Оригинальная статья
https://doi.org/10.21683/1729-2646-2023-23-2-57-63

Подход к обнаружению аномалий в самоподобном сетевом трафике

An approach to detecting anomalies in a self-similar network traffic

Веселова В.А.[1], Коломойцев В.С.[1]*
Veselova V.A.[1], Kolomoytsev V.S.[1]*
[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, Российская Федерация
[1]Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russian Federation
**Dekoros@guap.ru*

Веселова В.А.

Коломойцев В.С.

Резюме. Цель. *Воздействия кибератак приводят к выводу из эксплуатации элементов сети, хищению информации и другим неправомерным действиям. Зачастую кибератаки сопровождаются нехарактерной активностью трафика и появлением в нем аномалий. Целью статьи является разработка подхода к выявлению аномалий в сетевом трафике за счет определения степени самоподобия трафика с использованием фрактального анализа и статистических методов.* **Методы.** *В статье применяются методы математической статистики, математического анализа, фрактального анализа.* **Результаты.** *Предложен подход к обнаружению аномалий в сетевом трафике путем оценки свойства самоподобия и использования статистических методов для повышения точности определения кибератак. На первом этапе вычисляется показатель Херста для эталонного трафика. На втором этапе реальный трафик разбивается на оптимальные временные интервалы, для каждого интервала считается показатель Херста. Если выявленное значение показателя Херста отличается от значения, полученного для эталонного трафика, принимается решение о наличии аномалий. На заключительном этапе применяется статистический анализ для определения точного места аномалии. Проведен анализ фрактальных и статистических методов, в результате которого были определены более эффективные методы для использования в предлагаемом подходе. Для фрактального анализа предложен метод DFA, для статистического – ARFIMA.* **Заключение.** *Предлагаемый подход позволяет обнаружить кибератаки в реальном или близком к реальному масштабе времени.*

Abstract. Aim. *The effects of cyber attacks cause failures of network elements, theft of information and other unlawful actions. Cyber attacks are often accompanied by untypical traffic activity and anomalies. The paper aims to develop an approach to detecting anomalies in network traffic by identifying the degree of self-similarity of the traffic using fractal analysis and statistical methods.* **Methods.** *The paper uses methods of mathematical statistics, mathematical analysis, fractal analysis.* **Results.** *The paper suggests an approach to identifying anomalies in network traffic by evaluating self-similarity and using statistical methods for improving the accuracy of cyber attack detection. At the first stage, the Hurst exponent is calculated for the reference traffic. At the second stage, actual traffic is divided into optimal time intervals; for each interval, the Hurst exponent is calculated. If the identified value of the Hurst exponent differs from the one obtained for the reference traffic, it is decided that there is an anomaly. At the final stage, statistical analysis is used in order to precisely localise the anomaly. The authors analysed fractal and statistical methods that resulted in the identification of more efficient methods to be used as part of the proposed approach. For fractal analysis, the DFA method was proposed, while for statistical analysis, the ARFIMA method was proposed.* **Conclusion.** *The suggested approach allows identifying cyber attacks in real time or near-real time.*

Ключевые слова: *временной ряд, фрактальный анализ, статистический анализ, показатель Херста, аномалии, сетевой трафик.*
Keywords: *time series, fractal analysis, statistical analysis, Hurst exponent, anomalies, network traffic.*

Для цитирования: *Веселова В.А., Коломойцев В.С. Подход к обнаружению аномалий в самоподобном сетевом трафике // Надежность. 2023. №2. С. 57-63. https://doi.org/10.21683/1729-2646-2023-23-2-57-63*
For citation: *Veselova V.A., Kolomoytsev V.S. An approach to detecting anomalies in a self-similar network traffic. Dependability 2023;2:57-63. https://doi.org/10.21683/1729-2646-2023-23-2-57-63*

Поступила: *09.02.2023* / **После доработки:** *26.04.2023* / **К печати:** *15.06.2023*
Received on: *09.02.2023/* **Revised on:** *26.04.2023 /* **For printing:** *15.06.2023*

Введение

Использование повсеместно компьютерных сетей сопровождается генерацией большего потока сетевого трафика. Злоумышленники с целью сбора и хищения информации, вывода инфраструктуры из строя применяют кибератаки, однако их атаки могут быть не замечены в общем потоке трафика и привести к инцидентам в компьютерных сетях. Поэтому важной задачей является быстрое определение наличия аномалий в сетевом трафике и реагирования на них.

В исследованиях показано, что объединенный из нескольких источников трафик становится сильно автокоррелированным с долговременной зависимостью [1-6]. Таким образом, сетевой трафик способен сохранять свой характер при изменении масштаба времени. Поэтому его принято рассматривать, как самоподобный нестационарный процесс. Методы анализа самоподобных процессов основываются на фрактальном анализе [4-7]. В нескольких научных работах отмечается эффективное применение фрактального анализа для обнаружения аномалий сетевого трафика как общего характера, так и для обнаружения DDoS-атак [1–13].

Коэффициент Херста (H) является важнейшим параметром, характеризующим степень самоподобия. При $0{,}5 < H \leq 1{,}0$ процесс является строго самоподобным, при $H = 0{,}5$ – случайный процесс, при $0 \leq H < 0{,}5$ процесс не является самоподобным [1].

Данная работа посвящена разработке методики выявления аномалий в сетевом трафике за счет определения степени самоподобия трафика с использованием фрактального анализа и статистических методов.

Методы фрактального анализа

Для определения самоподобия трафика и значения показателя Херста используются R/S анализ и метод детрендированного флуктуационного анализа (Detrended Fluctuation Analysis, DFA) [2, 6, 7].

R/S анализ. Показатель Херста (H) определяется в терминах асимптотического поведения масштабированного диапазона, как функции отрезка времени временного ряда, следующим образом: $R / S = C \cdot n^H$. В указанной формуле R – размах накопленных отклонений n значений от среднего значения ряда, S – среднеквадратическое отклонение ряда наблюдений, n – число промежутков времени, C – заданная константа, положительное число (автор показателя Херст эмпирически рассчитал эту константу для сравнительно краткосрочных временных рядов природных явлений как 0,5) [7].

Этот метод может быть легко применен на практике. Обладая достаточным уровнем надежности, в то же время метод является простым в применении. Однако данный метод крайне чувствителен к длине ряда [6, 7].

Метод DFA. Метод детрендированного флуктуационного анализа в настоящее время является основным методом определения самоподобия для нестационарных временных рядов. В исследованиях показано, что метод способен оценивать H с высокой точностью и относительной простотой [8, 9, 10, 11]. Алгоритм DFA заключается в вычислении флуктуационной функции: $F(\delta) = \sqrt{\frac{1}{\delta}\sum_{t=1}^{\delta}(y(t) - Y_m(t))^2}$, где $Y_m(t)$ – локальный m-полиномиальный тренд в пределах данного сегмента, $y(t)$ – кумулятивный ряд, разбитый на N сегментов длиной δ. Для самоподобных процессов имеет место степенная зависимость: $\overline{F(\delta)} \sim \delta^H$. H определяется, как коэффициент при независимой переменной в уравнении линейной регрессии: $\ln \overline{F(\delta)} = H \cdot \ln \delta + b$, где b – свободный член.

При проведении сравнительных исследований эффективности работы рассмотренных методов оценивания H показано, что для стационарных временных рядов пригодны оба метода (R/S анализ и метод DFA) [7]. R/S анализ для временных рядов малой длины дает большую погрешность в результатах, чем метод DFA [7]. Также R/S анализ не применим для нестационарных рядов, так как дает большую погрешность, достигающую 20-30% [7]. Поэтому для нахождения показателя H в нестационарных процессах, к которым относиться и сетевой трафик, предполагается использовать метод DFA.

Статистические методы анализа сетевого трафика

Исследуем статистические методы анализа для прогнозирования ожидаемого значения сетевого трафика.

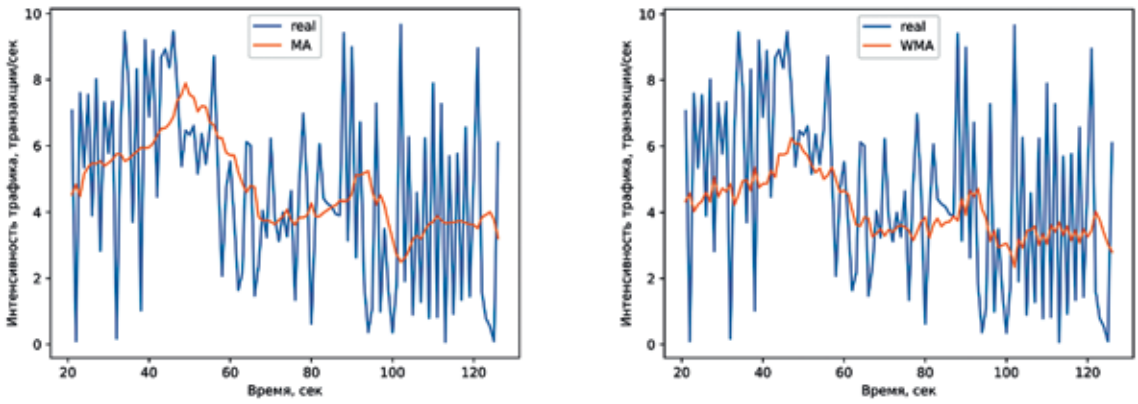
MA. Скользящее среднее (англ. moving average, MA) – общее название для семейства функций, значения которых в каждой точке определения равны некоторому среднему значению исходной функции за предыдущий период. Скользящее среднее (MA) можно рассчитать по формуле: $MA = \left(\sum_{i=0}^{n} p_i\right) \Big/ N$, где p_i – значения в периоде n, N – количество значений в периоде n.

На рис. 1а представлены результаты вычисления скользящего среднего для временного ряда. Метод MA отличается повышенной чувствительностью к выбросам данных. Кратковременный, но очень сильный всплеск приводит к достаточному длительному и существенному изменению амплитуды скользящего среднего Метод MA способен прогнозировать поведение трафика только на ближайшие периоды времени [13, 14].

WMA. Взвешенное скользящее среднее (англ. weighted moving average, WMA) – скользящее среднее, при вычислении которого вес каждого члена исходной функции, начиная с меньшего, равен соответствующему члену арифметической прогрессии. Вычислить взвешенное скользящее среднее можно по следующей формуле:

$$WMA = \sum_{i=0}^{n} w_i \cdot p_i \Big/ \sum_{i=0}^{n} w_i,$$

где p_i – значения в периоде n, w_i – вес значения.



а) б)

Рис. 1. Результаты применения статистических методов анализа: (а) – метод MA; (б) – метод WMA

На рис. 1б представлены результаты вычисления взвешенного скользящего среднего для временного ряда.

Метод WMA позволяет учитывать временный контекст. Чем раньше произошло событие, тем меньше его влияние на прогнозируемое событие. Метод WMA более чувствителен к колебаниям (см. рис. 1а и рис. 1б). Показано, что линия MA имеет более сглаженный характер, чем WMA.

ARIMA. ARIMA (англ. autoregressive integrated moving average) – интегрированная модель авторегрессии скользящего среднего – модель и методология анализа временных рядов [15]. ARIMA, представляет собой алгоритм прогнозирования, основанный на концепции, согласно которой данные предыдущих значений временного ряда могут использоваться только для прогнозирования будущих значений [12]. AR-часть ARIMA указывает, что изменяющаяся переменная, представляющая интерес, регрессирует по своим собственным предшествующим значениям. MA-часть указывает, что ошибка регрессии на самом деле представляет собой линейную комбинацию членов ошибки, значения которых произошли одновременно и в разное время в прошлом. I-часть (для «интегрированного») указывает, что значения данных были заменены разницей между их значениями и предыдущими значениями. Цель каждой из этих функций сделать так, чтобы модель как можно лучше соответствовала данным.

Модель ARIMA (p, d, q) для нестационарного временного ряда X_t имеет вид: $\Delta^d X_t = c + \sum_{i=1}^{p} a_i \Delta^d X_{t-1} + \sum_{j=1}^{q} b_j \varepsilon_{t-j} + \varepsilon_t$, где ε_t – стационарный временной ряд, c, a_i, b_j – параметры модели, Δ^d – оператор разности временного ряда порядка d.

На рис. 2 представлены результаты вычисления ARIMA для временного ряда. Из графика видно, что при помощи ARIMA можно спрогнозировать ожидаемые значения временного ряда с высокой степенью точности [16, 17].

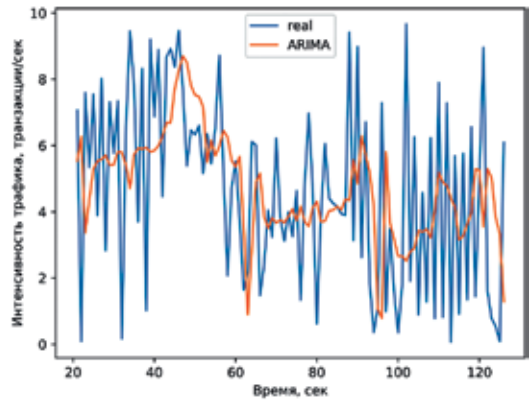


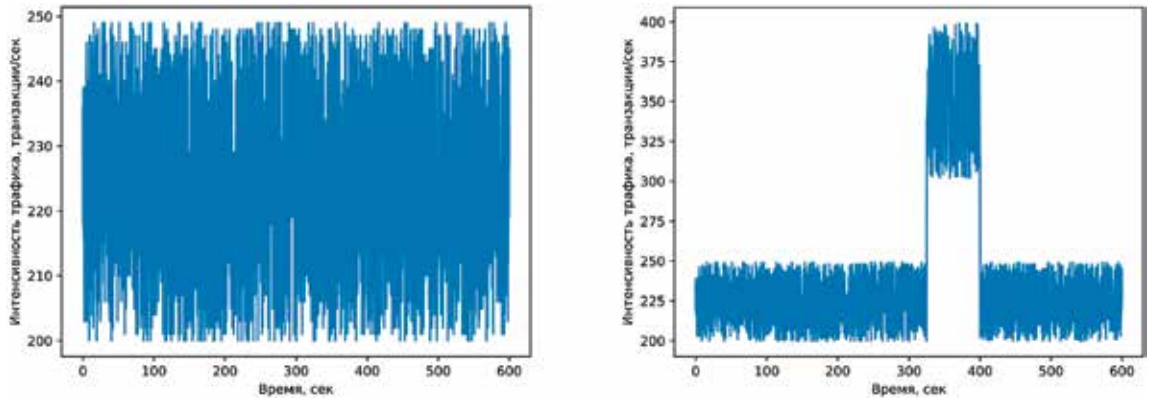
Рис. 2. Результаты применения ARIMA

ARFIMA. ARFIMA (p, d, q) – процесс авторегрессии дробного интегрированного скользящего среднего. Основное преимущество модели ARFIMA является то, что данный подход лучше работает при оценке феномена длительной памяти и производится оценка дробного параметра с использованием различных методов [15].

Модель ARFIMA (p, d, q) имеет тот же вид, что ARIMA. Единственным отличием между двумя моделями заключается в том, что d может принимать дробные значения в модели ARFIMA, в то время как в ARIMA модели может быть только целым [18]. Исследования показали, что степень разности связана с показателем

Табл. 1. Оценка статистических методов

Метод	MA	WMA	ARIMA	ARFIMA
Сложность	Низкая	Низкая	Средняя	Средняя
Точность	Низкая	Низкая	Высокая	Высокая
Применение к нестационарным моделям	–	–	+	+
Возможность использования метрик фрактального анализа	–	–	–	+



а) б)

Рис. 3. Интенсивность трафика: а) – эталонного; б) – с DDoS-атакой

Херста отношением: $d=H-0{,}5$. Таким образом, предполагается, что модель ARFIMA способна спрогнозировать более точное ожидаемое значение сетевого трафика, чем при использовании модели ARIMA.

В табл. 1 представлена оценка сложности реализации и точность применения статистических методов для поиска аномалий во временных рядах. Оценка сложности и точности методов проводилась на основе полученных результатов прогнозирования временных рядов различными статистическими методами. На основе полученных результатов можно сделать вывод, что прогнозирование с помощью ARIMA дает более точные результаты, чем MA и WMA, однако ARIMA и ARFIMA имеют более сложно математическую модель.

Описание метода детектирования аномалий

Исследовав существующие методы фрактального и статистического анализа, с помощью которых можно определить характеристики трафика, сигнализирующие об изменениях в его структуре, предложим следующий подход детектирования аномалий сетевого трафика, основанный на фрактальном и статистическом анализе.

На первом этапе (вспомогательном) анализируется самоподобные свойства эталонного трафика. В эталонном трафике отсутствуют аномалии. В результате этого анализа определяется значение показателя Херста, соответствующее эталонному трафику.

На втором этапе (основном) анализируется самоподобные свойства реального трафика, для которого могут быть характерны аномалии, вызванные воздействием кибератак. При этом используются те же методы определения значения показателя Херста, что и для эталонного трафика. Если полученное значение показателя Херста отличается от значения, полученного для эталонного трафика, принимается решение о наличии аномалий в реальном трафике, которые могут быть вызваны воздействием кибератак. Кроме того, на этом же этапе определяется минимальный размер группы пакетов, достаточный для точной оценки показателя самоподобия. Чем меньше размер группы, тем меньше времени потребуется для детектирования кибератаки. Однако при слишком маленьких размерах пакетов может ухудшаться точность детектирования аномалии.

Значение показателя Херста указывает на наличие или отсутствие самоподобия трафика. Отклонение показателя Херста реального трафика от эталонного может свидетельствовать об изменении фактуры трафика, которая может быть вызвана кибератакой в рассматриваемом диапазоне сетевого трафика. Для точного определения времени возникновения аномалии в рассматриваемом диапазоне, предлагается использовать статистические методы.

На третьем этапе на основе методов математической статистики осуществляется определение место аномалии и классификация кибератак с целью реализации мер защиты.

На рис. 3а представлена интенсивность эталонного трафика, измеряемая в количестве транзакций в секунду. Интенсивность имеет равномерный характер. На рис. 3б представлена интенсивность трафика с DDoS-атакой в промежутке времени с 325 до 400 секунд – в данный интервал времени наблюдается резкое увеличение интенсивности трафика.

Для эталонного и трафика с аномалией был рассчитан показатель Херста с помощью метода DFA. Для эталонного трафика была проведена оценка показателя самоподобия всего трафика без деления на группы ($H = 0{,}99$), трафик с аномалией был разделен на группы по 120 секунд, для каждой группы была проведена оценка показателя самоподобия.

Сравнение показателя Херста эталонного и реального трафиков проводится с помощью средней абсолютной ошибки (MAPE), по следующей формуле:

$$MAPE = \frac{1}{N}\sum_{t=1}^{N}\frac{\left|Z(t)-\hat{Z}(t)\right|}{Z(t)}\cdot 100\%, \qquad (1)$$

где $Z(t)$ – фактическое значение временного ряда, а $\hat{Z}(t)$ – прогнозируемое, N – количество отчетов.

Если значение MAPE превышает 5%, предполагается, что исследуемый временной отрезок реального трафика имеет аномалию.

На рис. 4 представлен график с полученными результатами показателя Херста для эталонного трафика и трафика с аномалией. Видно, что в интервал времени с 240 по 480 секунд показатель Херста трафика с аномалией отличается более чем на 5% от показателя Херста эталонного трафика, что свидетельствует об изменении самоподобной структуры трафика, что вызвано предполагаемой атакой.

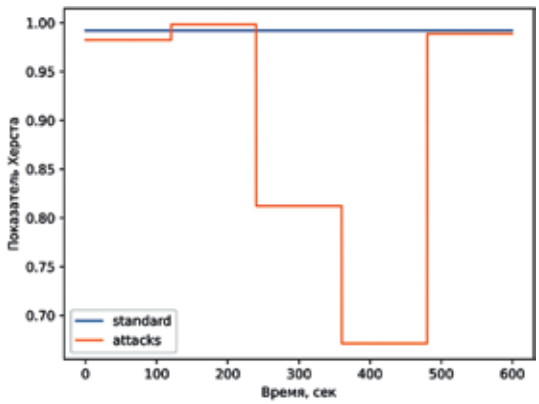


Рис. 4. Показатель Херста эталонного трафика и трафика с аномалией.

Из рассмотренных статистических методов для заключительного этапа детектирования точного времени появления аномалии предлагается использовать модель ARFIMA, которая способна спрогнозировать более точное ожидаемое значение сетевого трафика за счет использование дополнительного параметра *d*, который определяется, как *d*=*H*–0,5. На заключительной этапе, сравнение спрогнозированных данных, осуществляется с помощью вычисления MAPE по (1). Если MAPE превышает 10%, то данная точка определяется как начало/конец аномалии.

На рис. 5 представлены результаты применение модели ARFIMA для интервала времени (240-400 секунд), детектированного фрактальным анализом, красными точками на графике отмечены места, где спрогнозированные значения отличаются от реальных больше установленного порога в 10%. Первая группа точек в районе 330 секунд указывает на начало атаки, вторая группа в 400 секунд указывает на окончание атаки.

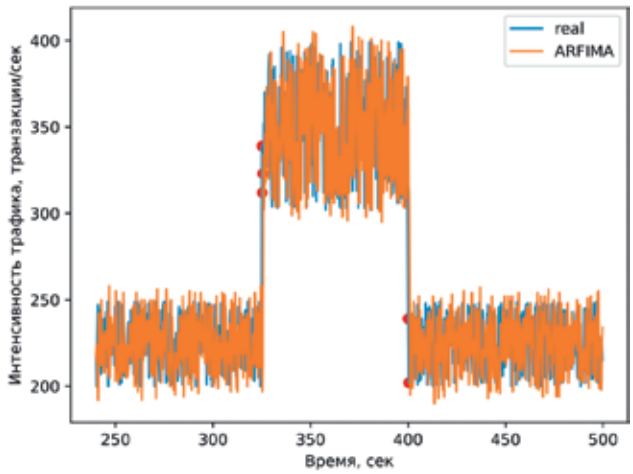


Рис. 5. Детектирование атаки с помощью ARFIMA.

Заключение

В результате исследования был предложен подход к обнаружению аномалий в самоподобном сетевом трафике, который заключается в определении показателя самоподобия, определяемый показателем Херста с помощью фрактального анализа и дополнительного детектирования аномалии с помощью статистического анализа. Преимущество описанного метода определения аномалий в сетевом трафике от отдельных методов фрактального или статистического анализа заключается в том, что данный метод, использующий гибридный подход и подобранные параметры трафика, позволяет выявлять в реальном и близком к реальному масштабу времени воздействие кибератак.

В работе был проведен сравнительный анализ фрактальных и статистических методов, в результате которого были определены более эффективные методы для использования в предлагаемом подходе. Для фрактального анализа выбран метод DFA, для статистического – ARFIMA. Метод DFA при тестировании фрактальных методов, позволяющих исследовать долговременные зависимости в трафике компьютерной сети, является более эффективным, чем R/S анализ, из-за его возможности обрабатывать не только стационарные, но и нестационарные ряды с высокой точностью. Модель ARFIMA позволяет спрогнозировать точные значения за счет использования дополнительного значения оценки длительной памяти, который задается фрактальной размерностью, определяемой при фрактальном анализе. Таким образом, использование предложенного гибридного подхода, включающих DFA и ARFIMA методы, позволяет повысить точность поиска аномалий в сетевом трафике.

Библиографический список

1. Перов Р.А., Лаута О.С., Крибель О.М., Федулов Ю.М. Комплексная методика обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Наукоемкие технологии в космических исследованиях Земли. 2022. № 2. С. 44-51. DOI: 10.36724/2409-5419-2022-14-2-44-51

2. Усков Е.Д., Корепанова Н.Л. Анализ информативных признаков аномалий сетевого трафика корпоративных сетей // Современные инновации. 2019. № 3(31). С. 13-16.

3. Суворов А.О., Суворова В.А. Интеллектуальный анализ сетевого трафика для идентификации компьютерных вторжений // Искусственный интеллект и принятие решений. 2019. № 1. С. 62-73. DOI: 10.14357/20718594190106

4. Барсуков И.С., Ряполов М.П., Бобрешов А.М. Алгоритм анализа фрактальных свойств трафика для

обнаружения сетевых аномалий // Радиолокация, навигация, связь: Сборник трудов XXVI Международной научно-технической конференции. 2020. Т. 4. С. 302-311.

5. Барсуков И.С., Ряполов М.П., Бобрешов А.М. Использование фрактальных свойств сетевого трафика для обнаружения LDoS-атак в клиент-серверных сетях // Нелинейный мир. 2019. Т. 17. № 2. С. 34-39. DOI: 10.18127/j20700970-201902-04

6. Барсуков И.С., Ряполов М.П. Использование фрактальных свойств трафика в цифровых сетях связи для детектирования сетевых аномалий // Вестник Воронежского государственного университета. 2018. № 3. С. 73-81.

7. Муллер Н.В., Младова Т.А. Комплексный анализ временных рядов с помощью фрактального и вейвлет-анализа // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2020. № 7(47). С. 20-25.

8. Латышев О.Г., Казак О.О. Тренд-анализ свойств породного массива на основе фрактального представления пространственных рядов // Известия Уральского государственного горного университета. 2018. № 2(50). С. 79-84. DOI: 10.21440/2307-2091-2018-2-79-84

9. Тумбинская М.В., Баянов Б.И., Рахимов Р.Ж. и др. Анализ и прогнозирование вредоносного сетевого трафика в облачных сервисах // Бизнес-информатика. 2019. Т. 13. № 1. С. 71-81.

10. Крибель А.М., Перов Р.А., Лаута О.С. и др. Модель выявления аномалий в сетевом трафике сети передачи данных в условиях компьютерных атак // Известия Тульского государственного университета. Технические науки. 2022. № 5. С. 228-239.

11. Лаута О.С., Карпов М.А., Крибель А.М. и др. Анализ процесса самоподобия сетевого трафика как подход к обнаружению кибератак на компьютерные сети / В сб.: Состояние и перспективы развития современной науки по направлению «Информационная безопасность», 21–22 апреля 2021 года, Анапа. С. 311-327.

12. Татарникова Т.М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5 (96). С. 35-43.

13. Джеффри Оуэн Кац, Донна Л., Мак Кормик. Энциклопедия торговых стратегий. М., Альпина Паблишер, 2002. 400 с.

14. Ямкин В.Н. Финансовый дилинг. Технический анализ. М., ИКФ Омег–Л., 2005. 480 с.

15. Гребенщикова А.А., Елагин В.С. Обзор модели авторегрессии и проинтегрированного скользящего среднего ARIMA для прогнозирования сетевого трафика. / В сб.: Актуальные проблемы инфотелекоммуникаций в науке и образовании, Санкт-Петербург, 24–25 февраля 2021 года. Т. 1. С-Пб: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. С. 266-271.

16. Дюсекенов Д.С., Тюменцев Е.А. Сравнительный анализ рекуррентных нейронных сетей и модели авторегрессии ARIMA при прогнозировании нестационарных временных рядов / В сб.: Прикладная математика и фундаментальная информатика, Омск, 16–21 мая 2022 года. Омск: Омский государственный технический университет, 2022. С. 86-87.

17. Симонов П. М., Гарафутдинов Р. В. Моделирование и прогнозирование динамики курсов финансовых инструментов с применением эконометрических моделей и фрактального анализа. Вестник Пермского университета. Серия: Экономика, 2019, т. 14, № 2, с. 268-288. doi:10.17072/1994-9960-2019-2-268-288.

18. Bukhari A.H., Raja M.A.Z., Sulaiman M. et al. Fractional Neuro-Sequential ARFIMA-LSTM for Financial Market Forecasting // IEEE Access. 2020. Vol. 8. Pp. 71326-71338. DOI: 10.1109/ACCESS.2020.2985763.

References

1. Perov R.A., Lauta O.S., Kribel A.M., Fedulov Yu.V. Complex method for detecting cyber attacks based on integration of fractal analysis and statistical methods. *High Tech in Earth Space Research* 2022;2:44-51. DOI: 10.36724/2409-5419-2022-14-2-44-51. (in Russ.)

2. Uskov E.D., Korepanova N.L. [Analysis of informative features of network traffic anomalies in corporate networks]. *Modern innovations* 2019;3(31):13-16. (in Russ.)

3. Suvorov A.O., Suvorova V.A. [Data mining of network traffic for identifying computer intrusions]. *Iskusstvenniy Intellekt i Prinyatie Resheniy* 2019;1:62-73. DOI: 10.14357/20718594190106. (in Russ.)

4. Barsukov I.S., Riapolov M.P., Bobreshov A.M. [An algorithm for analysing fractal properties of traffic for detecting network anomalies]. [Radar location, navigation, communication: Proceedings of the XXVI International Science and Engineering Conference] 2020;4:302-311. (in Russ.)

5. Barsukov I.S., Riapolov M.P., Bobreshov A.M. [Using fractal properties of network traffic for detecting LDoS attacks in dedicated server networks]. *Nelineyny mir* 2019;17(2):34-39. DOI: 10.18127/j20700970-201902-04. (in Russ.)

6. Barsukov I.S., Riapolov M.P. [Using fractal properties of traffic in digital communication networks for detecting network anomalies]. *Proceedings of Voronezh State University* 2018;3:73-81. (in Russ.)

7. Muller N.V., Mladova T.A. The complex analysis of time series using fractal and wavelet analysis. *Scholarly Notes of Komsomolsk-na-Amure State Technical University* 2020;7(47):20-25. (in Russ.)

8. Latyshev O.G., Kazak O.O. Trend analysis of the rock mass properties on the basis of fractal representation of spatial ranges. *News of the Ural State Mining University* 2018;2(50):79-84. DOI: 10.21440/2307-2091-2018-2-79-84. (in Russ.)

9. Tumbinskaya M.V., Bayanov B.I., Rakhimov R.Zh. at al. [Analysis and prediction of malicious network traffic in cloud services]. *Biznes-informatika* 2019;13(1):71-81. (in Russ.)

10. Kribel A.M., Perov R.A., Lauta O.S. et al. [Model of identifying anomalies in network traffic of a data communication network amid computer attacks]. *News of the Tula state university. Technical sciences* 2022;5:228-239. (in Russ.)

11. Lauta O.S., Karpov M.A., Kribel A.M. et al. [Analysis of the process of self-similarity of network traffic as an approach to identifying cyber attacks against computer networks]. In: [State of the art and prospects of development of the modern information security science, April 21-22, 2021, Anapa]. P. 311-327. (in Russ.)

12. Tatarnikova T.M. Statistical methods for studying network traffic. *Informatsionno-upravliaiushchie sistemy [Information and Control Systems]* 2018;5:35-43. (in Russ.)

13. Katz J.O., McCormick D.L. The Encyclopedia of Trading Strategies. Moscow: Alpina Publishing; 2002.

14. Yamkin V.N. [Financial dealing. A technical analysis]. Moscow: IKF Omeg-L; 2005. (in Russ.)

15. Grebenshchikova A.A., Yelagin V.S. [An overview of the autoregressive model and the ARIMA integrated running average for network traffic prediction]. In: [Topical problems of information telecommunications in science and education. Saint Petersburg, February 24-25, 2021. Vol. 1]. Saint Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications; 2021. P. 266-271. (in Russ.)

16. Diusekenov D.S., Tiumentsev E.A. [A comparative analysis of recurrent neural networks and the ARIMA autoregressive model with regard to the prediction of nonstationary time series]. In: [Applied mathematics and fundamental computer science. Omsk, May 16-21, 2022]. Omsk: Omsk State Technical University; 2022. P. 86-87. (in Russ.)

17. Simonov P.M., Garafutdinov R.V. [Simulation and prediction of financial instrument rates using econometric models and fractal analysis]. *Perm University Herald. Economy* 2019;14(2):268-288. doi:10.17072/1994-9960-2019-2-268-288. (in Russ.)

18. Bukhari A.H., Raja M.A.Z., Sulaiman M. et al. Fractional Neuro-Sequential ARFIMA-LSTM for Financial Market Forecasting. IEEE Access 2020;8:71326-71338. DOI: 10.1109/ACCESS.2020.2985763.

Сведения об авторах

Веселова Виктория Алексеевна – магистрант, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, Российская Федерация, e-mail: viktoriavslv44@gmail.com.

Коломойцев Владимир Сергеевич – доцент, кандидат технических наук, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, Российская Федерация, e-mail: Dekoros@guap.ru

About the authors

Viktoria A. Veselova, Master Student, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russian Federation, e-mail: viktoriavslv44@gmail.com.

Vladimir S. Kolomoytsev, Associate Professor, Candidate of Engineering, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russian Federation, e-mail: Dekoros@guap.ru.

Вклад авторов в статью

Веселова В.А. – анализ литературы по теме исследования, проведено сравнение возможностей статистических и фрактальных методов анализа трафика, выполнены необходимые для исследования расчеты.

Коломойцев В.С. – предложен гибридный метод, проведено исследование эффективности применения предложенного метода.

Конфликт интересов

Авторы заявляет об отсутствии конфликта интересов.