ОБНАРУЖЕНИЕ АНОМАЛИЙ В ИНФОРМАЦИОННЫХ ПРОЦЕССАХ НА ОСНОВЕ МУЛЬТИФРАКТАЛЬНОГО АНАЛИЗА

***Басараб Михаил Алексеевич**., доктор физико-математических наук, профессор*
Строганов И.С.

Основным требованием к современным системам обнаружения вторжений является возможность выявления аномалий в информационных процессах с целью обнаружения неизвестных типов атак. Приведен обзор существующих подходов к обнаружению сетевых аномалий на основе методов мультифрактального анализа. Представлены результаты вычисления показателя Херста для временного ряда загруженности процессора при различных видах деятельности пользователя.

***Ключевые слова**: фрактальный анализ, показатель Херста, обнаружение сетевых аномалий.*

ANOMALY DETECTION IN INFORMATION PROCESSES BASED ON MULTIFRACTAL ANALYSIS

***Mikhail Basarab** , doctor of physical and mathematical sciences, professor*
I.Stroganov

The basic requirement for modern intrusion detection systems is the ability to detect anomalies in the information processes in order to detect unknown attacks. An overview of existing approaches to the detection of network anomalies based on multifractal analysis is presented. The results of the Hurst exponent evaluation for the time series of CPU usage for different types of user activity are presented.

***Keywords**: fractal analysis, Hurst exponent, network anomaly detection.*

Введение

Сигнатурные методы анализа, используемые в современных системах обнаружения вторжений, направлены на выявление известных и точно описанных типов атак, и оказываются не в состоянии обнаружить их модификации или новые типы, что делает использование таких систем малоэффективным. Существующие решения частных случаев задачи обнаружения сетевых аномалий до сих пор не позволили разработать единый универсальный механизм выявления ранее неизвестных типов атак.

Актуальной задачей на данный момент является поиск более эффективных универсальных методов обнаружения сетевых аномалий, являющихся следствием технических сбоев или несанкционированного воздействия. Основным требованием к этим методам является возможность обнаружения произвольных типов аномалий, в том числе распределенных во времени. Статистические исследования сетевого трафика показывают наличие у него свойств фрактальности или самоподобия, а также изменчивость данных характеристик при появлении аномалий в сети, что позволяет использовать методы фрактального анализа для обнаружения атак [1, 2].

Целью исследования является обзор современных существующих подходов к обнаружению сетевых аномалий на основе методов фрактального анализа.

Методы обнаружения атак

Атака – преднамеренные действия нарушителя, приводящие к нарушению конфиденциальности, целостности или доступности системы.

Методы обнаружения атак делятся на:

1) сигнатурные;

2) поведенческие.

Сигнатурные методы предназначены для обнаружения известных и четко описанных атак и основаны на эталонной сверке последовательностей символов и событий с базой данных сигнатур атак. Преимущества сигнатурных методов: низкие требования к вычислительным ресурсам, достоверность обнаружения атак. Недостатки сигнатур-

ных методов: невозможность обнаружения новых типов атак и модификаций, существующих без строгой формализации ключевых слов сетевого трафика и обновления базы данных сигнатур.

Поведенческие методы предназначены для обнаружения неизвестных атак и основаны на выявлении аномалий, отклонений от штатного режима функционирования. Преимущества поведенческих методов: возможность анализа динамики процессов и возможность выявления новых типов атак. Недостатки поведенческих методов: более высокие требования к вычислительным ресурсам, более низкая достоверность обнаружения.

Фрактальный анализ

Временным рядом называется последовательность значений исследуемой величины, измеренных через равные промежутки времени.

Центральными понятиями фрактального анализа являются фрактальная размерность (D) и показатель Херста (H).

Фрактальная размерность множества (по Хаусдорфу) определяется:

$$D = -\lim_{\varepsilon \to 0} \frac{\lg[N(\varepsilon)]}{\lg[\varepsilon]},$$

где $N(\varepsilon)$ – минимальное число непустых кубов размером ε, покрывающих заданное множество.

Показатель Херста характеризует степень самоподобия процесса:

1. $0 < H < 0.5$ – случайный процесс, который не обладает самоподобием, характеризуется стремлением к среднему значению;
2. $H = 0.5$ – полностью случайный процесс без выраженной тенденции;
3. $H > 0.5$ – трендоустойчивый процесс, который обладает длительной памятью и является самоподобным.

Фрактальная размерность напрямую связана с показателем Херста соотношением: $D = 2 - H$. Это соотношение справедливо, когда структура кривой, описывающей фрактальную функцию, исследуется с высоким разрешением, то есть в локальном пределе.

Одним из популярных методов нахождения фрактальной размерности является R/S анализ [2]:

$$M\left[\frac{R(n)}{S(n)}\right] \sim cn^H \text{ при } n \to \infty,$$

где n – число значений временного ряда.

c – положительная конечная константа, не зависящая от n.

H – показатель Херста.

$R(n)$ – размах временного ряда:

$$R(n) = \max_{1 \le j \le n} \Delta_j - \min_{1 \le j \le n} \Delta_j$$

$$\Delta_k = \sum_{i=1}^{n} x_i - k\bar{x}, k = \overrightarrow{1,n}$$

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

$$S(n) = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2$$

Обзор существующих подходов

В работе [1] для обнаружения аномалий трафика используется метод максимумов модулей вейвлет-преобразования (ММВП), позволяющий выявить сингулярности сигнала.

В качестве анализируемых данных был взят сетевой трафик, собранный на граничном маршрутизаторе университетской сети Массачусетского технологического института (1999 DARPA Intrusion Detection Evaluation). Каждая последовательность длиной около 24 часа с шагом дискретизации в 1 с. Представлены образцы «чистого» трафика без атак, а также с различными аномалиями: при DDoS-атаках различных типах сканирования.

Алгоритм оценки параметров мультифрактального спектра следующий.

Выполняется декомпозиция исходного сигнала $f(t)$ при помощи вейвлет-преобразования материнским вейвлетом $\Psi(t)$ на коэффициенты:

$$W_f(u,j) = \left(f(t), \Psi_{u,s}(t)\right) = 2^{-j/2} \int \frac{t-u}{2^j} dt$$

Вычисляется функция разбиения:

$$S(q,j) = \sum_p |W_f(u_p, j)|^q$$

Для каждого $q \in R$ вычисляется масштабный показатель:

$$\tau(q,j) = \log_{j \to 0} \inf \frac{\ln S(q,j)}{\ln 2^j}$$

Вычисляется мультифрактальный спектр $f_L(a)$ при помощи преобразования Лежандра:

$$f_L(a) = \min_{q \in R}\left[q\left(a + \frac{1}{2}\right) - \tau(q)\right]$$

Для каждой октавы j вычисляются мультифрактальные размерности порядка q:

$$D_{q,j} = \frac{1}{q-1}\left[q\big(a(q,j) - f(a(q),j)\big)\right]$$

При $q < 0$ значение $S(q,j)$ зависит, в основном, от малых максимумов амплитуды $|W_f(u_p, j)|$, в результате чего вычисления могут быть неустойчивы. Чтобы избежать появления ложных максимумов модуля, созданных вычислительными

погрешностями в областях, где f почти константа, вейвлет-максимумы объединяются в цепочку, чтобы образовать кривую максимумов в зависимости от масштаба.

Если $\Psi = (-1)^P \theta^{(p)}$, где $\theta = \frac{1}{\sqrt{2\pi}} e^{-t^2/2}$ – функция Гаусса, то все линии максимумов $u_p(j)$ определяют кривые, которые распространяются до предела $j = 0$. Поэтому все линии максимумов, которые не распространяются до наименьшего масштаба, удаляются при вычислении $S(q,j)$.

Формализуя различие спектров трафика с аномалиями и без них, можно сравнивать фрактальные размерности D_1, корреляционные размерности D_2 и интервалы, характеризующие «ширину» спектра Лежандра для каждой из реализаций по каждой октаве (уровню) разложения j.

Информационные размерности сравниваемых реализаций D_1 различаются на небольшую постоянную величину и практически не зависят от количества уровней разложения. Это позволяет сделать вывод о том, что наличие в сигнале продолжительных атак и аномальной активности изменяет самоподобную природу трафика, и данное свойство можно использовать для выявления атак.

В работе [3] предлагается определять аномалии, основываясь на их самоподобии и распределении «тяжелых хвостов». Сетевые аномалии могут возникать вследствие перегрузок, ошибок сетевых устройств, DDoS-атак, попыток несанкционированного доступа.

Для уменьшения влияния периодичности сетевого трафика на оценку показателя Херста, временной ряд делится на 24 набора значений. Для каждого набора строится гистограмма для 24 равных промежутков времени. Для каждой группы находится число пакетов и средняя длина пакета для одночасовых интервалов времени. На следующем этапе вычисляется показатель Херста методом периодограммы, использующим наклон спектра мощности. Показатель Херста вычисляется из соотношения: $\beta - 1 = 1 - 2H$, где β – наклон прямой в логарифмическом масштабе.

На практике сначала анализируется трафик в штатном режиме функционирования сети в течение дня. При включении режима обнаружения аномалий вычисляемый показатель Херста сравнивается с соответствующим эталонным значением, вычисленным в нормальном режиме, для каждого параметра.

В работе [4] используется алгоритм обнаружения аномалий на основе дискретного стационарного вейвлет-преобразования (DSWT) и фрактальной размерности (FD).

На первом шаге выполняется фильтрация временного ряда с помощью дискретного стационарного вейвлет-преобразования. Эта предварительная обработка используется для увеличения точности предложенного метода: выделяются основные составляющие, детали отфильтровываются. Главным преимуществом дискретного стационарного вейвлет-преобразования перед классическим является сохранение временной информации исходного сигнала на каждом уровне.

На втором шаге выполняется обход временного ряда двумя соседними скользящими окнами R и S. Для каждого окна вычисляется фрактальная размерность FD по алгоритму Katz:

$$FD = \frac{\lg(L/a)}{\lg(d/a)}$$

L – длина временного ряда, d – расстояние между первой точкой ряда и наиболее удаленной от нее, a – среднее расстояние между двумя соседними точками.

Изменения статистических параметров сигнала отражаются на фрактальной размерности, для учета которых вводится функция:

$$G_k = |FD_{k+1} - FD_k|, k = 1, \dots, N$$

N – число точек G.

На третьем шаге ищутся локальные максимумы G, превышающие заданный порог, которые рассматриваются как отклонение от нормального поведения.

На точность метода значительно влияет длина скользящего окна. Для анализируемого окна длины l энергия функции G_l вычисляется следующим образом:

$$E_{G_l} = \frac{\sum_k |G_{l_k}|^2}{N}$$

Длина окна вычисляется как минимум нормированной энергетической функции E_{G_l}.

В работе [5] предлагается метод для обнаружения DDoS-атак на основе оценки показателя Херста с помощью дробного преобразования Фурье, осуществляющего переход в частотно-временную область.

Для сигнала $x(t)$ дробное преобразование Фурье определяется:

$$X_a(u) = F_a(u) = \int_{-\infty}^{\infty} x(t) K_a(t,u) dt$$

$$K_a(t,u) = \sqrt{1 - i \cdot \cot(\alpha)} \cdot \exp[i\pi(t^2 \cot(\alpha) - 2ut \cdot \csc(\alpha) + u^2 \cot(\alpha))], \alpha \neq \pi n$$

$$K_a(t,u) = \delta(t-u), \alpha = (2n \pm 1)\pi$$

$$n \in Z, \alpha = \frac{a\pi}{2}$$

a – порядок дробного преобразования Фурье, при a=1 формула превращается в стандартное преобразование Фурье.

Используя дискретное вейвлет-преобразование и многомасштабный метод анализа [6, 7], можно вычислить показатель Херста H, проанализировав выражение:

$G(j) \leftrightarrow (2H+1)j + constant$, где j – масштаб.

Далее осуществляется оптимальный выбор интервала масштабов, при этом используется метод одномерной взвешенной оценки наименьших квадратов [8].

Экспериментальная проверка предложенного метода показала его высокую точность, что позволило снизить число ложных срабатываний и пропусков при обнаружении атаки.

В работе [9] сетевой трафик разделяется на несколько непересекающихся сегментов. Оценивается показатель Херста для каждого сегмента. При преодолении пороговых значений трафик теряет свойство самоподобия, что расценивается как DDoS-атака. Но интенсивность DDoS-атаки может меняться, что приводит к изменению показателя Херста, поэтому методы обнаружения, основанные на фиксированном пороге, требуют гибкости и адаптивности.

В данной работе предлагается метод, состоящий из двух стадий:

1) статистический анализ временного ряда сетевого трафика с использованием дискретного вейвлет-преобразования и информационного критерия Шварца для нахождения точки изменения показателя Херста, сигнализирующей о начале DDoS-атаки;

2) адаптивное регулирование интенсивности DDoS-атаки на основе нечеткой логики, путем анализа показателя Херста и скорости его изменения.

Информационный критерий Шварца основан на функции максимального правдоподобия для модели и может применяться для обнаружения наличия пороговой точки путем сравнения вероятности нулевой гипотезы (точка отсутствует) и альтернативной (точка присутствует).

Показатель Херста оценивается с помощью дискретного вейвлет-преобразования, так как на практике этот метод является одним из наиболее надежных, поскольку более устойчив по отношению к гладким полиномиальным трендам и шумам.

Оценка осуществляется следующим образом. Для временного ряда сетевого трафика X в реальном режиме времени вычисляются вейвлет-коэффициенты $d(j,k)$ для каждого масштаба j и позиции k.

Далее выполняется детальная оценка дисперсии на каждом масштабе j:

$$S_j = \sum_{k=1}^{n_j} d^2(j,k)$$

n_j – число вейвлет-коэффициентов, доступных в масштабе j.

Допустим, приходит новый образец трафика, тогда сумма обновляется следующим образом:

$$n_j = n_j + 1$$
$$S_j = S_j + d^2(j, n_j)$$

Оценка дисперсии в масштабе j:

$$\varepsilon_j = \frac{S_j}{n_j}$$

Далее строится зависимость $\log_2(\varepsilon_j)$ от масштаба j и применяется взвешенная линейная регрессия для линейного участка, вычисляется наклон α. Не требуется каждый раз строить данную зависимость при каждом приходе новой порции трафика, это действие выполняется только при необходимости.

Затем вычисляется показатель Херста:

$$H = \frac{\alpha + 1}{2}$$

Принцип обнаружения атак следующий. Пусть X – временной ряд нормального трафика, Y – временной ряд трафика с аномалиями, Z – временной ряд аномалий, то есть выполняется соотношение: $Y=X+Z$. Основываясь на теоремах, приведенных в [10], можно сделать вывод о том, что независимо от наличия свойства самоподобия у Z, если X – стационарный самоподобный процесс второго порядка, то Y все еще будет самоподобным процессом, но степень самоподобия может меняться. Пусть r_X, r_Y, r_Z – автокорреляционные функции X, Y, Z соответственно. Тогда во время атаки интересует $||r_Y - r_X||$, причем $r_Y = r_X + r_Z$. Для каждого значения $H \in (0.5, 1]$ существует только одна автокорреляционная функция с самоподобием. Таким образом, рассматривается $||H_Y - H_X||$, где H_Y и H_X – средние значения показателей Херста Y и X соответственно.

Недостатком подхода является то, что коэффициенты вейвлет-преобразования и статистика на основе информационного критерия Шварца обновляются в момент прихода новых значений трафика, а обнаружение пороговой точки самоподобия трафика будет перезапущено для каждого масштаба. Таким образом, сигнал об изменении точки самоподобия будет подан, даже если это изменение произошло в другом масштабе в тот же момент времени.

После обнаружения атаки вблизи времени обнаружения трафик делится на части. Анализируя показатель Херста и скорость его изменения (разница между показателями Херста частей трафика до момента обнаружения и после), можно определить интенсивность DDoS-атаки, используя правила нечеткой логики.

Определение точки изменения самоподобия трафика с помощью информационного критерия Шварца основано на предположении, что энтропия последовательности с изменяющейся граничной точкой самоподобия больше, чем энтропия последовательности, в которой эта точка фиксирована.

Пусть имеется последовательность длины M. Предполагается, что есть только одна точка границы самоподобия на позиции $1 < g < M$. Чтобы одновременно вычислить присутствие и расположение этой точки, нужно вычислить энтропию всей последовательности, а также частей $f_1 = (1, \dots, g)$ и $f_2 = (g+1, \dots, M)$, сравнить их значения и заключить, является ли точка g граничной. Если энтропия отдельных частей значительно меньше энтропии целой последовательности, точка g считается граничной.

Общая схема обнаружения атаки показана на рис. 1.

В работе [10] вычисляются показатели Херста для четырех метрик трафика итеративным методом в режиме реального времени. Затем проверяется их попадание в доверительные интервалы нормальных значений. Далее осуществляется сбор и нормализация результатов обнаружения аномалий для оценки безопасности сетевого трафика.

***Рис.1**. Общая схема обнаружения атаки*

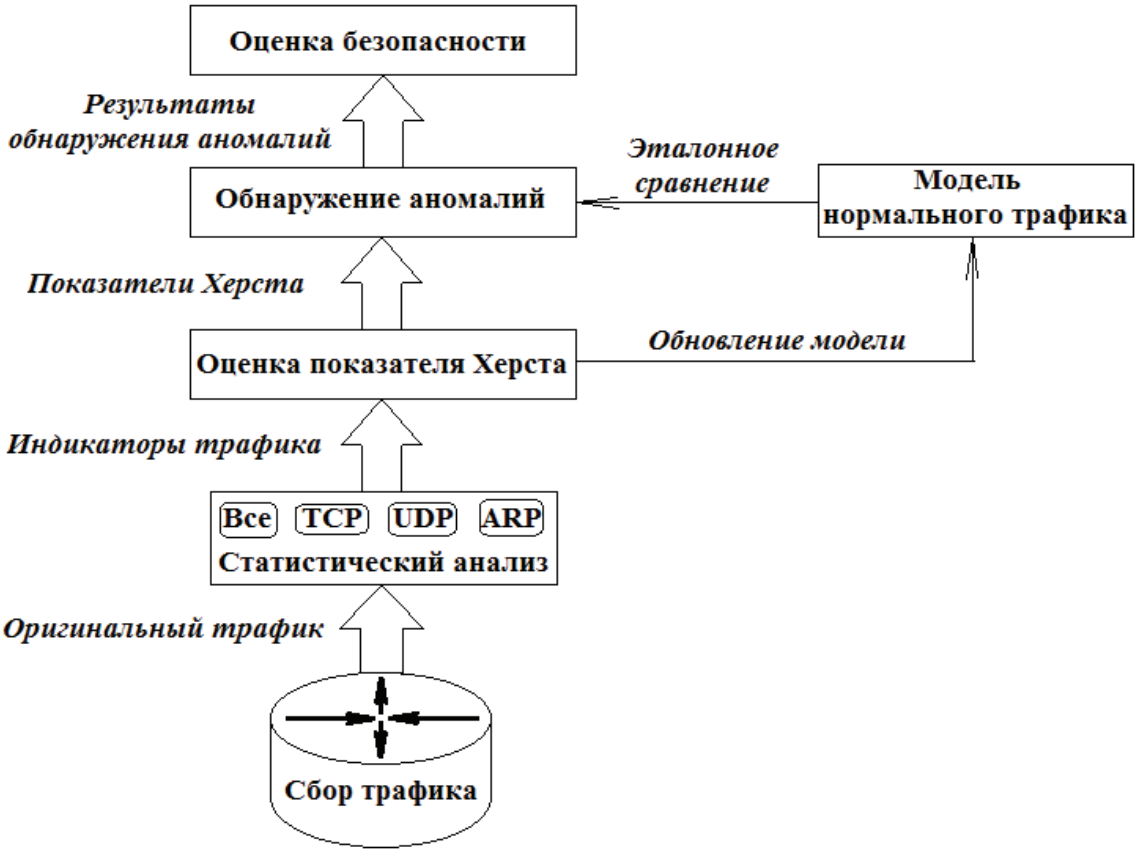

Рис.2. *Схема оценки безопасности трафика локальной сети*

Предлагается следующая схема оценки безопасности трафика локальной сети (рис.2).

Алгоритм оценки безопасности трафика делится на пять этапов:

1) сбор трафика;
2) статисти ческий анализ;
3) оценка показателя Херста;
4) обнаружение аномалий;
5) оценка безопасности.

Для уменьшения влияния на нормальное функционирование сети трафик дублируются на специальный сервер, занимающийся сбором трафика. Программное обеспечение сбора трафика на сервере включает Winpcap development kit, который имеет отличную производительность при сборе сетевых пакетов.

Из пакетов, принятых от маршрутизатора, извлекается информация о типе пакета, а также четыре метрики трафика: общее число пакетов, число TCP пакетов, UDP пакетов, ARP пакетов в единицу времени.

Вычисляются показатели Херста для четырех метрик трафика итеративным методом оценки в режиме реального времени. Эти значения используются для обнаружения аномалий и обновления модели нормального трафика.

Текущее вычисленное значение показателя Херста сравнивается со значением из нормальной модели поведения трафика. Если значение выходит за пределы допустимого, трафик считается аномальным. Нормальная модель трафика строится путем анализа нормальной работы сети в течение определенного промежутка времени. Модель включает нормальное значение показателя Херста и доверительный интервал, и может быть обновлена при обнаружении аномалий.

Критерием оценки безопасности является уровень риска, вычисляемый методом средневзвешенных величин, который учитывает результаты обнаружения аномалий от четырех метрик трафика. Уровень риска предоставляет администраторам текущее состояние передачи данных в сети с точки зрения безопасности.

Пусть X_n $(n = 1, 2, 3, \dots)$ – дискретный стохастический процесс, и выполняется:

$$X_i^{(m)} = \frac{1}{m} \sum_{k=(i-1)m+1}^{im} X_k$$

Тогда $X_n^{(m)}$ называются агрегированными процессами X_n порядка m с автокорреляционной функцией $\rho^m(k)$ порядка m.

Стационарный в широком смысле стохастический процесс X_n $(n = 1, 2, \dots)$ называется самоподобным, если X_n и его агрегированные процессы $X_n^{(m)}$ порядка m имеют одинаковые автокорреляционные функции $\rho^m(k) = \rho(k)(m = 1, 2, \dots)$.

Алгоритм итеративной оценки показателя Херста. Если стационарный в широком смысле временной ряд X_i сетевого трафика самоподобен в течение i-го периода времени, его автокорреляционная функция удовлетворяет:

$$\rho_K = H(2H-1)K^{2H-2}, K \to \infty$$

H $(0{,}5 < H < 1)$ – показатель Херста, который увеличивается при увеличении степени самоподобия процесса.

Поскольку $\sum_K \rho_K \to \infty$, самоподобный процесс часто называют длинномасштабной корреляцией. Чем больше K, тем большую релевантность имеет временной ряд.

Итеративная формула для вычисления H:

$$H_{i+1} = \sqrt{(\rho_k k^{2-2H_i} + H_i) \cdot 0{,}5}, \qquad k \to \infty$$

Для заданного временного ряда $X_1, \dots, X_n$ вычисляются:

1) математическое ожидание:

$$\hat{\mu} = \bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$$

2) ковариация:

$$\hat{\gamma}_k = \frac{1}{n-k}\sum_{i=1}^{n-k}(X_i - \bar{X})(X_{i+k} - \bar{X})$$

3) автокорреляционная функция:

$$\hat{\rho}_k = \frac{\hat{\gamma}_k}{\hat{\gamma}_0}, k = 0, 1, \dots$$

Оценка автокорреляционной функции $\hat{\rho}_k$ служит заменой ρ_k, тогда итеративная формула вычисления H принимает вид:

$$\widehat{H}_{i+1} = \sqrt{(\hat{\rho}_k k^{2-2\widehat{H}_i} + \widehat{H}_i) \cdot 0{,}5}, \qquad k \to \infty$$

Результаты эксперимента показали, что итеративная оценка показателя Херста имеет высокую скорость и точность, а также меньшие доверительные интервалы для нормальных значений по сравнению с методами VTP (variance-time plot), широко используемым time domain estimation, новым whittle estimator, который лучше метода вейвлет-анализа.

Для длинномасштабного корреляционного процесса полагается $\widehat{H}_0 = 0{,}5$.

Условием выполнения итеративной формулы для $\widehat{H}_{i+1}$ является то, что $k \to \infty$, однако результаты эксперимента показывают, что при $k = 1$ с помощью этой формулы можно получить показатель Херста с достаточной точностью, сократив при этом значительное число вычислений. Кроме того, результат неидеален, даже если k достаточно большое, поэтому принимается $k = 1$, и формула принимает упрощенный вид:

$$\widehat{H}_{i+1} = \sqrt{(\hat{\rho}_1 + \widehat{H}_i) \cdot 0{,}5}$$

В штатном режиме сетевой трафик удовлетворяет дневному шаблону. Для снижения влияния периодичности сетевого трафика на оценку показателя Херста необходимо обрабатывать трафик в различные периоды времени.

На практике сначала в течение недели вычисляются четыре вышеупомянутые метрики нормального трафика. Затем вычисляют средние за неделю нормальные значения показателей Херста для четырех метрик трафика для каждого дня. Далее применяется эффективный метод Kettani и Gubner для вычисления 98% доверительных интервалов показателей Херста $(0{,}5 \le H \le 0{,}95)$. Таким образом, устанавливается начальное состояние модели нормального трафика. При обнаружении в режиме реального времени значение текущего вычисленного показателя Херста проверяется на попадание в доверительный интервал нормальной модели трафика для каждой метрики. Если значение попадает в доверительный интервал, трафик считается нормальным, результат обнаружения – 0, в противном случае трафик считается аномальным, и результат обнаружения – 1. В первом случае необходимо обновить показатель Херста и доверительный интервал в нормальной модели трафика.

Метод нормализованной оценки безопасности основан на средневзвешенном методе для учета всех четырех метрик трафика. Уровень риска вычисляется следующим образом:

$$F_{traffic} = \sum_{i=1}^{4} w(i) \cdot F_{obs}(i), \qquad \sum_{i=1}^{4} w(i) = 1$$

$obs = \{1 - all\ packets, 2 - TCP\ packets,$
$3 - UDP\ packets, 4 - ARP\ packets\}$
$\mathrm{w} = \{0{,}4; 0{,}2; 0{,}2; 0{,}2\}$
$w(i)$ – вес $obs(i)$

Практическая часть

С целью проведения исследования было разработано программное обеспечение для фрактального анализа временных рядов (рис.3).

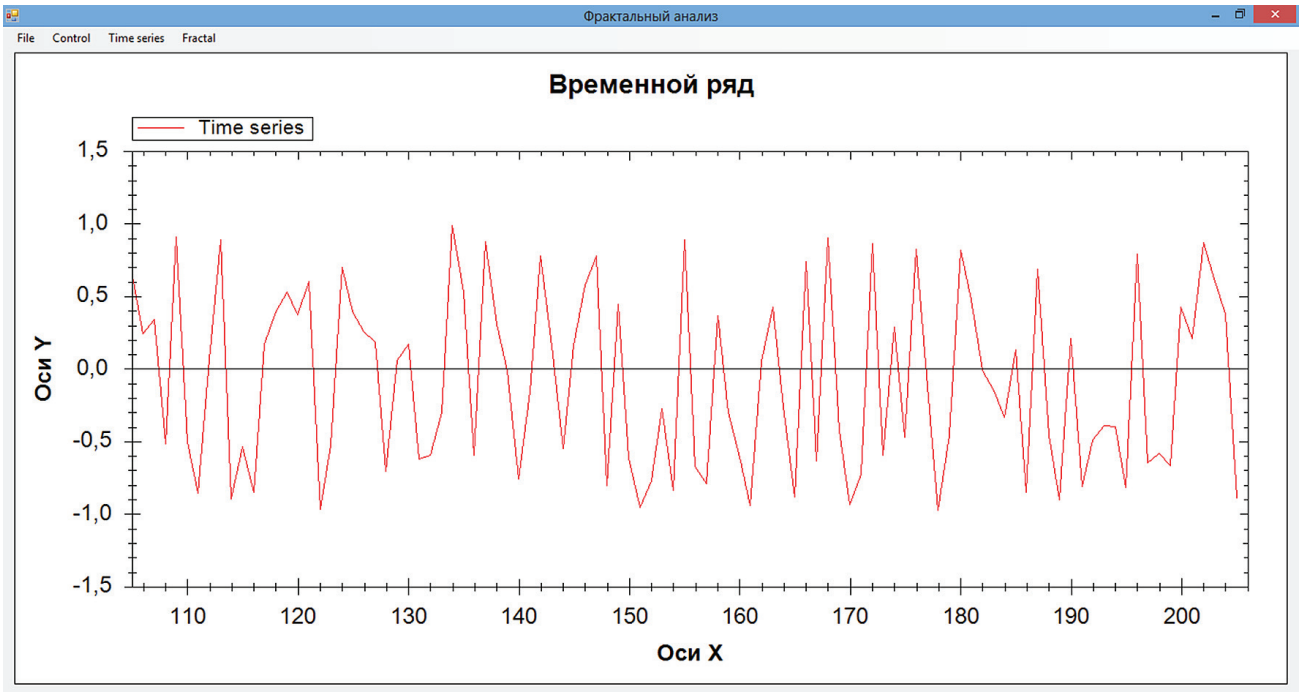

***Рис.3**. Общий вид разработанной программы*

Функциональные возможности:

1) моделирование временных рядов;

2) вычисление показателя Херста (H) методом R/S-анализа для заданного временного ряда.

Промоделирован временной ряд с равномерным распределением от 0 до 100 (рис. 4).

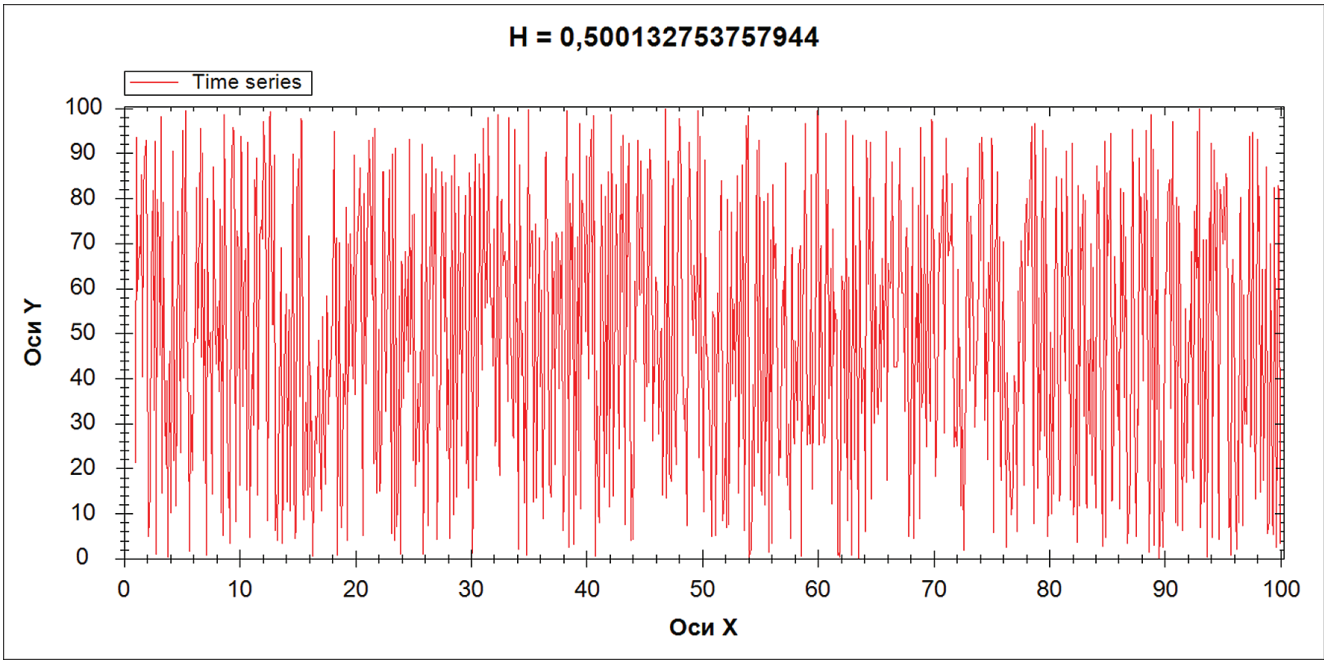

***Рис.4**. Равномерное распределение от 0 до 100*

Вычислены показатели Херста для временного ряда загруженности процессора при различных видах активности пользователя:

1) бездействие пользователя при отрисовке временного ряда загруженности процессора в реальном времени (рис.5):

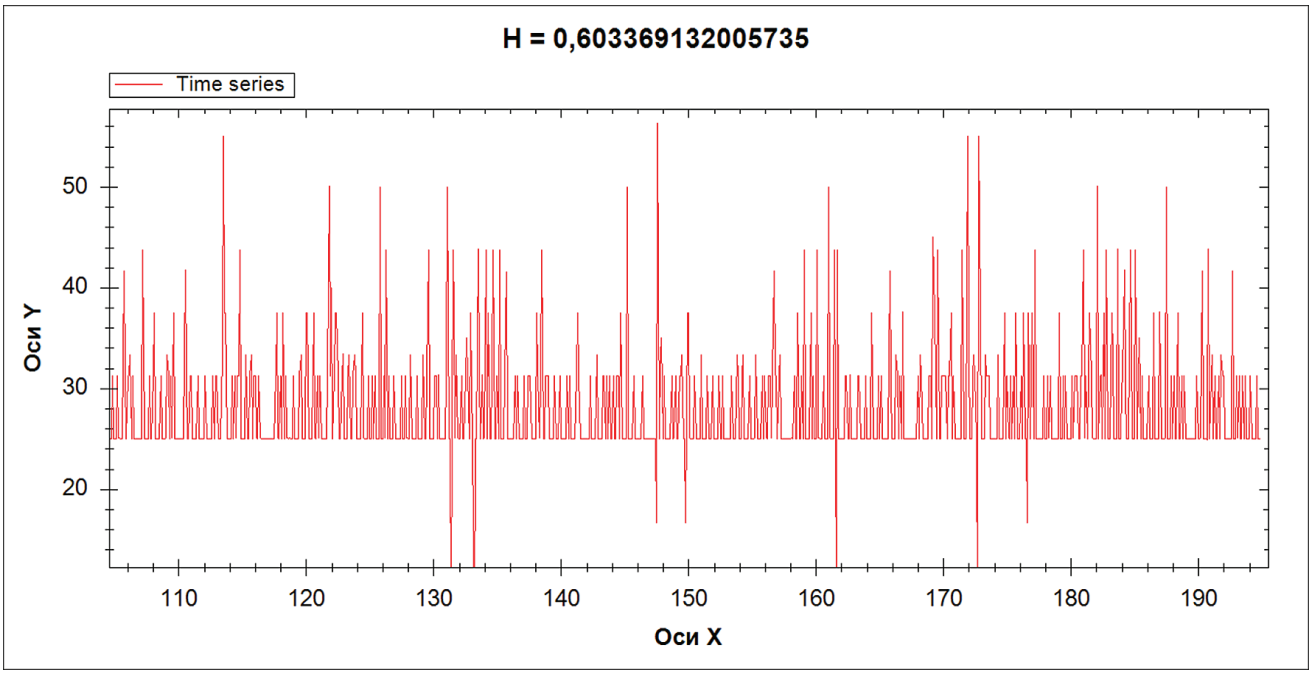

Рис.5. *Временной ряд загруженности процессора при отрисовке его графика*

2) работа пользователя, заключающаяся в открытии и чтении различных файлов, переходе по директориям (рис.6):

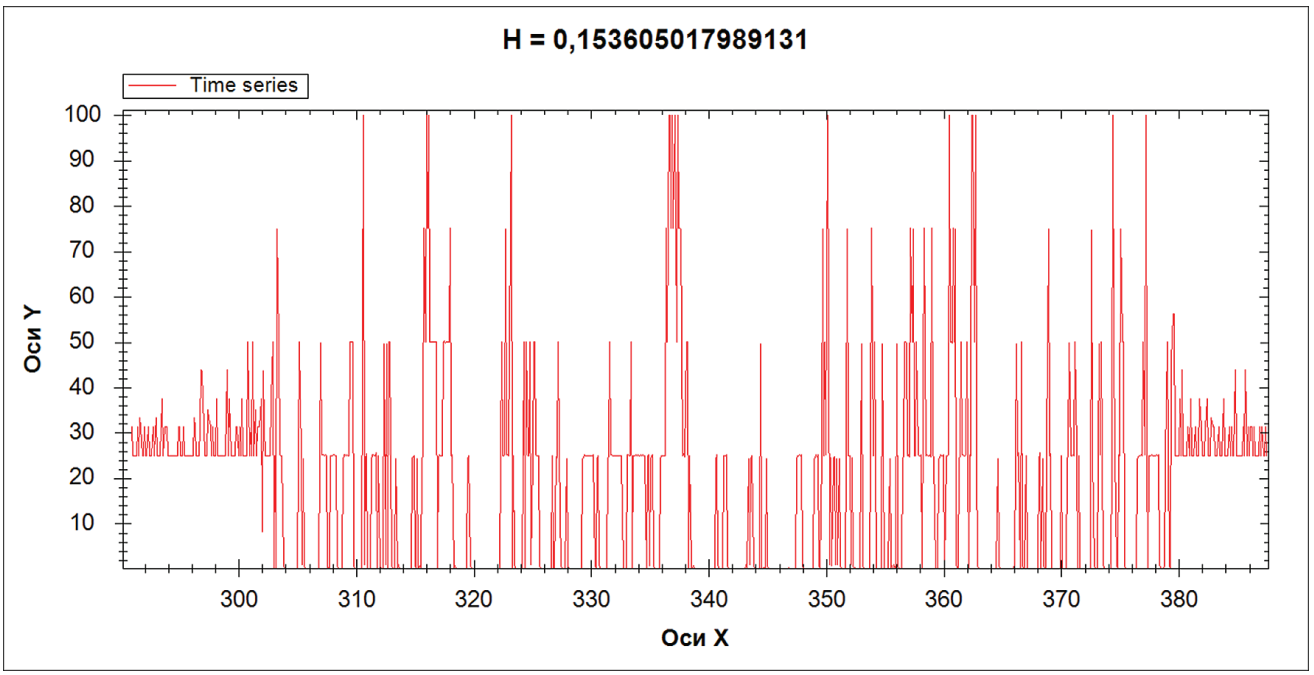

Рис.6. *Временной ряд загруженности процессора при открытии и чтении файлов и папок*

3) работа пользователя: набор текста в Microsoft Word (рис.7):

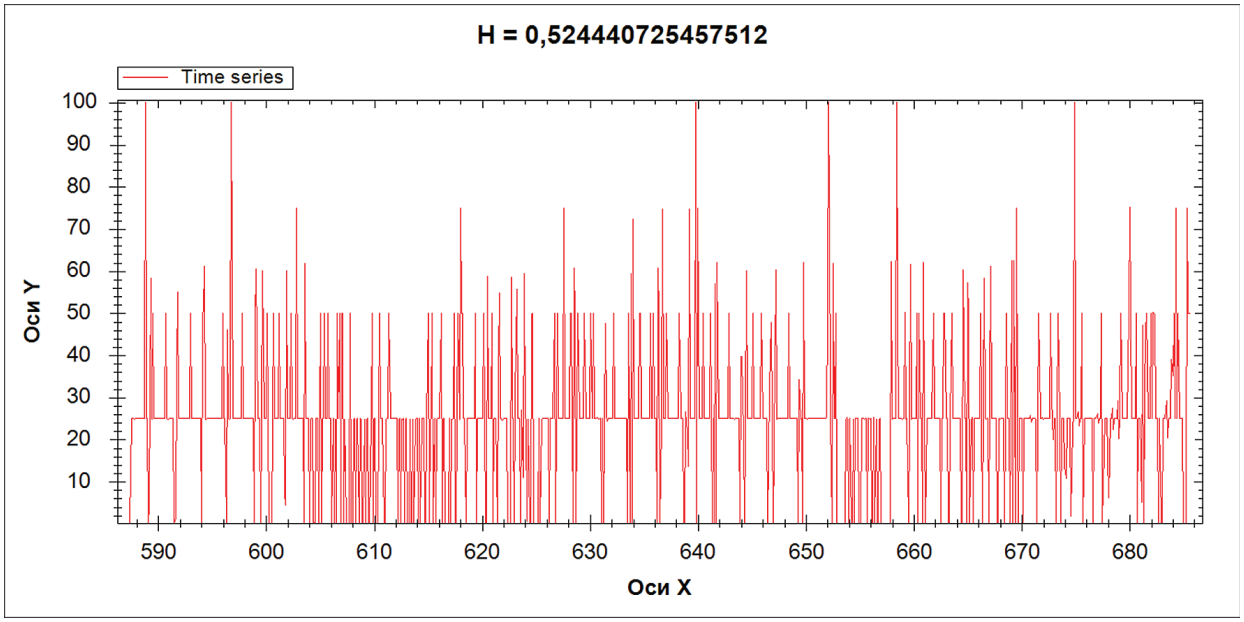

***Рис.7**. Временной ряд загруженности процессора при наборе текста в Microsoft Word*

4) проверка компьютера антивирусом Dr.Web (рис.8):

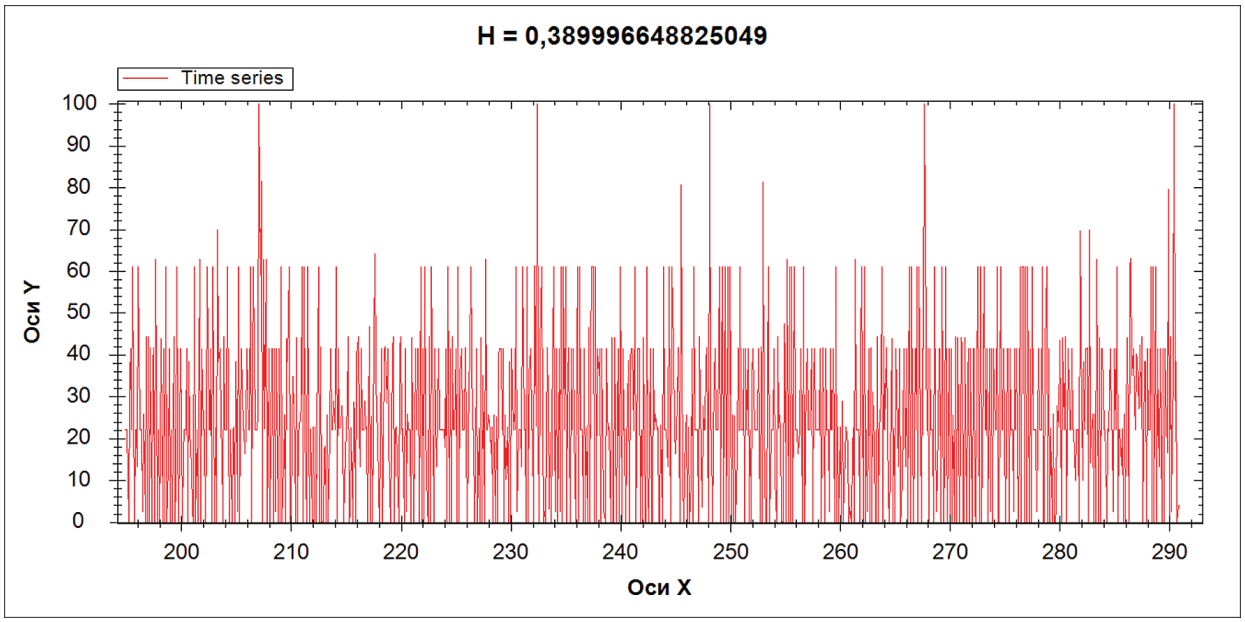

***Рис.8.** Временной ряд загруженности процессора при проверке файлов антивирусом*

Заключение

В данном обзоре речь идет в основном о сетевом трафике, для которого проводились многочисленные исследования, показавшие наличие у него свойства самоподобия, что позволяет использовать этот факт для создания модели нормального поведения.

В данной статье был проведен эксперимент для временного ряда загруженности процессора, фрактальные свойства которого неизвестны. Результаты показывают, что показатель Херста временного ряда данного параметра меняется при смене вида деятельности пользователя в широких пределах, что не позволяет сделать заключение о наличии или отсутствии самоподобия и делает невозможным обнаруживать аномалии, применяя только этот метод для данного параметра.

Литература:

1. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Москва. Горячая линия-Телеком. 2013. 220 с.
2. Шелухин О.И., Смольский С.М., Осин А.В. Самоподобие и фракталы. Телекоммуникационные приложения. Москва. Физматлит. 368 с.
3. Mazurek M., Pawel D. Network anomaly detection based on the statistical self-similarity factor for HTTP protocol.
4. Afshin Shaabany, Fatemeh Jamshidi, Network traffic deviation detection based on fractal dimension.
5. Chen Shi-wen, Wu Jiang-xing , Guo Tong, Lan Julong, Self-adaptive Detection Method for DDoS Attack Based on Fractional Fourier Transform and Self-similarity.
6. P. Ably, P. Flandrin, M. S. Taqqu, et al. Self-Similarity and long-range dependence through the wavelet lens [J]. In: Theory and Applications of Long Range Dependence, Boston: Birkhauser Press, 2002: 345-379.
7. J. Park and C. Park, Robust estimation of the Hurst parameter and selection of an onset scaling J. Statistica Sinica, 2009, 19 (4): 1531-1555.
8. P. Tarrio, A. M. Bernardos, J. R. Casar. Weighted Least Squares Techniques for Improved Received Signal Strength Based Localization[J]. Sensors 2011, 11: 8569-8592.
9. Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic.
10. Ruoyu Yan, Yingfeng Wang, Hurst parameter for security evaluation of LAN traffic.

References:

1. Sheluhin O.I., Sakalema D.G., Filinova A.S. Intrusion detection in computer networks (network anomalies). Textbook for universities. Grief UMO MO RF.
2. Sheluhin O.I., Sakalema D.G., Filinova A.S. Self-similarity and fractals. Telecommunication applications.
3. Mazurek M., Pawel D. Network anomaly detection based on the statistical self-similarity factor for HTTP protocol.
4. Afshin Shaabany, Fatemeh Jamshidi, Network traffic deviation detection based on fractal dimension.
5. Chen Shi-wen, Wu Jiang-xing , Guo Tong, Lan Julong, Self-adaptive Detection Method for DDoS Attack Based on Fractional Fourier Transform and Self-similarity.
6. P. Ably, P. Flandrin, M. S. Taqqu, et al. Self-Similarity and long-range dependence through the wavelet lens [J]. In: Theory and Applications of Long Range Dependence, Boston: Birkhauser Press, 2002: 345-379.
7. J. Park and C. Park, Robust estimation of the Hurst parameter and selection of an onset scaling [J]. Statistica Sinica, 2009, 19 (4): 1531-1555.
8. P. Tarrio, A. M. Bernardos, J. R. Casar. Weighted Least Squares Techniques for Improved Received Signal Strength Based Localization[J]. Sensors 2011, 11: 8569-8592.
9. Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic.
10. Ruoyu Yan, Yingfeng Wang, Hurst parameter for security evaluation of LAN traffic.