. С. 9–12.
11. *Кельберт М. Я., Сухов Ю. М.* Вероятность и статистика в примерах и задачах. Т. I: Основные понятия теории вероятностей и математической статистики. 2-е изд., доп. М.: МЦНМО, 2010. 486 с.

REFERENCES

1. *Kahn D.* The Codebreakers: the Story of Secret Writing. N.Y., Scribner, 1996. 1181 p.
2. *Schneier B.* Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996.
3. *Arbekov I. M.* Elementarnaya kvantovaya kriptografiya: Dlya kriptografov, ne znakomykh s kvantovoy mekhanikoy. [Elementary Quantum Cryptography: For Cryptographers who are not Familiar with Quantum Mechanics]. Moscow, URSS Publ., 2022. 168 p. (in Russian)
4. *Turam M., Barker E., Kelsey J., and McKay K.* Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publication 800-90B, 2018. 76 p.
5. *Arbekov I. M.* Kriterii sekretnosti klyucha [Key secrecy criteria]. Matem. Vopr. Kriptogr., 2016, vol. 7, no. 1, pp. 39–56. (in Russian)
6. *Arbekov I. M.* Lower bounds for the practical secrecy of a key. Matem. Vopr. Kriptogr., 2017, vol. 8, no. 2, pp. 29–38.
7. *Los A. B. and Mironkin V. O.* Teoretiko-informatsionnye aspekty zashchity informatsii [Information-Theoretical Aspects of Information Security]. Moscow, URSS Publ., 2023. 144 p. (in Russian)
8. *Los A. B., Nesterenko A. Yu., and Rogacheva O. A.* O vliyanii neravnoveroyatnosti vykhodnoy posledovatel'nosti na kachestvo kriptograficheskikh preobrazovaniy [On the effect of the nonprobability of the output sequence on the quality of cryptographic transformations]. Algebra, teoriya chisel, diskretnaya geometriya i mnogomasshtabnoe modelirovanie: Sovremennye problemy, prilozheniya i problemy istorii. Materialy XXII Mezhdunar. konf., posvyashchennoy 120-letiyu so dnya rozhdeniya akademika A. N. Kolmogorova i 60-letiyu so dnya otkrytiya shkoly-internata № 18 pri Moskovskom universitete. Tula, TGPU im. L. N. Tolstogo, 2023, pp. 151–157. (in Russian)

9. *Feller W.* An Introduction to Probability Theory and its Applications, vol. I. John Wiley & Sons, 1957.
10. *Karpov A. A., Mironkin V. O., and Mikhaylov M. M.* Ob entropiynykh kharakteristikakh posledovatel'noy protsedury oprobovaniya elementov polinomial'noy skhemy [On the entropy characteristics of a sequential procedure for testing elements of a polynomial scheme]. Obozr. Prikl. i Promyshl. Matem., 2021, vol. 28, no. 1, pp. 9–12. (in Russian)
11. *Kel'bert M. Ya. and Sukhov Yu. M.* Veroyatnost' i statistika v primerakh i zadachakh. T. I: Osnovnye ponyatiya teorii veroyatnostey i matematicheskoy statistiki [Probability and Statistics in Examples and Problems. Vol. I: Basic Concepts of Probability Theory and Mathematical Statistics]. 2nd ed. Moscow, MCCME Publ., 2010. 486 p. (in Russian)