БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Научно-исследовательский институт
прикладных проблем математики и информатики

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ: ТЕСТИРОВАНИЕ И ОЦЕНИВАНИЕ УРОВНЯ БЕЗОПАСНОСТИ

Юрий Семёнович Харин,
Владимир Юрьевич Палуха

ВВЕДЕНИЕ

Актуальным направлением криптологии является анализ качества и оценивание уровня безопасности криптографических генераторов случайных и псевдослучайных последовательностей [1, 2]. Генерация равномерно распределенной случайной последовательности (РРСП) представляет собой важную задачу для генерации «гаммы» в поточных криптосистемах, ключей и векторов инициализации, одноразовых чисел, в криптографических протоколах и схемах ЭЦП. В криптографии генерация случайности сводится к задаче генерации РРСП $x_t \in \{0, 1\}$, $t = 1, 2, \ldots$, для которой при любом $s = 1, 2, \ldots$ s-мерное распределение вероятностей является равномерным: $\mathbf{P}\{x_1 = j_1, x_2 = j_2, \ldots, x_s = j_s\} = 2^{-s}$. Для анализа качества выходных последовательностей длины T криптографических генераторов используются батареи статистических тестов проверки нулевой гипотезы $H_0 = \{x_t$ есть РРСП$\}$ против альтернативы $H_1 = \overline{H_0}$ [1 – 3].

ПРОБЛЕМЫ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ И СУЩЕСТВУЮЩИЕ ПОДХОДЫ К ИХ РАЗРЕШЕНИЮ

Проведенный в [2] обзор существующих тестов выявляет следующие недостатки: 1) многие из тестов ориентированы на проверку лишь частных случаев альтернативы $\overline{H_0}$; 2) многие тесты не фиксируют семейство альтернатив и не имеют оценок мощности w_T; 3) при включении нескольких тестов в «батарею» не удается учесть вероятностную зависимость тестовых статистик; 4) известны примеры генераторов псевдослучайных последовательностей, «уверенно» преодолевающих батареи тестов [4]. Особенно значимой критике подвергнута «батарея» тестов NIST STS, что привело к решению Национального института США по стандартизации о начале «ревизии» «батареи тестов» [5].

Для снижения этих недостатков криптографическое сообщество предлагает определенные подходы к статистическому тестированию. В [6] предлагается подход, основанный на теоретическом исследовании вероятностной зависимости тестовых статистик, входящих в батарею тестов. В [7] предлагается подход, основанный на двухэтапной проверке гипотез H_0, $\overline{H_0}$, включая на 2-ом этапе проверку соответствия равномерному закону распределения **P**-значений, вычисляемых на 1-ом этапе.

Для преодоления указанных недостатков в докладе предлагается 2 принципиально новых подхода к статистическому тестированию криптографических генераторов с использованием сложной нулевой гипотезы. На основе этих подходов впервые решается актуальная проблема статистического оценивания уровня безопасности криптографических генераторов по их выходным последовательностям.

НЕКОРРЕКТНОСТЬ МОДЕЛИ ПРОСТОЙ НУЛЕВОЙ ГИПОТЕЗЫ

В дополнение к указанным выше недостаткам существующих статистических тестов выделим **еще один их общий существенный недостаток**: некорректность модели простой нулевой гипотезы H_0 и необходимость использования сложной нулевой гипотезы при статистическом тестировании [8].

Этот недостаток проявляется в следующем парадоксе: при увеличении длины $T \to +\infty$ наблюдаемых последовательностей, порождаемых реально существующими генераторами случайности, вероятность принятия альтернативы $\overline{H_0}$ стремится к единице: $w_T \to 1$. Иначе говоря, «увеличением длины исследуемой последовательности T можно забраковать любой **реальный** генератор случайности».

ПОДХОД К СТАТИСТИЧЕСКОМУ ТЕСТИРОВАНИЮ НА ОСНОВЕ СЛОЖНОЙ НУЛЕВОЙ ГИПОТЕЗЫ

Объяснение этого «парадокса» состоит в следующем. Реальные генераторы случайности – не идеальны, они отклоняются от гипотезы H_0 по своему вероятностному распределению на некоторую величину $\varepsilon > 0$. Все тесты, включаемые в батареи тестов, как известно, обладают оптимальным свойством проверки простой гипотезы H_0 против сложной альтернативы $\overline{H_0}$ – свойством состоятельности: $w_T \to 1$ при $T \to +\infty$. Таким образом, этот «парадокс» порожден некорректностью математической модели нулевой гипотезы H_0. Для того, чтобы избежать этого «парадокса» нулевая гипотеза должна быть сложной: она должна задавать величину допуска $\varepsilon > 0$ отклонений от простой гипотезы H_0.

ПРОСТАЯ НУЛЕВАЯ ГИПОТЕЗА H_0

Пусть наблюдается двоичная случайная последовательность длины $T = n \cdot s$, разбитая на n последовательных s-грамм $\left(s \in \mathbb{N}\right)$:

$$X = X_1^T = \left(x_1, \ \ldots, \ x_T\right) \equiv \left(X_1^s, \ X_{s+1}^{2s}, \ \ldots, \ X_{(n-1)s+1}^{T}\right) \in V^T, \quad V = \left\{0, \ 1\right\}; \quad (1)$$

эти s-граммы независимы в совокупности и одинаково распределены с некоторым распределением $p = \left(p_{J_1^s}\right) \in \mathrm{P}$:

$$\mathbf{P}\left\{X_{(i-1)s+1}^{is} = J_1^s\right\} ::= \mathbf{P}\left\{x_{(i-1)s+1} = j_1, \ \ldots, \ x_{is} = j_s\right\} = p_{J_1^s}, \qquad (2)$$

$$J_1^s = \left(j_k\right) \in V^s, \quad i = 1, \ \ldots, \ n,$$

$$\mathcal{P} = \left\{p = \left(p_{J_1^s}\right) : \ p_{J_1^s} \geq 0, \ \ J_1^s \in V^s, \ \ \sum_{J_1^s \in V^s} p_{J_1^s} = 1\right\} - \qquad (3)$$

семейство (симплекс) всевозможных s-мерных вероятностных распределений на V^s. Для упрощения обозначений (1) – (3) перейдем от мультииндекса J_1^s к одномерному индексу $k \in \{0,\ 1,\ \ldots,\ 2^s - 1\}$:

$$k = \ < J_1^s > \ :: \ = \sum_{i=1}^{s} j_i \cdot 2^{i-1} \in \{0,\ 1,\ \ldots,\ K-1\},\ \ K = 2^s;$$

$$J_1^s = (j_1,\ \ldots, j_s) = \ > k < j_{s\text{-}i+1} = \left[\left(k - \sum_{l=s-i+2}^{s} j_l \cdot 2^{l-1} \right) \Big/ 2^{s-i} \right], i = 1,\ 2\ldots,\ s.$$

В существующих «батареях тестов» [3, 4], подвергнутых многочисленным модификациям и критике [4 – 8], используются тесты статистической проверки простой нулевой гипотезы

$$H_0 = \{ p = p^{(0)} \},\ \ p^{(0)} = \left(p_k^{(0)} \right),\ \ p_k^{(0)} \equiv 1/K, \qquad (4)$$

против сложной альтернативы $\overline{H_0}$, приводящие к указанному выше парадоксу.

СЛОЖНАЯ НУЛЕВАЯ ГИПОТЕЗА H_0^{ε}

Во избежание парадокса «неадекватности модели (4)» введем в рассмотрение сложную нулевую гипотезу:

$$H_0^{\varepsilon} = \left\{ p = (p_k) \in \mathcal{P}_0^{\varepsilon} \right\}, \mathcal{P}_0^{\varepsilon} = \left\{ p \in \mathcal{P} : \left\| p - p^{(0)} \right\| = \sqrt{\sum_{k=0}^{K-1} \left(p_k - \frac{1}{K} \right)^2} \le \varepsilon \right\} - (5)$$

пересечение симплекса $\mathcal{P}$ с гипершаром в $\mathbb{R}^K$ заданного радиуса ε с центром в точке p_* s-мерного равномерного распределения; $\varepsilon \in \left(0, \sqrt{1-1/K}\right)$ – достаточно малый параметр нулевой гипотезы (5), определяющий допустимые отклонения от простой гипотезы H_0. Гипотеза H_0 является предельной по отношению к $H_0^{\varepsilon} : H_0^{\varepsilon} \xrightarrow[\varepsilon \to 0]{} H_0$. Альтернатива также является сложной: $H_1^{\varepsilon} = \overline{H_0^{\varepsilon}} =: \left\{ p \in \mathcal{P} : \left\| p - p^{(0)} \right\| > \varepsilon \right\}$.

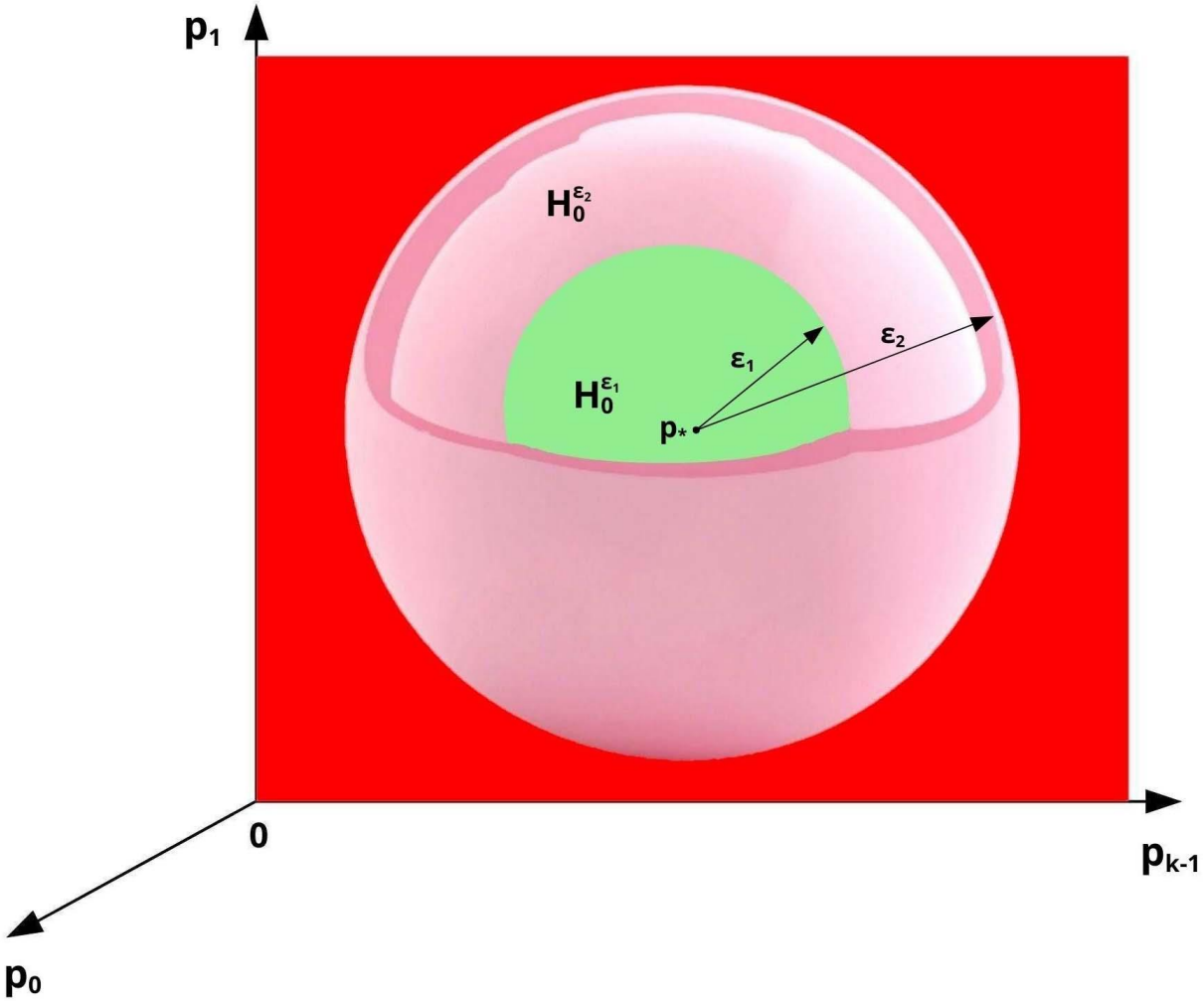

Рис. 1. Иллюстрация простой H_0 и двух сложных гипотез $H_0^{\varepsilon_1}, H_0^{\varepsilon_2}$: $p_* = p^{(0)}$

КРИТЕРИЙ ОТНОШЕНИЯ ПРАВДОПОДОБИЯ ДЛЯ ПРОВЕРКИ ГИПОТЕЗ $H_0^{\varepsilon}, H_1^{\varepsilon}$

Построим критерий отношения правдоподобия по наблюдаемой последовательности $X = X_1^T$ для проверки сложной нулевой гипотезы H_0^{ε} против сложной альтернативы H_1^{ε}.

Примем следующие обозначения: $\mathbf{1}\{C\}$ – индикатор события C, $\mathbf{1}_N$ – вектор-столбец, все N компонент которого равны единице;

$$\hat{p} = (\hat{p}_k),\ \hat{p}_k = \frac{\nu_k}{n},\ \nu_k = \sum_{i=1}^{n} \mathbf{1}\left\{\left\langle X_{(i-1)s+1}^{is} \right\rangle = k\right\} \geq 0,\ k = 0,1,\ \ldots,\ K-1, \quad -(6)$$

несмещенная, строго состоятельная, асимптотически нормальная и эффективная оценка максимального правдоподобия для p;

ν_k – частота встречаемости s-граммы $\rangle k \langle$ в последовательности n фрагментов X_1^s, X_{s+1}^{2s}, …, $X_{(n-1)s+1}^{T}$;

$$l(X;p) = \sum_{k=0}^{K-1} \nu_k \ln p_k = n \sum_{k=0}^{K-1} \hat{p}_k \ln p_k - \quad (7)$$

логарифмическая функция правдоподобия (ЛФП) для последовательности $X = X_1^T$;

$$S_\varepsilon = p \in \mathcal{P} : \left\| p - p^{(0)} \right\| = \varepsilon \subset \mathcal{P}_0^\varepsilon - \quad (8)$$

пересечение гиперсферы радиуса ε с центром в точке $p^{(0)} = \frac{1}{K}\mathbf{1}_K$ с симплексом $\mathcal{P}$;

$$l_{S_\varepsilon}^*(X) = \max_{p \in S_\varepsilon} l(X;p) - \quad (9)$$

максимальное значение ЛФП на гиперсфере S_ε, определяемой (8).

ТЕСТ ПРОВЕРКИ H_0^{ε}, H_1^{ε} НА ОСНОВЕ АСИМПТОТИЧЕСКИХ РАЗЛОЖЕНИЙ

Логарифмическая статистика отношения правдоподобия при проверке сложных гипотез для рассматриваемой модели наблюдений (1) – (5) имеет вид [9]:

$$\lambda(X) ::= \sup_{p \in \mathcal{P}_0^{\varepsilon}} l(X; p) - \sup_{p \in \mathcal{P}} l(X; p) \le 0,$$

$$\lambda(X) = \begin{cases} l_{S_\varepsilon}^*(X) - n \sum_{k=0}^{K-1} \hat{p}_k \ln \hat{p}_k, \text{ если } \left\| p - p^{(0)} \right\| > \varepsilon, \\ 0, \text{ если } \left\| \hat{p} - p^{(0)} \right\| \le \varepsilon. \end{cases} \quad (10)$$

Семейство всевозможных решающих правил (статистических тестов), основанное на логарифмической статистике отношения правдоподобия (10), определяется порогом (критическим значением) $\Delta_n \le 0$:

$$d = d(X) = \begin{cases} 0, \ \lambda(X) \geq \Delta_n, \\ 1, \ \lambda(X) < \Delta_n. \end{cases} \tag{11}$$

Основная трудность в реализации и теоретическом анализе решающего правила (10), (11) состоит в вычислении статистики (9), сводящемся к отысканию условного максимума $p = \left(p_k \right)$ по логарифмической функции правдоподобия (7) на гиперсфере (8) при дополнительных ограничениях: $\sum_{k=0}^{K-1} p_k = 1, \ p_k \geq 0$. В [8] доказано, что при $\varepsilon \to 0$ удается получить асимптотические разложения статистики $l^*_{S_\varepsilon}(X)$ с погрешностью $O\left(\varepsilon^2\right)$ и $O\left(\varepsilon^3\right)$, в частности:

$$\lambda(X) = \left(nH\left(\hat{p}\right) - \ln K + \varepsilon K \left\| p - p^{(0)} \right\| \right) + O\left(\varepsilon^2\right), \tag{12}$$

где $H\left(\hat{p}\right) = -\sum_{k=0}^{K-1} \hat{p}_k \ln \hat{p}_k \geq 0$ – подстановочная оценка энтропии Шеннона s-граммы, а $\hat{p} = \left(\hat{p}_k \right)$ определяется (6).

ВЕРОЯТНОСТНЫЕ ХАРАКТЕРИСТИКИ ТЕСТА

Теорема 1. *Если имеет место математическая модель двоичной последовательности (1) – (5), то при использовании аппроксимации (12) и* $n \to +\infty$ *заданный асимптотический размер* $0 < \alpha_0 < 1/2$ *достигается для теста*

$$d = d(X) = \begin{cases} 0, & \left\| p - p^{(0)} \right\| \le \gamma_n, \\ 1, & \left\| p - p^{(0)} \right\| > \gamma_n, \end{cases} \tag{13}$$

$$\gamma_n = \varepsilon + \frac{\Phi^{-1}(1-\alpha_0)}{\sqrt{n}} \sqrt{1/K + \varepsilon\left(e_K^+ - \varepsilon\right)}, \quad e_K^+ = \frac{1 - 2/K}{\sqrt{1 - 1/K}} \le 1,$$

где $\Phi^{-1}(\cdot)$ *– квантильная функция стандартного нормального закона* $\mathcal{N}_1(0,1)$.

Теорема 2. *В условиях Теоремы 1 при* $n \to +\infty$ *для частной альтернативы* $h^{\varepsilon_+} ::= \left\{ p \in S_{\varepsilon_+} \right\} \subset H_1^{\varepsilon}$ *и фиксированных* ε, ε_+, *таких, что* $\varepsilon_+ > \varepsilon$, *справедливо следующее асимптотическое приближение мощности* $w(\varepsilon_+)$ *решающего правила (13):*

$$w(\varepsilon_+) = \Phi\left(\sqrt{\frac{n}{K}} \frac{K\left(\varepsilon_+ - \varepsilon\right)}{\sqrt{1 + K\varepsilon_+\left(e_K - \varepsilon_+\right)}} - \sqrt{\frac{1 + K\varepsilon\left(e_K^+ - \varepsilon\right)}{1 + K\varepsilon_+\left(e_K - \varepsilon_+\right)}}\ \Phi^{-1}\left(1 - \alpha_0\right) \right), \quad (14)$$

где e_K^+ *определено в (13), а* $e_K = \sum_{k=0}^{K-1} \left(p_k - p_k^{(0)} \right)^3 / \varepsilon^3, \ \left| e_K \right| \le e_K^+.$

Следствие 1. *Выполняются свойство состоятельности решающего правила (13):*

$$w(\varepsilon_+) \xrightarrow[n \to +\infty]{} 1, \ \forall \varepsilon_+ > \varepsilon,$$

и свойство монотонности его мощности:

$$w(\varepsilon_+) \ge w(\varepsilon) = \alpha_0, \ \forall \varepsilon_+ \ge \varepsilon.$$

ТЕСТИРОВАНИЕ НА ОСНОВЕ ЭНТРОПИЙНЫХ ПРОФИЛЕЙ

Пусть наблюдается случайная выборка $X = \{x_t : t = 1, \ldots, n\}$ объёма n из распределения вероятностей $\{p_k : k \in A\}$, $p_k = \mathbf{P}\{x_t = k\}$, где $A = \{0, \ldots, K-1\}$, $K = 2^s$, порождённая исследуемым генератором. Построим частотные оценки:

$$\hat{p}_k = \frac{\nu_k}{n}, \ \nu_k = \sum_{t=1}^{n} \mathbf{1}\{x_t = k\} \geq 0, \ k \in A.$$

Будем использовать функционалы энтропии из Таблицы 1 и **асимптотику «растущей размерности»**:

$$n, \ K \to \infty, \ n / K \to \lambda, 0 < \lambda < \infty, \qquad (15)$$

которая отличается от классической ($n \to \infty$, $K < \infty$) тем, что длительность наблюдения n и число значений (сложность модели) K растут синхронно.

Таблица 1: Исследуемые функционалы энтропии ($x^{\underline{2}} =:: x(x-1)$)

Тип	Формула	Статистическая оценка
Энтропия Шеннона	$H(p) = -\sum_{k \in A} p_k \ln p_k$	$\hat{H}(n, K) = \ln n - \frac{1}{n} \sum_{k \in A} \nu_k \ln \nu_k$
Энтропия Реньи	$H_2(p) = -\ln\left(\sum_{k \in A} p_k^2 \right)$	$\hat{H}_2(n, K) = 2 \ln n - \ln\left(\sum_{k \in A} \nu_k^{\underline{2}} \right)$
Энтропия Тсаллиса	$S_2(p) = 1 - \sum_{k \in A} p_k^2$	$\hat{S}_2(n, K) = 1 - \frac{1}{n^2} \sum_{k \in A} \nu_k^{\underline{2}}$

Доказана асимптотическая нормальность оценок $\hat{H}$, $\hat{H}_2(n, K)$, $\hat{S}_2(n, K)$ при простой нулевой гипотезе H_0 и оценки $\hat{S}_2(n, K)$ при сложной нулевой гипотезе H_0^{ε}, определяемой (5). В таблице 2 приведены формулы асимптотических математических ожиданий и дисперсий оценок энтропии Шеннона, Реньи и Тсаллиса при справедливости гипотезы H_0 из [10, 11] и Тсаллиса при справедливости гипотезы H_0^{ε} из [12].

Таблица 2: Параметры асимптотически нормального распределения оценок энтропии

Тип энтропии; гипотеза	Математическое ожидание и дисперсия
Шеннон; H_0	$\mu_H = \ln n - e^{-\lambda}\sum_{k=1}^{+\infty}\frac{\lambda^k \ln(k+1)}{k!}$, $\sigma_H^2 = \frac{e^{-\lambda}}{n}\sum_{k=1}^{+\infty}\frac{(k+1)\lambda^k}{k!}\ln^2(k+1) -$ $-\frac{e^{-2\lambda}}{N}\left(\sum_{k=1}^{+\infty}\frac{\ln(k+1)\lambda^k}{k!}\right)^2 - \frac{e^{-2\lambda}}{n}\left(\sum_{k=1}^{+\infty}\ln(k+1)\frac{\lambda^k}{k!}(k+1-\lambda)\right)^2$
Реньи; H_0	$\mu_{H,2} = \ln K$, $\sigma_{H,2}^2 = \frac{2}{n\lambda}$
Тсаллис; H_0	$\mu_{S,2} = 1 - \frac{1}{K}$, $\sigma_{S,2}^2 = \frac{2}{Kn^2}$
Тсаллис; $H_0^{\varepsilon}, \varepsilon \le \varepsilon_+$	$\mu_{S,2}^{(\varepsilon_+)} = \mu_{S,2} - \varepsilon_+^2$, $\sigma_{S,2}^{2(\varepsilon_+)} = \sigma_{S,2}^2 + \frac{2}{n^2}(2\lambda+1)\varepsilon_+^2 + \frac{4\varepsilon_+^3}{n}(1-\varepsilon_+)$

Введём обозначения для проверки гипотез H_0, $H_0^{(\varepsilon)}$ об s-мерной равномерности $(1 \le s \le s_+)$: $\hat{h}(s)$ – статистическая оценка энтропии Шеннона, Реньи или Тсаллиса, μ_h и σ_h^2 – соответственно её асимптотические математическое ожидание и дисперсия при истинной гипотезе H_0. Статистический критерий асимптотического уровня значимости $\alpha \in \{0, 1\}$ проверки гипотез H_0, $\overline{H_0}$ $\left(H_0^{\varepsilon}, \overline{H_0^{\varepsilon}}\right)$ на основе статистики $\hat{h}(s)$ имеет вид:

$$\text{принимается} \quad \begin{cases} H_0 \left(H_0^{\varepsilon}\right), \text{ если } \Delta_- < \hat{h} < \Delta_+, \\ \overline{H_0} \left(\overline{H_0^{\varepsilon}}\right), \text{ в противном случае,} \end{cases} \tag{16}$$

где для простой гипотезы $\Delta_{\pm} = \mu_h \pm \sigma_h \Phi^{-1}\left(1-\alpha/2\right)$, для сложной гипотезы $\Delta_- = \mu_{S,2}^{(\varepsilon_+)} - \sigma_{S,2}^{(\varepsilon_+)} \Phi^{-1}\left(1-\alpha/2\right)$, $\Delta_+ = \mu_{S,2} + \sigma_{S,2}^{(\varepsilon_+)} \Phi^{-1}\left(1-\alpha/2\right)$; $\Phi(\cdot)$ – функция распределения стандартного нормального закона.

Для каждого значения $s = 1, \ldots, s_+$ вычислим оценку энтропии $\hat{h}(s)$, нормированные статистики $\tilde{h}_0$ и $\tilde{h}_\varepsilon$ для простой и сложной гипотез соответственно и вспомогательную статистику $\breve{h}_\varepsilon$ для вычисления двустороннего p-значения: $\tilde{h}_0 = \left(\hat{h} - \mu_h\right) \Big/ \sigma_h$, $\tilde{h}_\varepsilon = \left(\hat{S}_2 - \mu_{S,2}\right) \Big/ \sigma_{S,2}^{(\varepsilon_+)}$, $\breve{h}_\varepsilon = \left(\hat{S}_2 - \mu_{S,2}^{(\varepsilon_+)}\right) \Big/ \sigma_{S,2}^{(\varepsilon_+)}$. Формулы P-значений для простой H_0 и сложной H_0^ε гипотез равны соответственно:

$$\mathrm{P}_0 = 2\left(1 - \Phi\left(\left|\tilde{h}_0\right|\right)\right),\ \mathrm{P}_\varepsilon = \begin{cases} 2\left(1 - \Phi\left(\left|\tilde{h}_0\right|\right)\right), \text{ если } \hat{S}_2 > \mu_{S,2}, \\ 2 - \Phi\left(\left|\tilde{h}_0\right|\right) - \Phi\left(\left|\breve{h}_0\right|\right), \text{ если } \mu_{S,2}^{(\varepsilon_+)} \le \hat{S}_2 \le \mu_{S,2}, \\ 2\left(1 - \Phi\left(\left|\breve{h}_0\right|\right)\right), \text{ если } \hat{S}_2 < \mu_{S,2}^{(\varepsilon_+)}. \end{cases}$$

СТАТИСТИЧЕСКОЕ ОЦЕНИВАНИЕ УРОВНЕЙ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

Криптографические генераторы различаются по уровню ε отклонения от РРСП. Это позволяет ввести в рассмотрение различные уровни безопасности криптографических генераторов: чем больше ε, тем ниже уровень безопасности. Построенный тест (13) можно применить для статистического оценивания уровней безопасности (стойкости) криптографического генератора. Проиллюстрируем этот подход в ситуации, когда заданы $M = 3$ уровня безопасности.

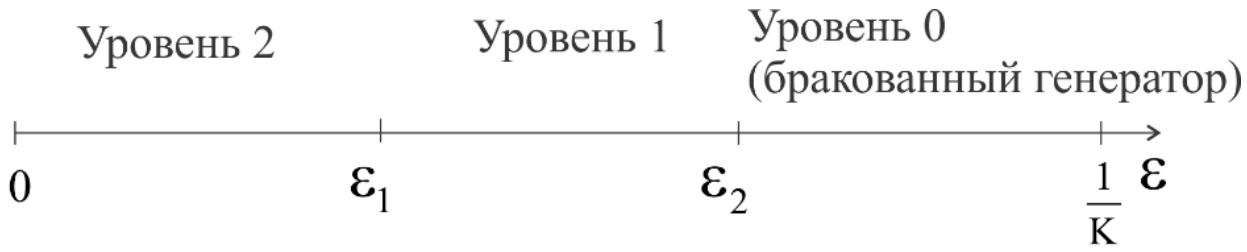

Рис. 2. Уровни безопасности генератора для $M = 3$

Здесь $0 < \varepsilon_1 < \varepsilon_2 < 1$ – два заданных критических значения допустимых отклонений $\left\| p - p^{(0)} \right\|$ распределения вероятностей s-грамм $p = \left(p_k \right)$ от равномерного распределения $p^{(0)} = \left(p_k^{(0)} \right)$. Определим вложенные сложные гипотезы $H_0^{\varepsilon_1} \subset H_0^{\varepsilon_2}$. С помощью статистического теста (13) по X_1^T последовательно проверяем пары гипотез $\left(H_0^{\varepsilon_1}, \overline{H_0^{\varepsilon_1}} \right)$ и $\left(H_0^{\varepsilon_2}, \overline{H_0^{\varepsilon_2}} \right)$. Анализируя полученные решения, находим оценки для уровня безопасности c:

$$c = \begin{cases} 2, \text{ если } d^{\varepsilon_1} = 0; \\ 1, \text{ если } d^{\varepsilon_1} = 1, d^{\varepsilon_2} = 0; \\ 0, \text{ если } d^{\varepsilon_2} = 1. \end{cases}$$

ПРОГРАММНЫЙ КОМПЛЕКС «ЭАДП»

В НИИ ППМИ БГУ разработан Программный Комплекс «Энтропийный анализ дискретных последовательностей» (ПК «ЭАДП») [12], позволяющий вычислять оценки энтропии дискретной последовательности и на основе (16) в асимптотике (15) принимать или отклонять нулевую гипотезу. ПК «ЭАДП» позволяет для заданного уровня значимости α вычислить последовательность статистик $\bar{h}(s) = \tilde{h}(s) \Big/ \left(\Phi^{-1}\left(1-\alpha/2\right) \right)$ для $s = 1, 2, \ldots, s_+$, и представлять ее в виде **графика, называемого энтропийным профилем выходной последовательности криптографического генератора** (см. рис. 3); H_0 принимается, если $\bar{h}_0(s) \in [-1; 1]$; H_0^{ε} принимается, если $\bar{h}_{\varepsilon}(s) \in \left[-1 - \varepsilon_+^2 \Big/ \left(\sigma_{S,2}^{(\varepsilon_+)} \Phi^{-1}\left(1-\alpha/2\right) \right), 1 \right]$.

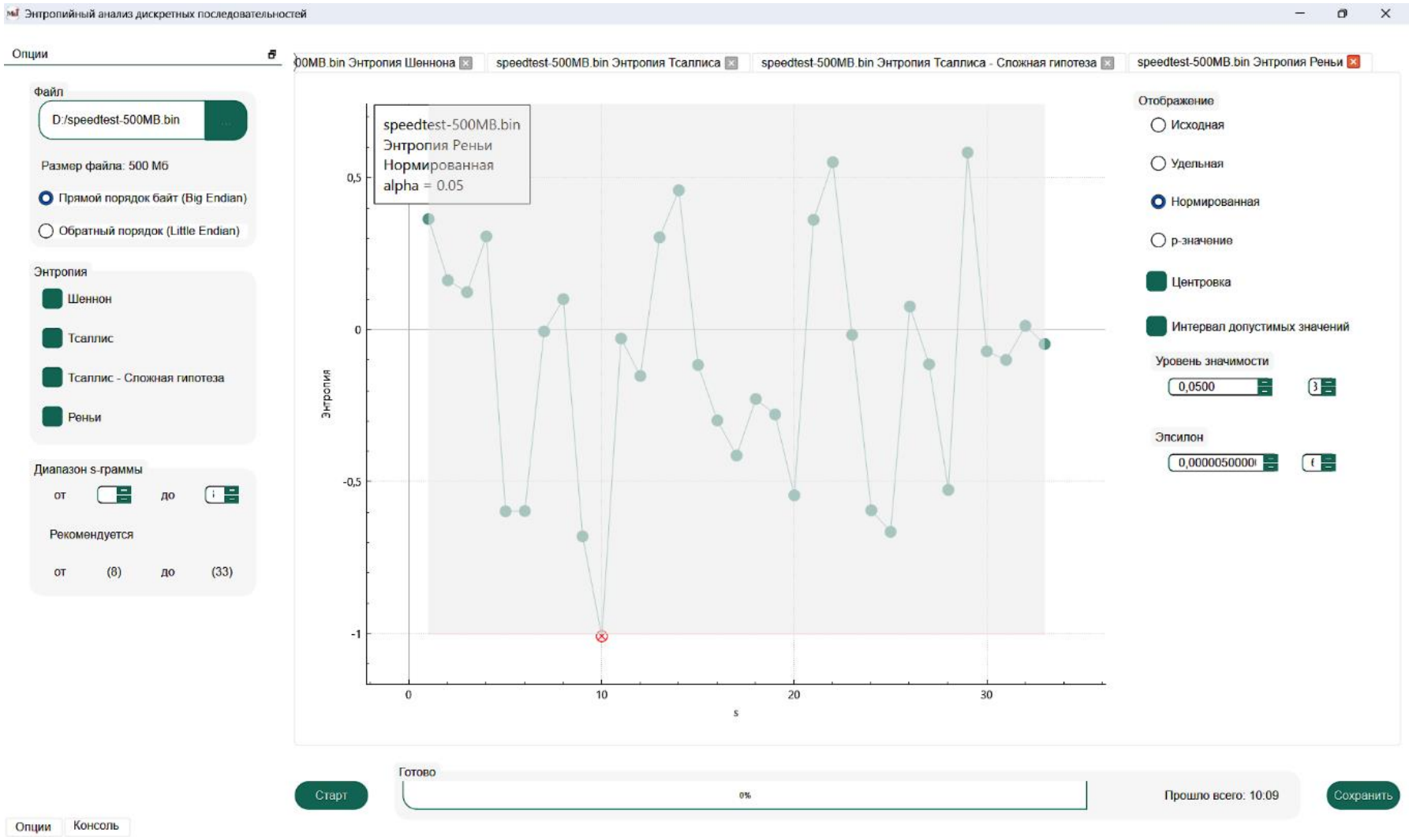

Рис. 3. Энтропийный профиль физического генератора

ЭКСПЕРИМЕНТЫ ПО ОЦЕНКЕ СТАТИСТИЧЕСКИХ ТЕСТОВ ДЛЯ СЛОЖНЫХ ГИПОТЕЗ

Для иллюстрации работоспособности построенного теста (13) при $s = 8$ (тестирование байтовой равномерности), $K = 2^s = 256$, $\varepsilon = 0.9 / K = 0.00352$ имитировалось по 100 реализаций двоичной последовательности (1) – (5) для $T \in \left\{2^{19},\ 2^{20}\right\}$, $\alpha_0 = 0.05$. Графики зависимости оценки вероятности принятия альтернативы $\hat{P}_1$ от $\left\| p - p^{(0)} \right\|$ представлены на рис. 4, 5 соответственно.

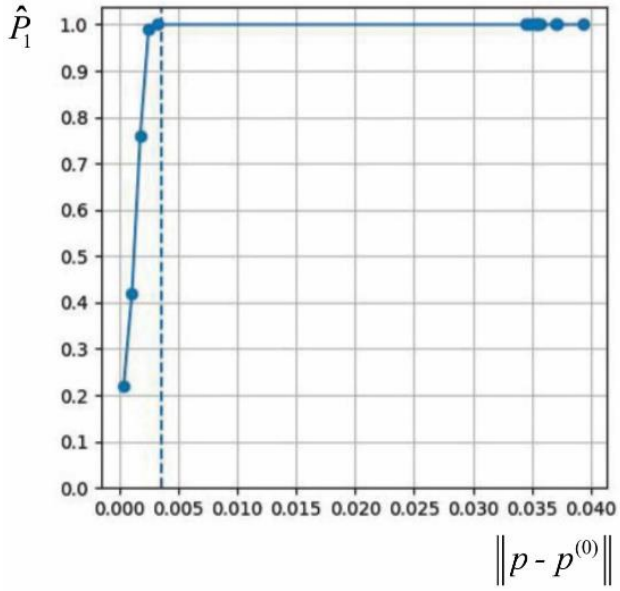

Рис. 4. Случай $T = 2^{19}$

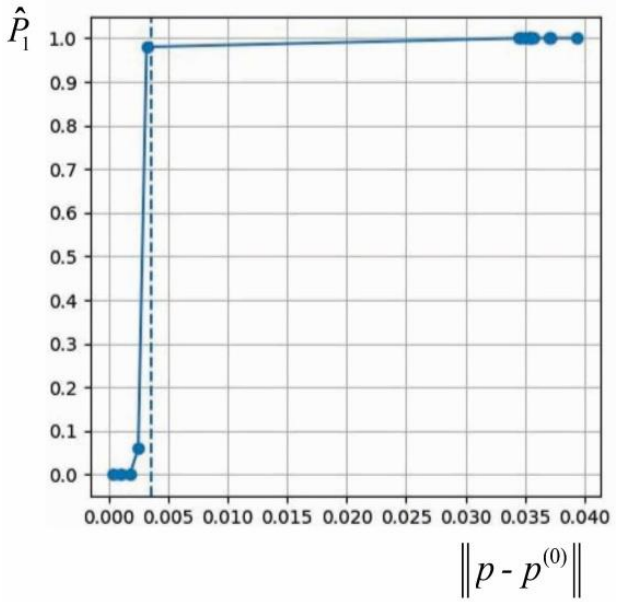

Рис. 5. Случай $T = 2^{20}$

Рис. 4, 5 иллюстрируют состоятельность построенного решающего правила (13). Видно также, что при увеличении длительности T последовательности X график зависимости $\hat{P}_1$ от $\left\|p - p^{(0)}\right\|$ приближается к ступенчатой функции со ступенькой в точке $\left\|p - p^{(0)}\right\| = \varepsilon$: при $\left\|p - p^{(0)}\right\| < \varepsilon$ величина $\hat{P}_1 < \alpha_0$, а при $\left\|p - p^{(0)}\right\| > \varepsilon$ величина $\hat{P}_1$ приближается к единичному значению.

ЭКСПЕРИМЕНТЫ ПО ОЦЕНКЕ УРОВНЕЙ БЕЗОПАСНОСТИ

Для иллюстрации подхода при $M = 3$ проведена следующая серия экспериментов. Рассматривались 3 генератора: № 1 (физический генератор [13]), № 2 (физический генератор), № 3 (псевдослучайный генератор из раздела 2.4 [14]). Длины последовательностей равны соответственно $125 \cdot 2^{20}$, $9999 \cdot 2^{10}$, 16776402; элементы последовательностей имеют длину 4 байта, т.е. $s = 32$ ($K = 2^{32}$). Уровни безопасности заданы следующим образом: $\varepsilon_1 = 7 \cdot 10^{-7}$, $\varepsilon_2 = 10^{-6}$. С помощью ПК «ЭАДП» были вычислены оценки энтропии Тсаллиса и границы интервалов допустимых значений для сложных нулевых гипотез при $\alpha = 0,05$. Результаты приведены в таблице 3.

Таблица 3 – Результаты оценивания уровня безопасности

№	$1-\hat{h}$	$1-\Delta_{-}^{\varepsilon_1}$	$1-\Delta_{+}^{\varepsilon_1}$	$1-\Delta_{-}^{\varepsilon_2}$	$1-\Delta_{+}^{\varepsilon_2}$	Оценка уровня безопасности c
1	$2,328\cdot10^{-10}$	$2,337\cdot10^{-10}$	$2,325\cdot10^{-10}$	$2,343\cdot10^{-10}$	$2,324\cdot10^{-10}$	2
2	$2,276\cdot10^{-10}$	$2,376\cdot10^{-10}$	$2,286\cdot10^{-10}$	$2,381\cdot10^{-10}$	$2,285\cdot10^{-10}$	0
3	$2,360\cdot10^{-10}$	$2,359\cdot10^{-10}$	$2,303\cdot10^{-10}$	$2,365\cdot10^{-10}$	$2,301\cdot10^{-10}$	1

ЗАКЛЮЧЕНИЕ

1. Представлен новый подход к статистическому тестированию, в котором нулевая гипотеза предполагается сложной и допускает отклонения распределения вероятностей s-грамм от равномерного, не превышающие некоторого фиксированного уровня ε. Построены статистические тесты отношения правдоподобия и на основе энтропийных функционалов Шеннона, Реньи и Тсаллиса.

2. Разработан подход к статистическому оцениванию уровня безопасности (стойкости) криптографического генератора на основе статистического тестирования его выходных последовательностей с использованием сложных нулевых гипотез. Предложен алгоритм статистического оценивания уровня безопасности криптографического генератора по M-значной шкале, основанный на $(M-1)$-кратном использовании теста (13) или (16).

3. Теоретические результаты проиллюстрированы результатами компьютерных экспериментов.

СПИСОК ЛИТЕРАТУРЫ

1. Алферов, А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин [и др.]. – М.: Гелиос АРВ, 2005. – 480 с.

2. Харин, Ю. С. Криптология / Ю. С. Харин, С. В. Агиевич, Д. В. Васильев [и др.]. – Минск: БГУ, 2023. – 512 с.

3. NIST SP 800-22: Download Documentation and Software. – URL: https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software.

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

5. Decision to Revise NIST SP 800-22 Rev. 1a. – URL: https://csrc.nist.gov/news/2022/decision-to-revise-nist-sp-800-22-rev-1a.

6. Савелов, М. П. Предельное совместное распределение статистик критериев пакета NIST “Monobit Test”, “Frequence Test within a Block”

и обобщения критерия “Approximate Entropy Test” / М. П. Савелов // Дискретная математика. – 2023. – Т. 35, № 2. – С. 93–108.

7. Serov, A. A. Reliability of two-level testing approach of the NIST test suite / A. A. Serov // Computer data analysis and modeling: stochastics and data science: Proceedings of the XIV international Conference, September 24–27, 2025. – Minsk: BSU, 2025. – P. 240–243.

8. Харин, Ю. С. О статистической проверке сложных гипотез об s-мерном равномерном распределении вероятностей двоичных последовательностей / Ю. С. Харин, А. М. Зубков // Дискретная математика. – 2024. – Т. 36, № 1. – С. 116-135.

9. Ивченко, Г. И. Математическая статистика / Г. И. Ивченко, Ю. И. Медведев. – М.: Высшая школа, 1992. – 304 с.

10. Палуха, В. Ю. Статистические оценки энтропии Реньи и Тсаллиса и их использование для проверки гипотез о «чистой случайности» / В. Ю. Палуха, Ю. С. Харин // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. – 2016. – № 2. – С. 37-47.

11. Палуха, В. Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности / В. Ю. Палуха // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. – 2017. – № 1. – С. 79-88.

12. Палуха, В. Ю. Статистическое тестирование равномерности дискретного распределения вероятностей на основе энтропии Тсаллиса / В. Ю. Палуха, Ю. С. Харин // Дискретная математика. – 2024. – Т. 36, № 4. – С. 101-116.

13. speedtest-500MB.bin [Electronic resource] // Humboldt Berlin University, Faculty of Mathematics and Natural Sciences, Department of Physics. – URL: http://qrng.physik.hu-berlin.de/files/speedtest-500MB.bin.

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

СПАСИБО ЗА ВНИМАНИЕ!