## Д. В. Ложкарев, магистрант

## BА. В. Коробейников, кандидат технических наук, доцент

## Е. А. Филиппова, магистрант

## кафедра «Программное обеспечение»

## Ижевский государственный технический университет имени М. Т. Калашникова

## [[1]](#footnote-1)©

## D. V. Lozhkarev, Master’s Degree Student

## A. V. Korobeynikov, PhD in Engineering, Associate Professor

## E. A. Filippova, Master’s Degree Student

## Department of Software

## Kalashnikov Izhevsk State Technical University

### Ритмографический анализ событий корпоративного сетовоготрафика системы *CISCO MARS*

**Rhythmographic analysis of the corporate network traffic**

**events of The CISCO MARS System**

*Рассматривается анализ вариабельности ритма событий сетевого трафика. За основу анализа ритма событий взята методика, применяемая для анализа вариабельности сердечного ритма человека. Изложена методика вычисления параметров и построения диаграмм ритмографического анализа. Практическое применение предлагаемого подхода в составе программного обеспечения анализа событий сетевого трафика позволит проводить оперативную оценку ритмографического характера отдельных событий и выполнять обнаружение сетевых аномалий.*

*Network traffic events rate variability is considered. The analysis is based on human heart rate variability analysis. The procedure of parameters calculation and diagram creating of rythmographic analysis is described. The considered method application in network events rate variability analysis software will allow rapid assessment rythmographic character of network events and detect network anomalies.*

**Ключевые слова:** вариабельность сердечного ритма; ВСР; вариабельность ритма сетевых событий; ритмография; обнаружений аномалий сетевого трафика.

**Keywords:** heart rate variability; HRV; network events rate variability; rythmography; network traffic anomalies detection.

Число злоумышленников, которые наносят вредоносные действия узлам корпоративной сети, возрастают с каждым годом. Это связано с развитием новых стандартов передачи данных в среде, которые с каждым годом повышают либо пропускную способность канала, либо надежность передачи путем избыточности. Кроме того, число пользователей корпоративных сетей также стремительно растет, и с этим ростом увеличивается количество вредоносной активности [1, 2].

#### Таблица 1. Распределение количества событий

|  |  |
| --- | --- |
| Номер события | Количество за все время |
| 72 | 96 539 |
| 70 | 36 814 |
| … | … |
| 34 |  8 523 |
| 30 |  7 367 |
| 61 |  7 215 |

… … …



*Рис. 1*. Ритмограмма (событие – 19, период – все время)

Результаты экспериментов подтверждают применимость методики ритмографического анализа принятого в кардиологии для анализа ритма появления событий корпоративного сетевого трафика системы *Cisco MARS* [3]. В ходе исследований было разработано программное обеспечение на языке *Python*. Практическое применение предложенного подхода требует дальнейших исследований.

Список литературы

1*. Коробейников А. В*. Алгоритмы и комплексы программ мониторно-компьютерных систем для анализа морфологии и ритма электрокардиограмм : дис… канд. техн. наук. – Ижевск, 2004. – 170 с.

2. *Коробейников А. В.* Стохастический подход к секвенциальному анализу событий корпоративного сетевого трафика системы Cisco MARS / А. В. Коробейников, А. В. Конин, А. С. Менлитдинов // Вестник КИГИТ. – 2012. – № 7 (25). – С. 60–70.

3. *Gary Halleen.* Security Monitoring with Cisco Security MARS / Gary Halleen, Greg Kellogg. – Cisco Press 800 East 96th Street Indianapolis, In 46240 USA. – 2007.

1. © Ложкарев Д. В., Коробейников А. В., Филиппова Е. А., 2020 [↑](#footnote-ref-1)