

Научная статья

УДК 004.056.

DOI:10.31854/1813-324X-2022-8-3-117-126



# Модификация алгоритма обнаружения сетевых атак методом фиксации скачков фрактальной размерности в режиме online

Олег Иванович Шелухин<sup>1</sup>, sheluhin@mail.ru

Сергей Юрьевич Рыбаков<sup>1✉</sup>, svolkov97@gmail.com

Анна Вячеславовна Ванюшина<sup>1</sup>, a.v.vaniushina@mtuci.ru

<sup>1</sup>Московский технический университет связи и информатики,  
Москва, 111024, Российская Федерация

**Аннотация:** В работе рассматривается модификация алгоритма обнаружения аномалий в сетевом трафике при использовании текущих оценок скачка фрактальной размерности в режиме реального времени. Модификация алгоритма заключается в дополнительной пороговой обработке (трешолдинге) полученных оценок фрактальной размерности и последующей вторичной фильтрации. Показано, что фильтрация с применением процедуры трешолдинга позволяет повысить точность текущей оценки фрактальной размерности и увеличить достоверность обнаружения аномалии в сетевом трафике в режиме online.

**Ключевые слова:** показатель Херста, фрактальный анализ, фрактальный гауссовский шум, кратномасштабный анализ, трешолдинг, скользящее окно

**Ссылка для цитирования:** Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Модификация алгоритма обнаружения сетевых атак методом фиксации скачков фрактальной размерности в режиме online // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 117–126. DOI:10.31854/1813-324X-2022-8-3-117-126

## Modified Algorithm for Detecting Network Attacks Using the Fractal Dimension Jump Estimation Method in Online Mode

Oleg Sheluhin<sup>1</sup>, sheluhin@mail.ru

Sergey Rybakov<sup>1✉</sup>, svolkov97@gmail.com

Anna Vanyushina<sup>1</sup>, a.v.vaniushina@mtuci.ru

<sup>1</sup>Moscow Technical University of Communications and Informatics,  
Moscow, 111024, Russian Federation

**Abstract:** The paper considers a modification of the well-known algorithm for detecting anomalies in network traffic using a real-time fractal dimension jump estimation method. The modification uses real-time thresholding to provide additional filtering of the estimated fractal network traffic dimension. The accuracy of the current estimate of the fractal dimension and the reliability of anomaly detection in network traffic in online mode is improved by adding extra filtering to the algorithm.

**Keywords:** Hurst exponent, fractal analysis, fractal Gaussian noise, multiresolution analysis, thresholding, sliding window

**For citation:** Sheluhin O., Rybakov S., Vanyushina A. Modified Algorithm for Detecting Network Attacks Using the Fractal Dimension Jump Estimation Method in Online Mode. *Proc. of Telecom. Universities.* 2022;8(3): 117–126. (in Russ.) DOI:10.31854/1813-324X-2022-8-3-117-126

## Введение

Обеспечение сетевой безопасности в условиях воздействия сетевых атак является важной проблемой современных систем связи. Проблема обнаружения (поиска) аномалий в сетевом трафике обусловлена несовершенством математического аппарата или алгоритма системы обеспечения информационной безопасности. Большая часть из известных алгоритмов и методов достаточно трудны в программной реализации и имеют ряд недостатков, связанных с недостоверным определением момента начала аномалии.

В работах [1–3] доказано, что сетевой трафик обладает свойствами самоподобия. Учитывая то, что любая атака или аномальная активность в сети может привести к резкому изменению текущего значения фрактальной размерности, данное свойство можно использовать для точного определения момента начала атаки или аномалии. Фрактальный анализ основан на выявлении несвойственных для нормального сетевого трафика структурных особенностей при помощи кратномасштабного анализа и оценки показателя Херста, который однозначно связан с фрактальной размерностью Хаусдорфа  $D_f$  соотношением  $D_f = 2 - H$ .

В работах [4, 5, 6] получены алгоритмы обнаружения сетевых атак на основе анализа скачков фрактальной размерности при резких изменениях свойств сетевого трафика. Однако полученные при этом алгоритмы не являются итеративными, что усложняет использование их в процессе обработки. Кроме того, наблюдаемые при этом флуктуации текущего показателя Херста  $H$  могут рассматриваться как дополнительный шум обработки, что также снижает эффективность таких алгоритмов.

В отличие от известных работ предлагается модифицировать алгоритм обработки путем дополнительной фильтрации текущих оценок  $H$ , что позволяет повысить точность текущей оценки фрактальной размерности, а также достоверность обнаружения аномалии в сетевом трафике в режиме online.

## Кратномасштабный анализ

Как известно [7–9], любую последовательность дискретных отсчетов при конечном числе уровней разложения  $P$  анализируемого процесса  $y(t_i)$  по системе масштабирующих функций и вейвлет-функций можно представить в виде упорядоченной совокупности коэффициентов вейвлет-декомпозиции (разложения):

$$y(t_i) = \sum_{k=1} a_{m,k} \Phi_{m,k}(t_i) + \sum_{m=1} \sum_{k=1} d_{m,k} \Psi_{m,k}(t_i), \quad (1)$$

$m, k \in I,$

где  $\Phi_{m,k}(t_i)$  – базисная масштабирующая функция;  $\Psi_{m,k}(t_i)$  – материнский вейвлет;  $a_{m,k}, d_{m,k}$  – коэффициенты аппроксимации и детализации анализируемого процесса;  $m, k$  – параметры масштаба и сдвига в пространстве целых чисел  $I$ .

Для того, чтобы адаптировать соотношение (1) к обработке сигнала в режиме реального времени, необходимо фиксировать длительность скользящего окна размером  $M$ .

Выполняя дискретное вейвлет-преобразование (ДВП) анализируемого процесса внутри скользящего окна размером в  $M$  отсчетов, в каждый момент времени  $t_i$ , будет получен набор коэффициентов аппроксимации  $\{a_{1x}, a_{2x}, a_{3x}, \dots, a_{nx}\}_{t,j}$  и детализации  $\{d_{1x}, d_{2x}, d_{3x}, \dots, d_{nx}\}_{t,j}$  на каждом уровне декомпозиции  $j$ . Причем количество вейвлет-коэффициентов  $n$  на уровне  $j$  в окне  $M$  будет определяться выражением  $n = \frac{M}{2^j}$ . Таким образом, в соответствии с положениями вейвлет-анализа [9] временной ряд  $y(t)$  может быть представлен в виде:

$$y(t) = y_j(t) + \sum_{j=1}^J D_j(t), \quad (2)$$

где  $y_j(t) = \sum_{k=0}^{n_0-1} a_{j,k} \Phi_{j,k}(t)$  – функция первичной аппроксимации, которая соответствует масштабу  $J$  ( $J < J_{\max}$ );  $a_{j,k} = \langle y(t), \Phi_{j,k} \rangle$  – масштабный коэффициент аппроксимации, который равен скалярному произведению исходного ряда  $y(t)$  и масштабной функции «самого грубого» масштаба  $J$ , смещенной на  $k$  единиц масштаба вправо от начала координат;  $D_j(t) = \sum_{k=0}^{n_0-1} d_{j,k} \Psi_{j,k}(t)$  – функция детализации  $j$ -го масштаба;  $d_{j,k} = \langle y(t), \Psi_{j,k} \rangle$  – вейвлет-коэффициент детализации масштаба  $j$ , равный скалярному произведению исходного ряда  $y(t)$  и вейвлета масштаба  $j$ , смещенного на  $k$  единиц масштаба вправо от начала координат;  $n_0 = 2^{J_{\max}}$ , ( $n_0 \leq N$ );  $J_{\max} = \lfloor \log_2 N \rfloor$  – максимальное количество уровней разложения;  $\lfloor \log_2 N \rfloor$  – целая часть числа.

## Метод оценки скачка фрактальной размерности

Пусть декомпозиция дискретного случайного процесса  $X(t_i)$ , который определен на интервале  $i = 1, \dots, N$ , осуществляется в скользящем окне размера  $M$ . В результате движения окна анализа «пробежит»  $m$  положений, где  $m = 1, \dots, N - M$ . Тогда детализирующие коэффициенты при  $m$ -ом положении окна анализа  $d_{j,k}^m$  будут вычислены в конце анализируемого интервала.

В соответствии с уравнением (3) для получения текущей оценки показателя Херста  $\hat{H}_m$  при  $m$ -ом положении окна анализа необходимо выполнить линейную регрессию на шкале  $j$  в диапазоне  $[j_1, j_2]$ :

$$\log_2(\mu_{j,m}) = \log_2\left(\frac{1}{n_j} \sum_k |d_x^{(m)}(j,k)|^2\right) = (2\hat{H}_m - 1)_j + \hat{c} = a_m j + \hat{c}, \text{ где } \hat{c} = \text{const.} \quad (3)$$

Формула (3) позволяет оценить показатель Херста  $\hat{H}_m$  процессов с долговременной зависимостью в виде линейной зависимости. Это значит, что, если процесс  $X(t_i)$  является долговременно зависимым процессом с показателем Херста  $H_m$ , то график зависимости  $\log_2(\mu_{j,m})$  от  $j$  имеет линейный наклон  $2\hat{H}_m - 1$ , и масштабный показатель  $\hat{a}_m = (2\hat{H}_m - 1)$  может быть получен путем оценки наклона графика функции  $\log_2(\mu_{j,m})$  от  $j$  при каждом  $m$ -ом положении окна анализа.

Для получения взвешенной оценки масштабного показателя  $\hat{a}_m$  на интервале  $[j_1, j_2]$  при  $m$ -ом положении окна анализа необходимо проделать следующие вычисления:

$$\hat{a}_m = \sum_j w_j y_{j,m}, \quad (4)$$

$$\hat{c}_m = \sum_j v_j y_{j,m}, \quad (5)$$

$$w_j = \frac{S_j - S_1}{(SS_2 - S_1^2)\sigma_j^2} \quad (6)$$

$$y_{j,m} = \log_2(\mu_{j,m}) - g(j), \quad (7)$$

$$g(j) = \psi\left(\frac{n_j}{2}\right) \ln 2 - \log_2\left(\frac{n_j}{2}\right) = \frac{\Gamma'\left(\frac{n_j}{2}\right)}{\Gamma\left(\frac{n_j}{2}\right) \ln 2} - \log_2\left(\frac{n_j}{2}\right) \sim -\frac{1}{n_j \ln 2}, \quad (8)$$

$$\sigma_j^2 = \frac{\xi(2, \frac{n_j}{2})}{\ln^2 2} \sim \frac{2}{n_j \ln^2 2}, \quad (9)$$

$$v_j = \frac{S_2 - jS_1}{(SS_2 - S_1^2)\sigma_j^2}, \quad (10)$$

$$S = \sum_{j=j_1}^{j_2} 1/\sigma_j^2, \quad S_1 = \sum_{j=j_1}^{j_2} j/\sigma_j^2, \quad S_2 = \sum_{j=j_1}^{j_2} j^2/\sigma_j^2, \quad (11)$$

где  $\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt$  - гамма-функция;  $\Gamma'$  - ее производная;  $\xi(2, z) = \sum_0^\infty 1/(z+n)^2$  - обобщенная зета-функция Римана;  $\psi(x) = \Gamma'(x)/\Gamma(x)$  - пси-функция (или дигамма-функция);  $n_j$  - количество детализирующих коэффициентов на соответствующем уровне вейвлет-разложения ( $j$ ).

Так, определив квантили  $S, S_1$  и  $S_2$  и получив взвешенную оценку  $\hat{a}$  для  $a$ :

$$\hat{a} = \frac{\sum_{j=j_1}^{j_2} y_{j,m} (S_j - S_1) / \sigma_j^2}{SS_2 - S_1^2}, \quad (12)$$

которая является не смещенной на интервале  $[j_1, j_2]$ .

Вычисление текущего значения показателя Херста  $\hat{H}_m$  при  $m$ -ом окне анализа описывается следующей формулой:

$$\hat{H}_m = \frac{1 + \hat{a}_m}{2}, \quad m = \overline{1, M}. \quad (13)$$

Используя формулы (4-12), можно преобразовать соотношение (13) для оценки параметра Херста в  $m$ -положении скользящего окна в следующий вид:

$$\hat{H}_m = \frac{1}{2} \left[ \frac{\sum_{j=j_1}^{j_2} S_j \eta_{j,m} - \sum_{j=j_1}^{j_2} S_j j \sum_{j=j_1}^{j_2} S_j j \eta_{j,m}}{\sum_{j=j_1}^{j_2} S_j \sum_{j=j_1}^{j_2} S_j j^2 - \left(\sum_{j=j_1}^{j_2} S_j j\right)^2} + 1 \right], \quad (14)$$

где  $\eta_{j,m} = \log_2\left(\frac{1}{n_j} \sum_k |d_x^{(m)}(j,k)|^2\right)$ , и весовой коэффициент  $S_j = (n \ln^2 2) / 2^{j+1}$  является обратной функцией теоретической асимптотической дисперсии.

### Вторичная фильтрация оценки показателя Херста

На практике при использовании оценки показателя Херста в скользящем окне возникает проблема правильного обнаружения аномалий, т. к. оценка получается с высокой дисперсией и резкими скачками  $H$ . Это можно заметить на рисунке 1. Для нейтрализации резких выбросов и уменьшения дисперсии предлагается воспользоваться процедурой трешолдинга (*от англ. Thresholding*) - пороговой обработкой данных [10, 11].

Пусть  $\hat{H}(t_m)$  - оценка показателя Херста, определенная на интервале  $m = 1, \dots, L$ , а фильтрация полученной оценки производится с применением прямого дискретного вейвлет-преобразования в скользящем окне размера  $L$ . Смещение окна фильтрации производится с некоторым шагом  $s \leq L$ . Так при смещении слева-направо окно фильтрации «пробежит»  $z$  положений  $Z = L/s, z = 1, \dots, Z$ .

Тогда формула для фильтрации по вейвлет коэффициентам с применением трешолдинга примет следующий вид:

$$\tilde{H}(t_m) = \sum_{l=1}^{L_0} a_{j_0,l}^{(H)} \phi_l^{(H)}(t_m) + \sum_{j=1}^J \sum_{l=1}^{L_j} T(d_{j,l}^{(H)}) \psi_{j,l}^{(H)}(t_m), \quad (15)$$

где  $a_{j_0,l}^{(H)}, d_{j,l}^{(H)}$  - аппроксимирующие и детализирующие коэффициенты оценки показателя Херста при  $z$ -ом положении окна фильтрации;  $T(d_{j,l}^{(H)})$  - фильтрованные детализирующие вейвлет-коэффициенты;  $a_{j_0,l}^{(H)} = < \hat{H}(t_m), \phi_l^{(H)} >$  - аппроксимирующие вейвлет-коэффициенты;  $d_{j,l}^{(H)} = < \hat{H}(t_m), \psi_{j,l}^{(H)} >$  - детализирующие вейвлет-коэффициенты;  $L_0 = 2^{j_{\max}}, (L_0 \leq L)$ ;  $J_{\max} = \lceil \log_2 L \rceil$  - максимальное число масштабов разложения;  $\lceil \log_2 L \rceil$  - целая часть числа.

Наибольшее распространение получили следующие виды трешолдинга [7, 12, 13]:

- жесткий трешолдинг –  $T_h = d_{j,l}^{(H)} I(|d_{j,l}^{(H)}| > \tau)$ ;
- мягкий трешолдинг –  $T_s = \text{sign}(d)(|d_{j,l}^{(H)}| - \tau) \times I(|d_{j,l}^{(H)}| \geq \tau)$ .

В исследовании использовался жесткий трешолдинг.

Алгоритм формирования оценки после вторичной фильтрации выглядит следующим образом:

- 1) фильтрация производится в окне размером  $L$ ;
- 2) производится 6-уровневое ДВП накопленной оценки показателей Херста  $\tilde{H}(t_m)$ ;
- 3) происходит удаление всех детализирующих вейвлет-коэффициентов  $d_{j,l}^{(H)}$ ;
- 4) применяется обратное ДВП.

В результате вторичной фильтрации формируется оценка без аномальных выбросов.

### Тестирование алгоритма

Для тестирования работоспособности описанного алгоритма, путем моделирования формировался фрактальный гауссовский шум (ФГШ) [14–18] длиной в 300 000 отсчетов с меняющимся показателем Херста в пределах [0,55 : 0,95]. Размер скользящего окна  $M = 1000$ .

Структура моделируемого трафика представлена в таблице 1. В результате имитации был смоделирован трафик в виде ФГШ, состоящего из ше-

сти фрагментов одинаковой длительности, но имеющих разную фрактальную размерность, как это видно из таблицы 1.

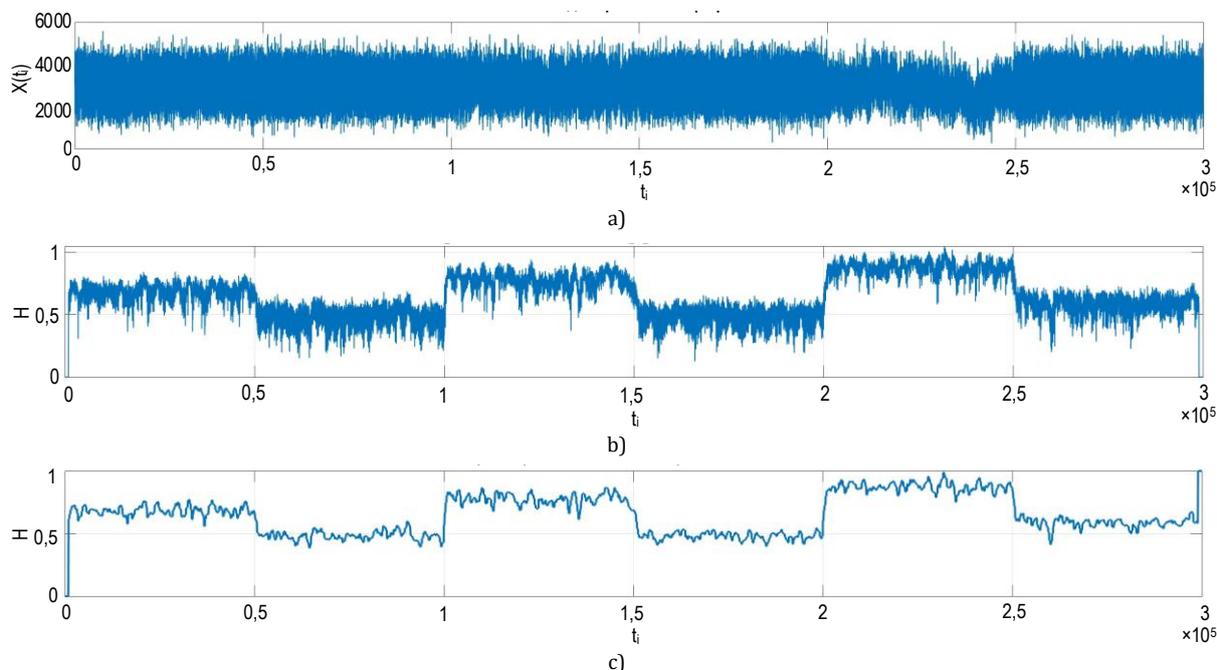
**ТАБЛИЦА 1. Показатель Херста на промежутках моделируемого трафика**

TABLE 1. Hurst Exponent at Intervals of Simulated Traffic

Промежуток	Показатель Херста
0–50 000	0,7
50 000–100 000	0,5
100 000–150 000	0,8
150 000–200 000	0,5
200 000–250 000	0,9
250 000–300 000	0,6

На рисунке 1а показана тестовая последовательность, смоделированная при помощи генератора ФГШ, а на рисунке 1б – оценка показателя Херста в скользящем окне полученная с помощью алгоритма (14).

Из представленной реализации видно, что алгоритм (14) фиксирует скачки фрактальной размерности (показателя Херста) в тестовой последовательности. Вместе с тем видно, что при использовании подобного скользящего окна наблюдаются значительные флуктуации оценки показателя  $H$  вокруг среднего значения. Флуктуации вызваны пересчетом значений показателя  $H$  при каждом единичном шаге смещения окна анализа.



**Рис. 1. Иллюстрация работы алгоритма: а) смоделированный трафик; б) полученная оценка показателя Херста в скользящем окне; в) отфильтрованная оценка показателя Херста**

Fig. 1. Algorithm Operation Illustration: a) Simulated Traffic; b) Derived Hurst Exponent Estimate in a Sliding Window; c) Filtered Hurst Exponent Estimate

Чтобы этого избежать и получить усредненные оценки, предлагается произвести дополнительную фильтрацию оценок  $\hat{H}(t_m)$ , сформированных с помощью соотношения (14). С этой целью применена пороговая обработка данных с помощью соотношения (15). В результате формируется последовательность оценок  $\hat{H}(t_m)$ , как это иллюстрируется на рисунке 1с.

Важно отметить, что как текущие средние значения, так и моменты смены показателя  $H$  не изменяются и алгоритм (15) по-прежнему достоверно отслеживает скачки фрактальной размерности.

### Влияние типа вейвлета

Важное значение при практической реализации предложенного алгоритма обработки имеет выбор материнского вейвлета в алгоритмах (14) и (15). Для выбора типа материнского вейвлета  $\psi_{m,k}(t_i)$ , используемого при обработке генерировалась последовательность ФГШ длиной 10 000 отсчетов с показателем Херста  $H = 0,95$ , представленная на рисунке 2а.

На рисунке 2б показаны текущие оценки показателя Херста в скользящем окне с использованием алгоритма (14) и разных типов вейвлетов; на рисунке 2с показаны текущие оценки показателя Херста в скользящем окне – алгоритма обработки (15) и тех

же типов вейвлетов. Использовались вейвлеты Хаара, Добеши4, Симлет4, Коифлет4 и Мейера.

Сравнение рисунков 2б и 2с позволяет визуально иллюстрировать эффективность вторичной фильтрации оценок показателя Херста.

В таблице 2 представлены численные оценки среднего значения и дисперсии показателя Херста при использовании разных материнских вейвлетов.

ТАБЛИЦА 2. Средние значения и дисперсии оценок показателя Херста

TABLE 2. Mean Values and Variances of Estimates

Тип вейвлета	До / после фильтрации	
	среднее значение	дисперсия
Хаар	0,9333 / 0,933	0,0022 / 0,0012
Добеши4	0,9008 / 0,9009	0,0025 / 0,0017
Симлет4	0,8912 / 0,8913	0,0023 / 0,0016
Коифлет4	0,8291 / 0,8293	0,0024 / 0,0020
Мейер	0,7430 / 0,7431	0,0047 / 0,0024

Из представленных численных значений видно, что более точно алгоритм оценивает показатель Херста при использовании вейвлетов Хаара, Добеши4, Симлет4. Наименьший разброс в оценке показателя Херста наблюдается для вейвлета Хаара, который и использовался в дальнейшем.

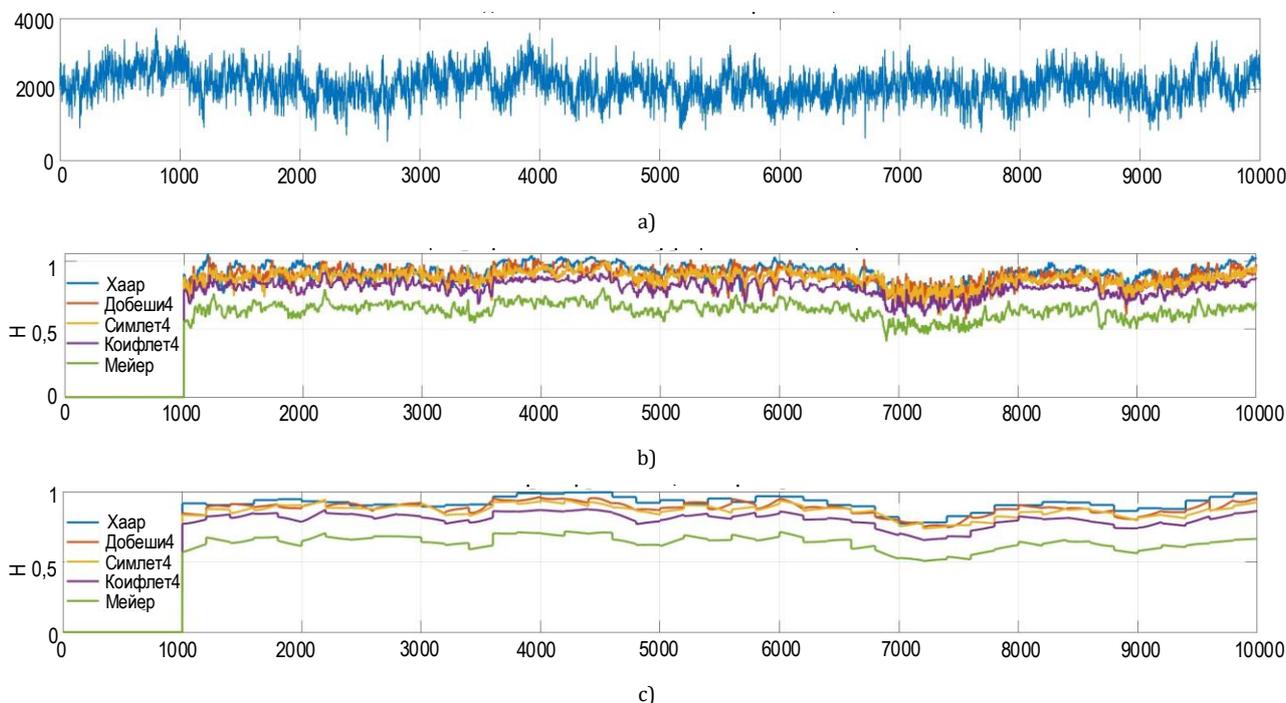


Рис. 2. Тестирование алгоритма при использовании разных типов вейвлетов: а) сгенерированная последовательность с  $H = 0,95$ ; б) оценка показателя Херста в скользящем окне с использованием разных типов вейвлетов; в) отфильтрованная оценка

Fig. 2. Testing the Algorithm Using Different Types of Wavelets: a) Generated Sequence with a Hurst Exponent of 0,95; b) Estimation of the Hurst Exponent in a Sliding Window Using Different Types of Wavelets; c) Filtered Estimate

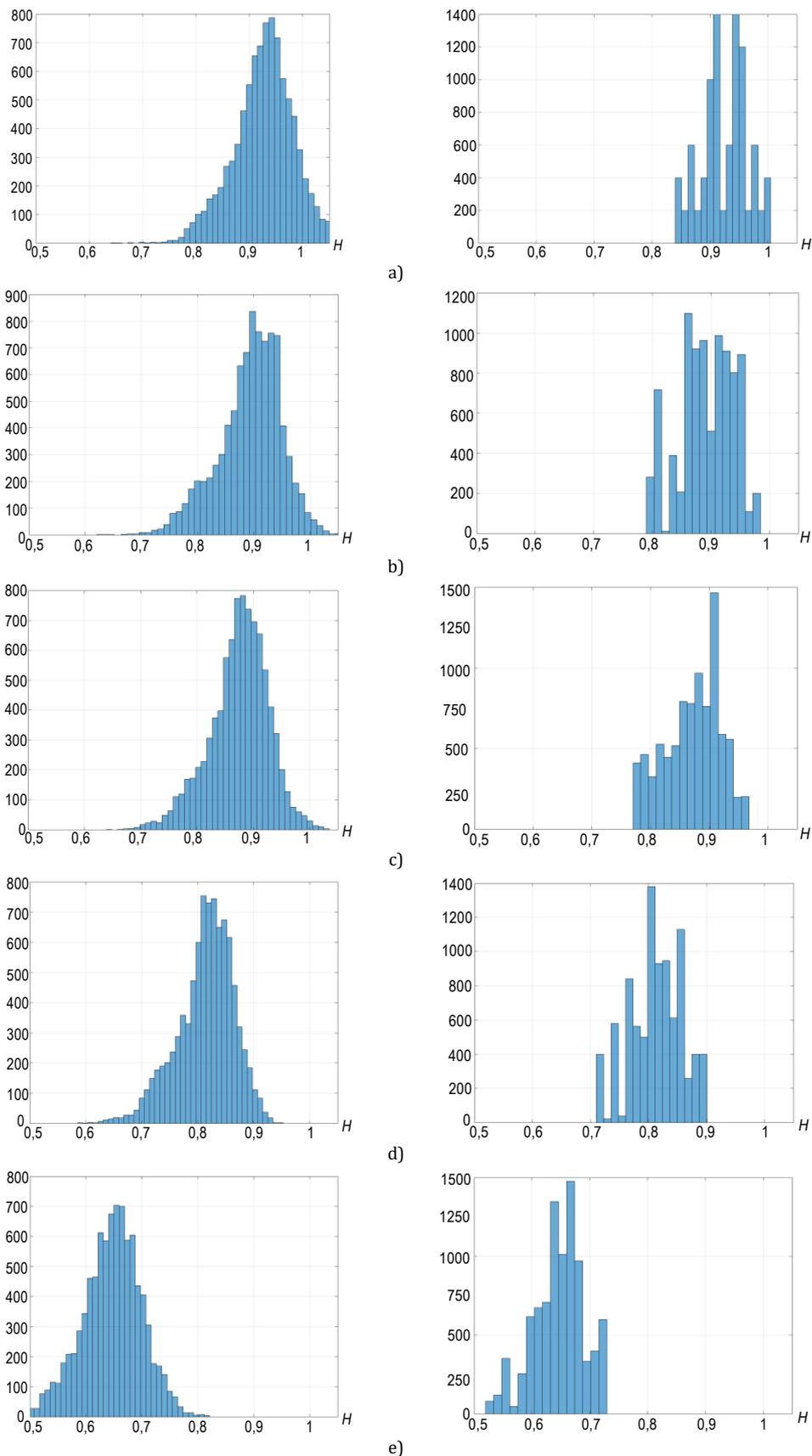


Рис. 3. Распределение оценки Херста: а) Хаар; б) Добеши4; в) Симлет4; д) Коифлет4; е) Мейер

Fig. 3. Distribution of the Hurst Estimate: a) Haar; b) Daubechies4; c) Symlet4; d) Coiflet4; e) Meyer

На рисунке 3 представлены гистограммы распределений оценки Херста для ФГШ с показателем Херста  $H = 0,95$  до (слева) и после (справа) фильтрации.

Сравнение представленных гистограмм иллюстрирует эффективность предложенной пороговой обработки для формирования оценок фрактальной размерности. Видно, что введение жесткого трешолдинга уменьшает динамический диапазон изменения текущих значений оценок показателя Херста и определяется введенным пороговым уровнем  $\tau$ .

### Экспериментальные результаты

Рассмотрим работу предложенного алгоритма (15) на реальных данных. В качестве исходных данных взята реализация сетевого трафика из дампа

DARPA99 [4]. Реализация, представленная на рисунке 4а, имеет длительность  $N = 10\ 000$ , включает в себя как нормальный трафик, так и аномалию в виде атаки Neptune (SYN-flood). Размер окна анализа был выбран равным  $M = 1000$ , а количество уровней разложения  $J = 10$ . Использовался вейвлет Хаара.

На рисунках 4б и 4с представлены  $\hat{H}(t_m)$  и усредненные  $\bar{H}(t_m)$  оценки показателя Херста, по которым видно, что атака может быть обнаружена с помощью пороговой обработки текущих оценок фрактальной размерности трафика в скользящем окне в режиме реального времени. Как видно из рисунка 4с, предпочтение следует отдать использованию усредненных оценок.

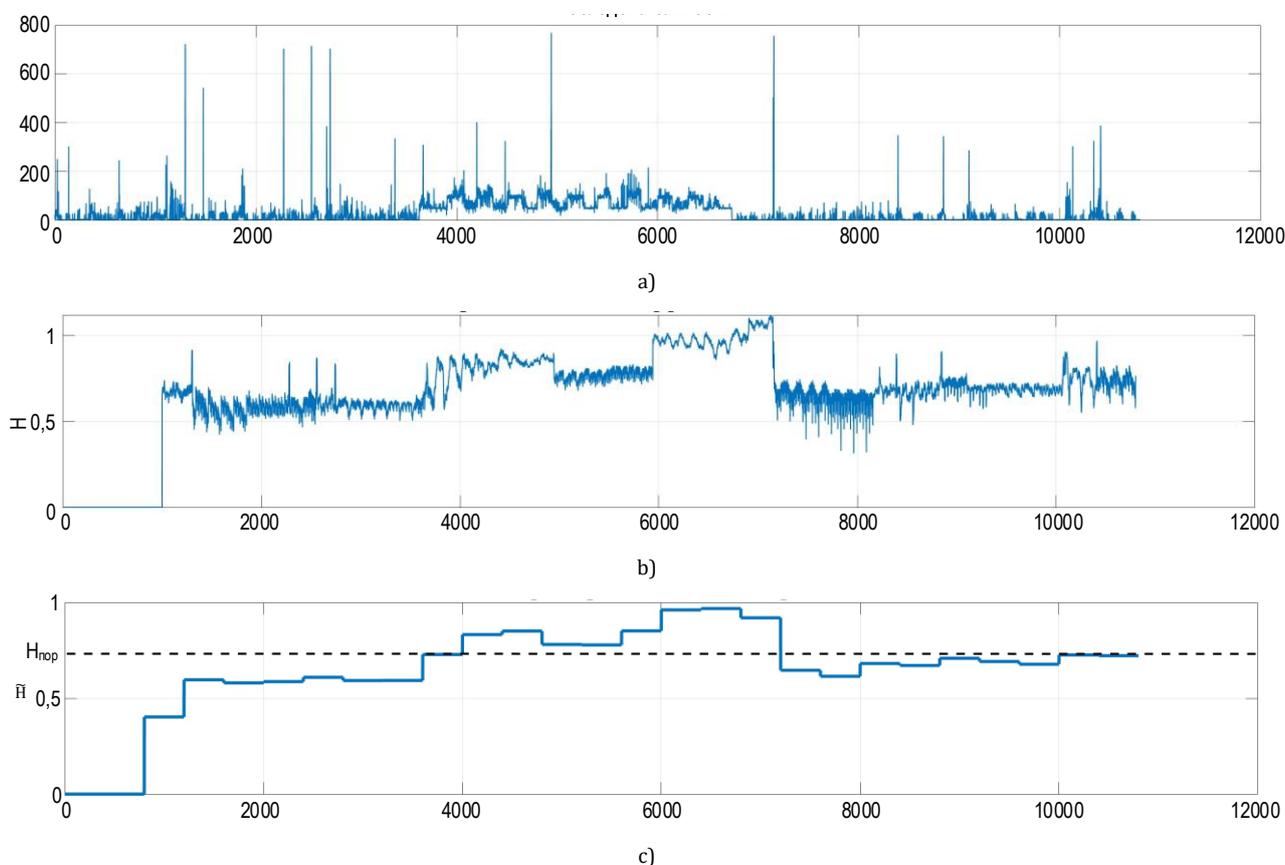


Рис. 4. Тестирование алгоритма на реальных данных: а) график реализации трафика с атакой Neptune; б) оценка Херста в скользящем окне; в) оценка показателя Херста после вторичной фильтрации

Fig. 4. Testing the Algorithm on Real Data: a) Neptune Attack Traffic Graph; b) Sliding Window Hurst Estimate; c) Filtered Estimate

На рисунке 5 представлены гистограммы распределения показателя Херста, иллюстрирующие возможность обнаружения атаки с помощью пороговой фиксации оценок фрактальной размерности. Выбор порога обнаружения  $H_{\text{порог}}$  определяется требуемой величиной вероятности ошибок первого рода Рлт.

На рисунке 6 представлены зависимости характеристик вероятности правильного обнаружения

Рп и ложного срабатывания Рлт в зависимости от порога обнаружения при разной длительности окна  $M$  до и после фильтрации. При расчетах принято  $L = 500$ .

Как видно из представленных зависимостей, достоверность правильного обнаружения атаки возрастает при увеличении длительности окна анализа. Одновременно наблюдается снижение вероятности ложной фиксации Рлт.

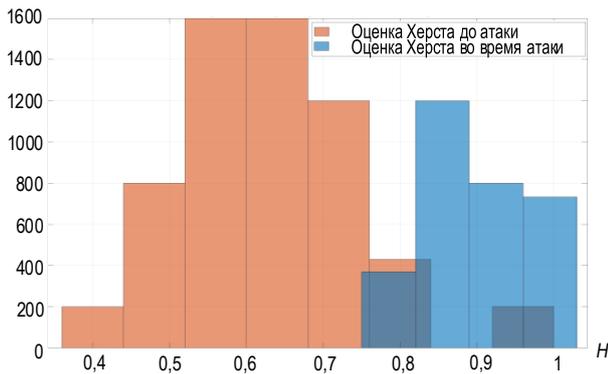


Рис. 5. Распределение фильтрованной оценки показателя Херста до и во время атаки

Fig. 5. Graph of the Distribution of the Hurst Exponent before the Attack (Pink) and on the Attack (Blue)

С длительностью окна анализа тесно связана величина количества уровней разложения  $J$ , используемых при вейвлет-анализе в формулах (14 и 15). Чем больше длительность окна анализа  $M$ , тем больше уровней разложения может быть получено и тем большее количество коэффициентов детализации может быть использовано при реализации алгоритмов (14 и 15).

Из рисунков 6а и 6б видно, что дополнительная фильтрация оценок показателя Херста позволяет повысить достоверность обнаружения  $P_d$  (ступенчатая линия) при малой длительности окна анализа, при этом снижается и величина ложных срабатываний  $P_{лт}$ . Увеличение длительности окна анализа при процедуре трешолдинга незначительно влияет на характеристики обнаружения.

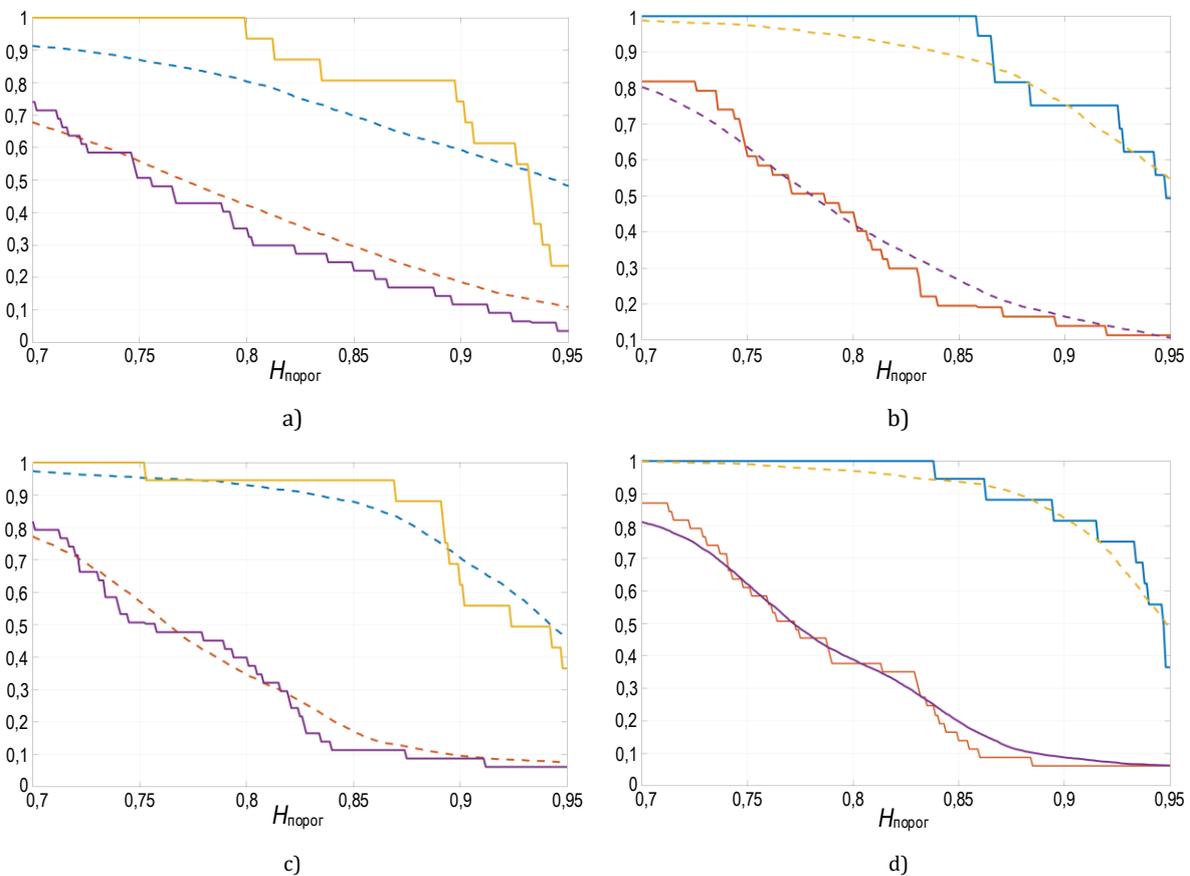


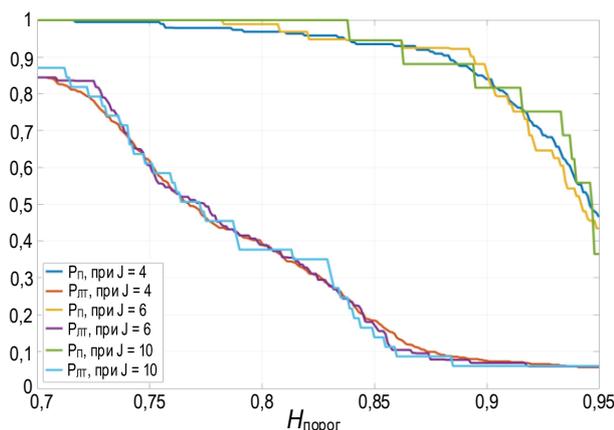
Рис. 6. Зависимости  $P_n$  и  $P_{лт}$  от порогового уровня при использовании разной длины окна анализа  $M$  до (пунктирная кривая) и после фильтрации (ступенчатая кривая) при а)  $M = 200$ ; б)  $M = 500$ ; в)  $M = 700$ ; д)  $M = 1000$

Fig. 6. Dependences of  $P_n$  and  $P_{лт}$  on the Threshold Level When Using Different Lengths of the Analysis Window  $M$  up to (Dashed Curve) and after Filtering (Stepped Curve) at а)  $M = 200$ ; б)  $M = 500$ ; в)  $M = 700$ ; д)  $M = 1000$

На рисунке 7 представлены зависимости характеристик вероятности правильного обнаружения  $P_d$  и ложного срабатывания  $P_{лт}$  от порога обнаружения при разном уровне разложения и вторичной пороговой обработке показателя Херста.

Как видно, при увеличении уровня разложения в режиме вторичной фильтрации удается добиться

уменьшения числа ложных срабатываний. Из полученных зависимостей видно, что при уровне разложения  $J = 10$  достигается минимальная вероятность ложной тревоги, так, например, при выборе порогового уровня  $H_{порог} = 0,85$  величина вероятности правильного обнаружения составляет  $P_d = 0,95$ , а  $P_{лт} = 0,1$ .



**Рис. 7. Зависимости  $P_n$  и  $P_{лт}$  от порога обнаружения при использовании разного количества уровней разложения при пороговой обработке**

*Fig. 7. Graph of the Dependence of the Probability of Correct Detection and False Positive on the Detection Threshold when Using a Different Number of Decomposition Levels during Filtering*

## Выводы

Для решения задачи обнаружения аномалий в режиме реального времени предложено модифицировать алгоритм оценки скачка фрактальной размерности на основе упорядоченной совокупности коэффициентов вейвлет-декомпозиции анализируемого трафика с помощью дополнительной пороговой обработки коэффициентов детализации в виде жесткого трешолдинга и последующей вторичной фильтрации.

Показано, что для вейвлет-декомпозиции целесообразно использовать вейвлет Хаара, показавший наилучшие результаты. При вторичной фильтрации наименьший разброс в оценке показателя Херста наблюдается при применении вейвлета Хаара. Проведенные исследования показали, что применение дополнительной процедуры трешолдинга позволяет улучшить достоверность обнаружения до 10 %.

## Список источников

1. Ahmed M., Mahmood A.N., Hu J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. 2016. Vol. 60. PP. 19–31. DOI:10.1016/j.jnca.2015.11.016
2. Шелухин О.И., Осин А.В., Смольский С.М. Самоподобие и фракталы. Телекоммуникационные приложения. М.: Физматлит, 2008. 368 с.
3. Басараб М.А., Строганов И.С. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4(7). С. 30–40.
4. Sheluhin O.I., Lukin I.Yu. Network Traffic Anomalies Detection Using a Fixing Method of of Multifractal Dimension Jumps in a Real-Time Mode // Automatic Control and Computer Sciences. 2018. Vol. 52. Iss. 5. PP. 421–430. DOI:10.3103/S0146411618050115
5. Bhuyan M.H., Bhattacharyya D.K., Kalita J.K. Network Anomaly Detection: Methods, Systems and Tools // IEEE Communications Surveys & Tutorials. 2013. Vol. 60. Iss. 1. PP. 303–336. DOI:10.1109/SURV.2013.052213.00046
6. Chandola V., Banerjee A., Kumar V. Anomaly Detection for Discrete Sequences: A Survey // IEEE Transactions on Knowledge and Data Engineering. 2012. Vol. 24. Iss. 5. PP. 823–839. DOI:10.1109/TKDE.2010.235
7. Шелухин О.И., Рыбаков С.Ю., Магомедова Д.И. Скрытие информации в аудиосигналах с использованием детерминированного хаоса // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 1. С. 80–91. DOI:10.36724/2409-5419-2021-13-1-80-91
8. Sheluhin O.I., Sirukhi J.W., Pankrushin A.V. Wavelet type selection in the problem of anomaly intrusions detection in computer networks using multifractal analysis methods // T-Comm. 2015. Vol. 9. Iss. 4. PP. 88–92.
9. Mallat S. A Wavelet Tour of Signal Processing: The Sparse Way. Burlington: Academic Press, 2008. 832 p.
10. Kaur G., Saxena V., Prakash J. Study of Self-Similarity for Detection of Rate-Based Network Anomalies // International Journal of Security and Its Applications. 2017. Vol. 11. Iss. 8. PP. 27–44. DOI:10.14257/ijisia.2017.11.8.03
11. Riedi R.H., Crouse M.S., Ribeiro V.J., Baraniuk R.G. A Multifractal Wavelet Model with Application to Network Traffic // IEEE Transactions on Information Theory. 1999. Vol. 45. Iss. 3. PP. 992–1018. DOI:10.1109/18.761337
12. Басараб М.А., Шелухин О.И., Коновалов И.А. Оценка влияния трешолдинга на достоверность обнаружения аномальных вторжений в компьютерные сети статистическим методом // Вестник МГТУ им. Н.Э. Баумана. Серия Приборостроение. 2018. № 5(122). С. 56–67. DOI:10.18698/0236-3933-2018-5-56-67
13. Zhang Y., Ding W., Pan Z., Qin J. Improved Wavelet Threshold for Image De-noising // Frontiers in Neuroscience. 2019. Vol. 13. P. 39. DOI:10.3389/fnins.2019.00039
14. Delignières D. Correlation Properties of (Discrete) Fractional Gaussian Noise and Fractional Brownian Motion // Mathematical Problems in Engineering. 2015. P. 485623. DOI:10.1155/2015/485623
15. Li M. Generalized fractional Gaussian noise and its application to traffic modeling // Physica A: Statistical Mechanics and Its Applications. 2021. Vol. 579. P. 126138. DOI:10.1016/j.physa.2021.126138
16. Li M., Sun X., Xiao X. Revisiting fractional Gaussian noise // Physica A: Statistical Mechanics and Its Applications. 2019. Vol. 514. PP. 56–62. DOI:10.1016/j.physa.2018.09.008
17. Brouste A., Soltane M., Votsi I. One-step estimation for the fractional Gaussian noise at high-frequency // ESAIM: Probability and Statistics. 2020. Vol. 24. PP. 827–841. DOI:10.1051/ps/2020022
18. Sørbye S.H., Rue H. Fractional Gaussian noise: Prior specification and model comparison // Environmetrics. 2017. Vol. 29. Iss. 5-6. P. e2457. DOI:10.1002/env.2457

## References

1. Ahmed M., Mahmood A.N., Hu J. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*. 2016;60:19–31. DOI:10.1016/j.jnca.2015.11.016
2. Sheluhin O.I., Osin A.V., Smolsky S.M. *Self-Similarity and Fractals. Telecommunication Applications*. Moscow: Fizmatlit Publ.; 2008. 368 p. (in Russ.)
3. Basarab M., Stroganov I. Anomaly Detection in Information Processes Based on Multifractal Analysis. *Voprosy kiberneticheskoy bezopasnosti*. 2014;4(7):30–40. (in Russ.)
4. Sheluhin O.I., Lukin I.Yu. Network Traffic Anomalies Detection Using a Fixing Method of of Multifractal Dimension Jumps in a Real-Time Mode. *Automatic Control and Computer Sciences*. 2018;52(5):421–430. DOI:10.3103/S0146411618050115
5. Bhuyan M.H., Bhattacharyya D.K., Kalita J.K. Network Anomaly Detection: Methods, Systems and Tools. *IEEE Communications Surveys & Tutorials*. 2013;60(1):303–336. DOI:10.1109/SURV.2013.052213.00046
6. Chandola V., Banerjee A., Kumar V. Anomaly Detection for Discrete Sequences: A Survey. *IEEE Transactions on Knowledge and Data Engineering*. 2012;24(5):823–839. DOI:10.1109/TKDE.2010.235
7. Sheluhin O.I., Rybakov S.Y., Magomedova D.I. Audio Steganography Method Using Determined Chaos. *H&ES Research*. 2021;13(1):80–91. (in Russ.) DOI:10.36724/2409-5419-2021-13-1-80-91
8. Sheluhin O.I., Sirukhi J.W., Pankrushin A.V. Wavelet type selection in the problem of anomaly intrusions detection in computer networks using multifractal analysis methods. *T-Comm*. 2015;9(4):88–92.
9. Mallat S. *A Wavelet Tour of Signal Processing: The Sparse Way*. Burlington: Academic Press; 2008. 832 p.
10. Kaur G., Saxena V., Prakash J. Study of Self-Similarity for Detection of Rate-Based Network Anomalies. *International Journal of Security and Its Applications*. 2017;11(8):27–44. DOI:10.14257/ijasia.2017.11.8.03
11. Riedi R.H., Crouse M.S., Ribeiro V.J., Baraniuk R.G. A Multifractal Wavelet Model with Application to Network Traffic. *IEEE Transactions on Information Theory*. 1999;45(3):992–1018. DOI:10.1109/18.761337
12. Basarab M.A., Sheluhin O.I., Konovalov I.A. Assessment of the Thresholding Impact on Reliability of Anomaly Detection in Network Traffic Using Statistical Approach. *Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*. 2018;5(122):56–67. DOI:10.18698/0236-3933-2018-5-56-67
13. Zhang Y., Ding W., Pan Z., Qin J. Improved Wavelet Threshold for Image De-noising. *Frontiers in Neuroscience*. 2019;13:39. DOI:10.3389/fnins.2019.00039
14. Delignières D. Correlation Properties of (Discrete) Fractional Gaussian Noise and Fractional Brownian Motion. *Mathematical Problems in Engineering*. 2015:485623. DOI:10.1155/2015/485623
15. Li M. Generalized fractional Gaussian noise and its application to traffic modeling. *Physica A: Statistical Mechanics and Its Applications*. 2021:579. 126138. DOI:10.1016/j.physa.2021.126138
16. Li M., Sun X., Xiao X. Revisiting fractional Gaussian noise. *Physica A: Statistical Mechanics and Its Applications*. 2019;514:56–62. DOI:10.1016/j.physa.2018.09.008
17. Brouste A., Soltane M., Votsi I. One-step estimation for the fractional Gaussian noise at high-frequency. *ESAIM: Probability and Statistics*. 2020;24:827–841. DOI:10.1051/ps/2020022
18. Sørbye S.H., Rue H. Fractional Gaussian noise: Prior specification and model comparison. *Environmetrics*. 2017;29(5-6):e2457. DOI:10.1002/env.2457

Статья поступила в редакцию 27.06.2022; одобрена после рецензирования 27.07.2022; принята к публикации 28.07.2022.

The article was submitted 27.06.2022; approved after reviewing 27.07.2022; accepted for publication 28.07.2022.

## Информация об авторах:

**ШЕЛУХИН**  
Олег Иванович

доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность» Московского технического университета связи и информатики

 <https://orcid.org/0000-0001-7564-6744>

**РЫБАКОВ**  
Сергей Юрьевич

главный специалист НОЦ «Информационная безопасность» Московского технического университета связи и информатики

 <https://orcid.org/0000-0002-4593-9009>

**ВАНЮШИНА**  
Анна Вячеславовна

кандидат технических наук, доцент кафедры «Информационная безопасность» Московского технического университета связи и информатики

 <https://orcid.org/0000-0001-8729-6729>