4. *Provos, N.* Defending against statistical steganalysis / N. Provos // Proc. of the 10 USENIX Security Simposium. – 2001. – P.~323–325.

5. *Sallee, P.* Model-based methods for steganography and steganalysis / P. Sallee // International Journal of Image and Graphics. – 2005. – Vol.~5~(1). – P. 167–190.

6. *Westfeld, A. A.* High capacity despite better steganalysis (F5 – a steganographic algorithm) / A. A. Westfeld // Lecture Notes in Computer Science. – 2001. – Vol.~2137. – P.~289–302.

ЭНТРОПИЙНЫЕ ХАРАКТЕРИСТИКИ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В КРИПТОГРАФИИ

В. Ю. ПАЛУХА, Ю. С. ХАРИН

Современные средства криптографической защиты информации используют генераторы случайных и псевдослучайных последовательностей. Стойкость криптосистем зависит от того, насколько близка генерируемая последовательность по своим свойствам к равномерно распределённой случайной последовательности (РРСП). Одним из подходов к оценке качества генератора является статистическое оценивание энтропии и сравнение полученной оценки с ожидаемым значением для РРСП. Существуют различные функционалы энтропии, например, в [1] приводятся 23 функционала. Наибольшее распространение имеет энтропия Шеннона, которая и рассматривается в данной статье.

Статистическая оценка энтропии. Будем рассматривать стационарные в узком смысле двоичные последовательности $\{x_t\} \in V = \{0,1\}$ на некотором вероятностном пространстве (Ω, *F*, *P*). Пусть $p_{i_1,\dots,i_s} = P\{x_{t+1} = i_1, \dots, x_{t+s} = i_s\}$ – распределение вероятностей *s*-граммы $(x_{t+1},\dots,x_{t+s}) \in V_s$, которое не зависит от $t \in \mathrm{N}_0 = \mathrm{N} \cup \{0\}$. Многомерная (*s*-мерная) энтропия Шеннона для фрагмента длины $s \geq 1$ согласно [2] имеет вид

$$H\{x_1,\dots,x_s\} = h(s) = -\sum_{i_1,\dots,i_s \in V} p_{i_1,\dots,i_s} \ln p_{i_1,\dots,i_s}.$$

Пусть наблюдается n фрагментов длины s: $X^{(k)} = (x_1^{(k)},\dots,x_s^{(k)}) \in V_s, \quad k = 1,\dots,n$, сформированных из элементов последовательности $\{x_t\}$. Построим частотную оценку вероятности $p_J(s) = P\{X^{(k)} = J_1^s\}$, где $J_1^s = (j_1,\dots,j_s) \in V_s$ – мультииндекс, по n фрагментам длины $s \geq 1$:

$$\hat{p}_J(s) = \frac{v_J}{n}, \quad v_J = \sum_{k=1}^{n} \delta_{X^{(k)},J}, \quad \delta_{X^{(k)},J} = \begin{cases} 1, X^{(k)} = J; \\ 0, X^{(k)} \neq J \end{cases}$$

и затем построим оценку *s*-мерной энтропии по «подстановочному» принципу

$$\hat{h}(n,s) = -\sum_{J \in V_s} \hat{p}_J(s) \ln \hat{p}_J(s). \qquad (1)$$

Распределение вероятностей статистической оценки многомерной энтропии описывается следующей теоремой, которая опирается на результаты, полученные в [3].

Теорема. При истинной гипотезе H_* = {{x_t} есть РРСП} статистическая оценка *s*-мерной энтропии (1), построенная по подстановочному принципу, в специальной асимптотике $n, N = 2^s \to \infty, \quad n/N \to \lambda, \quad 0 < \lambda < \infty$, имеет асимптотически нормальное распределение: $\hat{h}(n,s) \sim N(\mu, \sigma^2)$, где для параметров асимптотического распределения справедливы следующие формулы

$$\mu = \ln n - e^{-\lambda}\sum_{k=1}^{+\infty}\frac{\ln(k+1)\lambda^k}{k!}, \qquad (2)$$

$$\sigma^2 = \frac{e^{-\lambda}}{n}\sum_{k=1}^{+\infty}\frac{(k+1)\lambda^k}{k!}\ln^2(k+1) - \frac{e^{-2\lambda}}{2^s}\left(\sum_{k=1}^{+\infty}\frac{\ln(k+1)\lambda^k}{k!}\right)^2 - \frac{e^{-2\lambda}}{n}\left(\sum_{k=1}^{+\infty}\ln(k+1)\frac{\lambda^k}{k!}(k+1-\lambda)\right)^2.$$

Способы построения оценки. Опишем несколько способов построения оценки энтропии в зависимости от способа формирования $\{X^{(k)}\}$, а также поведение последовательности оценок энтропии для каждого из способов.

В первом случае будем строить частотные оценки по пересекающимся фрагментам. Пусть наблюдается последовательность $x_1, \ldots, x_T \in V$. «Зациклим» последовательность до длины $T + s - 1$: $x_{T+1} = x_1$, ..., $x_{T+s-1} = x_{s-1}$. Тогда $X^{(k)} = (x_1^{(k)}, \ldots, x_s^{(k)}) = (x_k, \ldots, x_{k+s-1}) \in V_s$, $k = 1, \ldots, T$, $n = T$. При фиксированном $T = n$ с ростом s получаем $E_{H_*}\{\hat{h}(T, s)\} \sim \ln T$, поскольку второе слагаемое в (2) стремится к нулю, так как $\lambda \to 0$. Для данного случая в [4] также дана формула для вычисления математического ожидания оценки, однако она более громоздкая, чем (2). На рис. 1 представлены последовательность значений математического ожидания оценки энтропии для $T = 2^{33}$ (жирная линия) и прямая $y = s\ln 2$, которая отображает истинные значения энтропии, которые бы наблюдались в случае бесконечной последовательности.

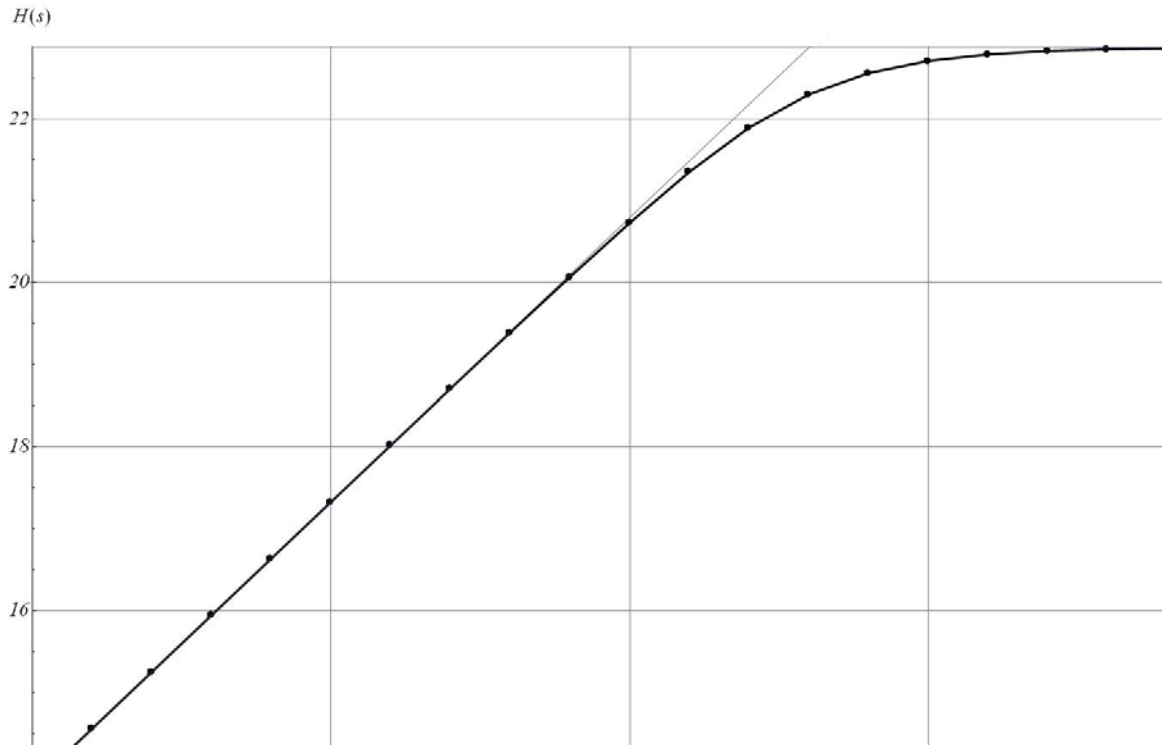

Рис. 1. **Последовательность оценок энтропии по пересекающимся фрагментам**

Во втором случае будем строить частотные оценки по непересекающимся фрагментам. Сначала рассмотрим построение оценки по соседним фрагментам длины s. Пусть, как и в первом случае, наблюдается последовательность $x_1, \ldots, x_T \in V$. Тогда $X^{(k)} = (x_1^{(k)}, \ldots, x_s^{(k)}) = (x_{(k-1)s+1}, \ldots, x_{ks}) \in V_s$, $k = 1, \ldots, n$, $n = \lfloor T/s \rfloor$. Если T не кратно s, то для удобства отбросим последние элементы последовательности и положим $n = T/s$. Получим $\ln n = \ln T - \ln s$. Поэтому при фиксированном T с ростом s число наблюдаемых

фрагментов n будет уменьшаться, а второе слагаемое в (2) стремиться к нулю, так как $\lambda \to 0$, и, следовательно, математическое ожидание оценки (1) сначала будет расти, приближаясь к значению $\ln T$ (но не достигая его), а затем постепенно уменьшаться до 0. Последовательность математических ожиданий оценки энтропии для $T = 2^{33}$ (жирная линия) и прямая $y = s\ln 2$ представлены на рисунке 2.

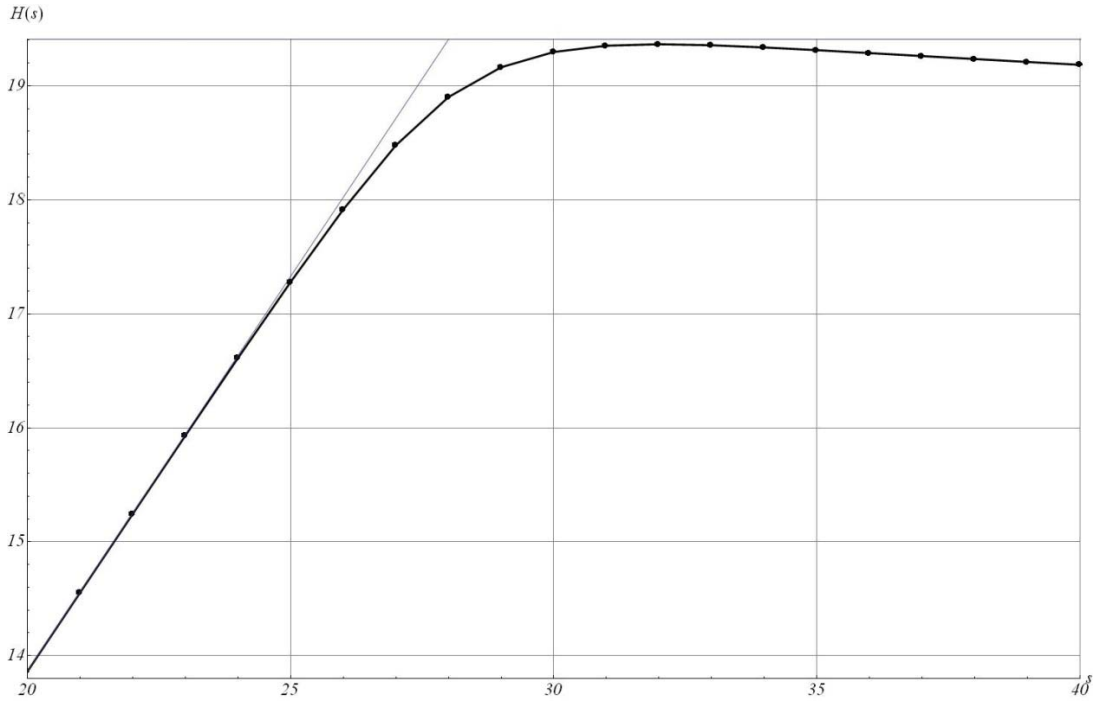

Рис. 2. **Последовательность оценок энтропии по непересекающимся фрагментам**

В третьем случае последовательность $x_1, \ldots, x_T \in V$ разделена на блоки длины S. Таким образом, например, формируются гаммы блочных алгоритмов шифрования. Практическую значимость будут иметь оценки энтропии, построенные по фрагментам, лежащим внутри блоков. Итак, пусть наблюдаемая последовательность состоит из $n = T/S$ блоков длины S: $X^{(k)} = (x_1^{(k)}, \ldots, x_S^{(k)}) = (x_{(k-1)S+1}, \ldots, x_{kS}) \in V_S, \quad k = 1, \ldots, n$. Будем строить статистическую оценку энтропии (1) по фрагментам длины $s \le S$: $\tilde{X}^{(k)} = (x_1^{(k)}, \ldots, x_s^{(k)}) = (x_{(k-1)S+1}, \ldots, x_{(k-1)S+s}) \in V_s, \quad k = 1, \ldots, n$. В этом случае при фиксированном T с ростом s число наблюдаемых фрагментов n будет постоянным, второе слагаемое в (2) стремится к нулю, так как $\lambda \to$, и математическое ожидание оценки (1) будет эквивалентно $\ln n$. Поведение последовательности математических ожиданий оценок энтропии будет аналогично первому случаю, отличие будет заключаться в величине n.

Построение последовательностей оценок энтропии является одним из подходов к оценке качества криптографического генератора. Сравнение построенных по выходной последовательности генератора статистических оценок энтропии Шеннона с их математическим ожиданием для РРСП позволяет сделать выводы о близости выходной последовательности генератора по своим свойствам к чисто случайной последовательности.

Список использованных источников

1. *Esteban, M. D.* A summary on entropy statistics / M. D. Esteban, D. Morales // Kybernetika. – 1995. – Vol. 31, № 4. – P. 337–346.

2. Криптология / Ю. С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.

3. *Holst, L.* Asymptotic normality and efficiency for certain goodness-of-fit tests / L. Holst // Biometrika. – 1972. – № 59. – P. 137–145.

4. *Палуха, В. Ю.* О вероятностных свойствах статистической оценки многомерной энтропии Шеннона / В. Ю. Палуха, Ю. С. Харин // Теория вероятностей, случайные процессы, математическая статистика и приложения: материалы междунар. науч. конф., Минск, 23–26 фев. 2015 г. – Минск: РИВШ, 2015. – С. 236–241.

МЕСТО И РОЛЬ ДИСЦИПЛИН ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ ИНЖЕНЕРНЫХ КАДРОВ В БНТУ

В. Ф. ГОЛИКОВ

Широкое использование информационных технологий позволяет эффективно решать многие задачи в различных сферах человеческой деятельности. Вместе с тем многопользовательский характер информационных систем, открытость информационных ресурсов не исключают преднамеренные или непреднамеренные действия над ними. Поэтому вопросы подготовки кадров, использующих информационные технологии и системы, в области информационной безопасности являются актуальными.

Белорусский национальный технический университет – крупнейшее учебное заведение Республики Беларусь – ежегодно выпускает тысячи специалистов инженерного профиля. При этом студенты практически любой специальности используют компьютерные технологии в своей области деятельности. Начальные знания в области информационной безопасности многие из них получают в дисциплинах по компьютерным технологиям на младших курсах, а более профессиональные – на старших курсах. Так, студенты первой ступени высшего образования специальностей 1-40 01 01 «Программное обеспечение информационных технологий», 1-40 01 02 «Информационные системы и технологии», 1-53 01 02 «Автоматизированные системы обработки информации» изучают основные методы и средства защиты информации в курсе «Защита информационных ресурсов компьютерных систем и сетей». Основное внимание в нем уделяется рассмотрению методов защиты от несанкционированного доступа к информации в компьютерных сетях с помощью программных и аппаратно-программных средств, базирующихся на криптографических преобразованиях; угроз в коммуникационных сетях и мер по предотвращению попыток реализации этих угроз, а также методов симметричного шифрования, криптографии с открытыми ключами, хэш-функций, основ построения и использования межсетевых экранов, практических вопросов сетевой безопасности, методов обеспечения надежного хранения информации в компьютерных сетях.

В результате освоения дисциплины студент должен

знать:

- особенности компьютерных систем как объекта защиты;
- основные методы защиты информации в компьютерных системах;
- основные криптографические алгоритмы;

уметь:

- выбирать и использовать средства защиты информации в компьютерных системах;
- проектировать средства защиты для информационных систем и оценивать уровень их безопасности.

Задача дисциплины «Защита информационных ресурсов компьютерных систем и сетей» состоит в получении студентами основных теоретических знаний по защите информации от несанкционированного доступа к информации в компьютерных се-