DOI: 10.18137/RNU.V9187.23.01.P.94 УДК 004.056

А.И. Плаван, В.Г. Карташевский

СРЕДНЕКВАДРАТИЧЕСКАЯ ОШИБКА ФИЛЬТРАЦИИ КАК КРИТЕРИЙ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА[1]

Аннотация. Рассматривается способ обнаружения аномалий в сетевом трафике на основе фильтрации случайного процесса, представляющего ожидаемую интенсивность трафика. Для этого процесса синтезируется фильтр, оптимальный по критерию минимума среднеквадратической ошибки, учитывающий флуктуации трафика от ожидаемых значений в качестве шума. Для фильтра определяется минимальная среднеквадратическая ошибка. Проводится компьютерное моделирование фильтрации реализаций процесса, представляющего ожидаемый сетевой трафик, при отсутствии и наличии аномалии, имеющей определенную автокорреляционную функцию, и при различных значениях отношения сигнал/шум. Результаты моделирования позволяют говорить о том, что отклонение значения среднеквадратической ошибки фильтрации от минимального (ожидаемого) значения может указывать на наличие аномального источника трафика в сети, то есть использоваться в качестве критерия обнаружения аномалии.

Ключевые слова: обнаружение вторжений, обнаружение аномалий, сетевой трафик, фильтр Винера, распределение Вейбулла.

A.I. Plavan, V.G. Kartashevsky

MEAN SQUARE FILTERING ERROR AS A CRITERION FOR DETECTING NETWORK TRAFFIC ANOMALIES

Abstract. The paper considers a method for anomaly detection in network traffic which is based on filtering a random process, representing the expected traffic intensity. A filter that minimizes mean square error is obtained for this process, taking into account traffic fluctuations from expected values as noise. The minimum value of mean square error is determined for the filter. Simulation is performed for the filtering of random samples of process, representing the expected traffic intensity, in the absence and presence of an anomaly with a certain autocorrelation function, and at various values of the signal-to-noise ratio. The simulation results suggest that the deviation of the mean square filtering error from the minimum (expected) value may indicate the presence of an anomalous traffic source in the network, i. e. can be used as an anomaly detection criterion.

Keywords: intrusion detection, anomaly detection, network traffic, Wiener filter, Weibull distribution.

Введение

Известно, что сетевой трафик обладает свойством самоподобия, или фрактальности. Этим свойством могут обладать интервалы времени между поступлениями пакетов (inter-arrival times) либо суммарное количество пакетов (или байт) в единицу времени. Самоподобие предполагает наличие автокорреляционной функции (далее – АКФ) определенного вида. Так, в работе Ли [1] проводилось исследование трассировок трафика на транзитном канале к вышестоящему интернет-провайдеру, предоставленного MAWI

[1] Данная работа выполнена в рамках Всероссийского конкурса научных проектов аспирантов, соискателей и молодых ученых на проведение научных исследований и разработок в области информационной безопасности для задач цифровой экономики (конкурс «Гранты ИБ МТУСИ», http://ib.mtuci.ru/grant-ib).

Плаван Алексей Игоревич
аспирант кафедры информационной безопасности, Поволжский государственный университет телекоммуникаций и информатики, город Самара. Сфера научных интересов: анализ и моделирование сетевого трафика; обнаружение вторжений; статистический анализ. Автор более 10 научных публикаций. ORCID: 0000-0002-4911-7459, ResearcherID: HGB-2716-2022, SPIN-код: 1130-6500.
Электронный адрес: aleksej-plavan@ya.ru

Карташевский Вячеслав Григорьевич
доктор технических наук, профессор, заведующий кафедрой информационной безопасности, Поволжский государственный университет телекоммуникаций и информатики, город Самара. Сфера научных интересов: цифровая обработка сигналов; сетевые технологии; информационная безопасность. Автор более 300 научных публикаций. ORCID: 0000-0003-1114-3966, ResearcherID: A-7260-2017, Scopus Author ID: 6507054475, SPIN-код: 8588-7740.
Электронный адрес: v.kartashevskiy@psuti.ru

(Measurement and Analysis on the WIDE Internet) Working Group[1] и собранного в период с 1 января 2007 года по 31 декабря 2018 года. Было показано, что АКФ ежедневного трафика на этом интервале времени может быть аппроксимирована АКФ процесса Коши. Соответственно, можно предположить, что ожидаемый трафик некоторой сети в определенное время суток может быть охарактеризован АКФ конкретного вида. Знание об этих закономерностях сетевого трафика должно учитываться при разработке новых способов обнаружения аномалий и атак для повышения их эффективности.

Разработанность темы

В литературе под обнаружением аномалий обычно понимается либо обнаружение специальных сигнатур (например, IP-адресов из черного списка), либо отклонений в последовательности значений некоторого параметра, выделенной из сетевого трафика [2]. Иногда используются данные протоколов SNMP и NetFlow (и их вариантов) [3].

Выделяются алгоритмы обнаружения отклонений, основанные на анализе суммарного объема трафика или отдельных его признаков. В работе [4] проводится обзор различных методов, в том числе метода главных компонент (PCA) применительно к объему трафика, подходы на основе вейвлетов применительно к сигналам, выделенным из трафика.

В работе [5] для анализа различных временных рядов, выделенных из сетевых потоков, применяется алгоритм на основе фильтра Калмана и двухшагового метода прогноза и коррекции. По отклонению значений, полученных на этапе коррекции, делается вывод о наличии аномалии в рассматриваемых данных. Размерность данных предварительно уменьшается путем применения метода главных компонент.

Басараб и др. [6] приводят обзор существующих подходов к обнаружению сетевых аномалий на основе методов мультифрактального анализа, так как сетевой трафик проявляет фрактальные свойства и может быть охарактеризован некоторым значением показателя Херста. При возникновении аномалии значения показателя Херста и фрактальной размерности могут отклоняться от ожидаемого.

[1] Архив трафика MAWI Working Group. URL: http://mawi.wide.ad.jp/mawi/ (дата обращения: 22.03.2023).

В данной работе предлагается способ обнаружения аномалий на основе линейной фильтрации временного ряда, полученного из трафика и представляющего его интенсивность. Фильтр Винера, синтезированный для трафика в нормальном состоянии сети, позволяет вычислить минимальное значение среднеквадратической ошибки фильтрации. Значительное отклонение значения ошибки, полученной во время функционирования сети, может служить признаком аномалии.

Методология

Сетевой трафик можно рассматривать как аддитивную смесь

$$x(t)=s(t)+n(t), \tag{1}$$

где $s(t)$ – процесс, представляющий ожидаемый трафик (количество пакетов в единицу времени); $n(t)$ – процесс, представляющий флуктуации трафика в разные дни и недели (шум наблюдений).

Процесс $s(t)$ не может иметь отрицательные значения, так как представляет по определению неотрицательную величину. Сложение с $n(t)$ также не должно приводить к появлению отрицательных значений:

$$min\ s(t)+min\ n(t)\geq 0. \tag{2}$$

Фильтр Винера является оптимальным по критерию минимума среднеквадратической ошибки:

$$\varepsilon^2(t)=E\left\{\left(\hat{s}(t)-s(t)\right)^2\right\}, \tag{3}$$

где $E\{\cdot\}$ – символ усреднения.

Для применения данного фильтра процессы $s(t)$ и $n(t)$ должны быть в широком смысле стационарными. В [7] представлены выражения для получения импульсной характеристики фильтра в непрерывном времени. При компьютерном моделировании разумно перейти к рассмотрению дискретного времени. В матричной форме импульсная характеристика фильтра Винера может быть получена как

$$\mathrm{h}=\mathrm{B_x}^{-1}\cdot\mathrm{b_{xs}}, \tag{4}$$

где $\mathbf{h}$ – вектор отсчетов импульсной характеристики фильтра; $\mathbf{B}_x$ – корреляционная матрица процесса $x(t)$; $\mathbf{b}_{xs}$ – вектор отсчетов взаимной корреляционной функции (далее – ВКФ) процессов $x(t)$ и $s(t)$ [7].

С учетом (1) это выражение примет вид

$$\mathrm{h}=\left(\mathrm{B_s}+\mathrm{B_{sn}}+\mathrm{B_{ns}}+\mathrm{B_n}\right)^{-1}\cdot\left(\mathrm{b_s}+\mathrm{b_{sn}}\right), \tag{5}$$

где $\mathbf{B}_s$ – корреляционная матрица процесса $s(t)$; $\mathbf{B}_{sn}$ – матрица взаимной корреляции процессов $s(t)$ и $n(t)$; $\mathbf{B}_{ns}$ – матрица взаимной корреляции процессов $n(t)$ и $s(t)$; $\mathbf{B}_n$ – корреляционная матрица процесса $n(t)$; $\mathbf{b}_s$ – вектор отсчетов АКФ процесса $s(t)$; $\mathbf{b}_{sn}$ – вектор отсчетов ВКФ процессов $s(t)$ и $n(t)$ [7].

Значение среднеквадратической ошибки фильтрации (3) равно нулю только в том случае, если спектры процессов $s(t)$ и $n(t)$ в частотной области не пересекаются, что в реальных условиях практически недостижимо.

Минимальное значение ошибки может быть найдено как [8]

$$\varepsilon_{min}^2=\mathrm{b_s}[0]-\mathrm{b_{xs}}^T\cdot\mathrm{B_x}^{-1}\cdot\mathrm{b_{xs}}. \tag{6}$$

При этом нормированное минимальное значение ошибки (возможные значения которой лежат в интервале [0,1]) [8]

$$\tilde{\varepsilon}^2_{min} = \frac{\varepsilon^2_{min}}{\sigma^2_s}, \tag{7}$$

где s^2_s – дисперсия процесса, представляющего нормальный трафик.

Суть методики обнаружения аномалий сводится к следующему. Во время периода обучения (наблюдения трафика, характерного для нормального функционирования сети) выделяются локально-стационарные *периоды*, соответствующие основным *сценариям* использования сети, сохраняются их статистические характеристики для дальнейшей идентификации и выборочные АКФ (8), необходимые для синтеза фильтра. После анализа разброса значений для разных *периодов*, соответствующих одному и тому же *сценарию*, принимается некоторая модель процесса, представляющего шум наблюдений. Он может быть как коррелирован с ожидаемым трафиком, так и не коррелирован. В соответствие сценарию использования сети ставится фильтр с определенной импульсной характеристикой и минимальной среднеквадратической ошибкой:

$$B_{xy}(\tau) = \frac{1}{N}\sum_{t=0}^{N}\Big(x(t+\tau) - E\{x\}\Big)\cdot\Big(y(t) - E\{y\}\Big). \tag{8}$$

Во время использования сети с определенной периодичностью происходит фильтрация трафика, наблюдаемого на текущем интервале (в текущем скользящем окне). По статистическим характеристикам текущего периода определяется наиболее вероятный сценарий использования: к трафику применяется фильтр, и для полученной оценки вычисляется среднеквадратическая ошибка фильтрации. Ее значение сравнивается с минимальным значением для данного сценария.

Процесс на выходе фильтра, или оценка, вообще говоря, является смещенной, поскольку в соответствии с (2) обладает ненулевым средним. Для получения несмещенной оценки перед применением фильтра из $x(t)$ необходимо вычесть средние значения $s(t)$ и $n(t)$. Для восстановления реального значения оценки эти значения необходимо прибавить после фильтрации.

Значительное отклонение ошибки фильтрации от предварительно вычисленного минимального значения может говорить о том, что в наблюдаемом трафике появился его новый аномальный источник. Для определения значимости отклонения необходимо выбрать некоторый статистический критерий принятия решения, например, t-тест Стьюдента.

В данной работе проводится моделирование такого случая и рассматривается один локально-стационарный период. В соответствии с условием (2) для моделирования $s(t)$ используется случайный процесс с законом распределения Вейбулла с параметрами формы и масштаба, равными единице. Данный закон распределения характерен для трафика с долговременными зависимостями [9]. В качестве модели $n(t)$ принимается случайный процесс $Y = |X|$, где X – некоррелированный случайный процесс с нормальным законом распределения $\mathcal{N}\left(0, \sigma^2\right)$.

Предполагается, что процесс $s(t)$ имеет АКФ вида $\sin(x)/x$:

$$B(\tau) = \sigma^2 \frac{sin(\tau/\tau_0)}{\tau/\tau_0}, \tag{9}$$

где s^2 – параметр дисперсии; t_0 – параметр времени корреляции.

Для моделирования задаются значения параметров $\sigma = 1$ и $\tau_0 = 500$. Предполагается, что взаимная корреляция между $s(t)$ и $n(t)$ отсутствует, тогда формулы (5) и (6) примут вид соответственно

$$\mathrm{h} = \left(\mathrm{B_s} + \mathrm{B_n}\right)^{-1} \cdot \mathrm{b_s}; \tag{10}$$

$$e^{\,2}_{min} = \mathrm{b_s}[0] - \mathrm{b_s}^{T} \cdot \left(\mathrm{B_s} + \mathrm{B_n}\right)^{-1} \cdot \mathrm{b_s}. \tag{11}$$

При моделировании учитываются первые 1000 отсчетов корреляционных функций (порядок фильтра = 1000). Нормированная среднеквадратическая ошибка в том случае, когда процесс *s(t)* имеет закон распределения Вейбулла, примет вид

$$\tilde{\varepsilon}^2_{min} = \frac{\varepsilon^2_{min}}{\sigma^2_{s_w}} = \frac{\varepsilon^2_{min}}{\lambda^2\left[\Gamma\left(1+\frac{2}{k}\right) - \Gamma^2\left(1+\frac{1}{k}\right)\right]}, \tag{12}$$

где $y^{\,2}_{s_w}$ – дисперсия распределения Вейбулла; λ – коэффициент масштаба распределения Вейбулла; *k* – коэффициент формы распределения Вейбулла; *Γ(·)* – гамма-функция.

Для моделирования случайного процесса с заданным законом распределения и автокорреляционной функцией используется методика, основанная на получении циркулянтной корреляционной матрицы и преобразовании Фурье [10].

Определяется нормированное минимальное значение среднеквадратической ошибки при различных значениях отношения сигнал/шум и реальное значение ошибки для случая, когда фильтр применяется к процессу (1). Затем производится моделирование случая, когда в трафике появляется аномальный процесс *a(t)*, то есть процесс на входе фильтра определяется как

$$x'(t) = s(t) + n(t) + a(t). \tag{13}$$

Рассматривается три случая: а) процесс *a(t)* имеет АКФ вида sin*(x)/x* (9); б) процесс *a(t)* имеет АКФ экспоненциального вида (14); в) процесс *a(t)* имеет АКФ треугольного вида (15).

$$B(\tau) = \sigma^2 exp\left(-\frac{|\tau|}{\tau_0}\right). \tag{14}$$

$$B(\tau) = \begin{cases} \sigma^2\left(1 - \dfrac{|\tau|}{\tau_0}\right), & |\tau| \le \tau_0 \\ 0, & |\tau| > \tau_0 \end{cases}. \tag{15}$$

Процесс *a(t)* действует на всем периоде наблюдений. Определяется реальное значение нормированной среднеквадратической ошибки фильтрации при различных значениях отношения сигнал/шум (SNR). Параметр σ^2 шума *n(t)* определяется из соотношения

$$\sigma^2 = \frac{E\left\{s(t)^2\right\}}{SNR}, \tag{16}$$

где $E\{\cdot^2\}$ – второй момент случайной величины; *SNR* – отношение сигнал/шум.

Результаты

Моделирование производилось в специально разработанной программе на языке Python. Рассматривались следующие значения отношения сигнал/шум: 1/100, 1/10, 1/2, 1, 2, 10, 100. Для каждого значения был синтезирован фильтр и проведено по 10 экспериментов, в каждом из которых генерировались случайные последовательности длиной 100 000 отсчетов с заданными законами распределения и АКФ, к которым применялся фильтр.

Сначала рассматривался процесс *x(t)* (1) без аномалии (Рисунок 1). Пунктирной линией представлены рассчитанные по формуле (12) нормированные минимальные значения среднеквадратической ошибки. Средние за 10 экспериментов значения среднеквадратической ошибки фильтрации представлены сплошной линией, вертикальными чертами отмечены значения стандартного отклонения для каждого значения отношения сигнал/шум.

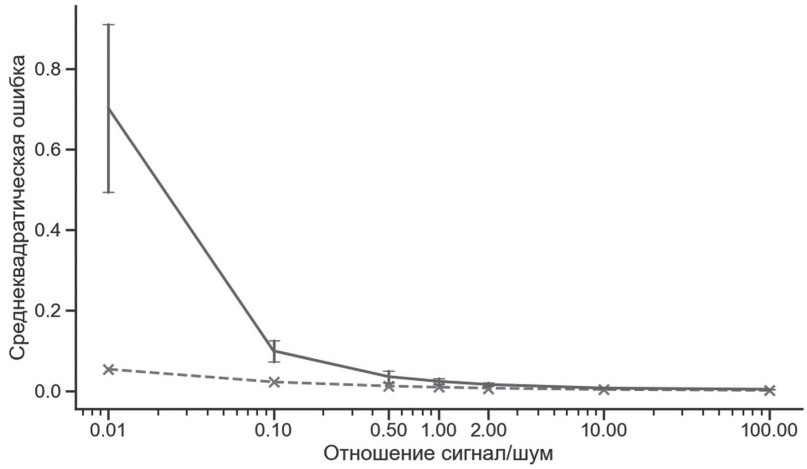

Рисунок 1. Среднеквадратическая ошибка фильтрации трафика без аномалии
Источник: составлено авторами.

По графику видно, что в случаях, когда шум преобладает, реальное значение ошибки сильно отклоняется от минимального. При уменьшении мощности шума реальное значение ошибки приближается к минимальному.

На Рисунке 2 представлен график для процесса *x'(t)* (13) с различными видами аномалий, где дополнительно было отмечено значение ошибки, равной 1.

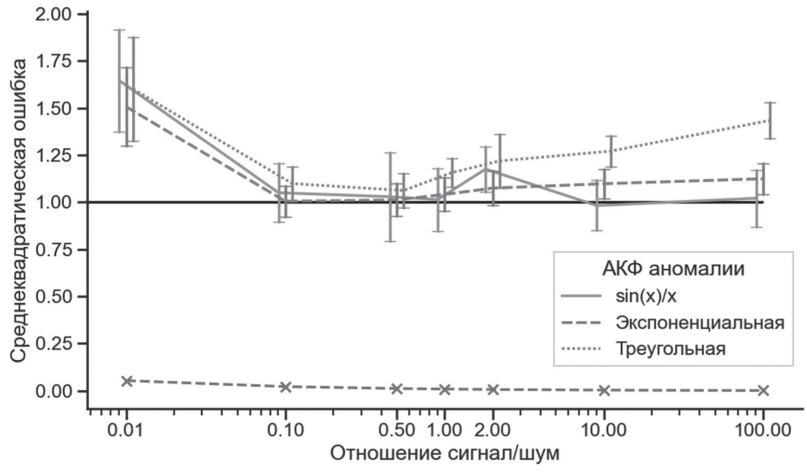

Рисунок 2. Среднеквадратическая ошибка фильтрации трафика с аномалией
Источник: составлено авторами.

Если на вход фильтра поступает процесс $x(t)$ без аномалии, то значение нормированной ошибки должно лежать в интервале [0,1] [8]. По графику видно, что почти во всех случаях наличие аномалии в поступающем на вход фильтра трафике приводит к увеличению значения ошибки и превышению верхней границы, равной 1.

Заключение

Рассмотрен способ обнаружения аномалий в сетевом трафике на основе фильтрации наблюдаемого трафика. Проведено компьютерное моделирование с использованием сгенерированных реализаций случайного процесса $x(t)$, имеющих заданную АКФ. При добавлении к процессу, представляющему нормальный трафик, процесса, представляющего погрешность изменений (шум), для которых был синтезирован фильтр, значение среднеквадратической ошибки фильтрации не сильно отклоняется от ожидаемого минимального значения. При добавлении к поступающему на вход фильтра трафику аномального процесса $a(t)$ значение среднеквадратической ошибки фильтрации значительно возрастает и выходит за интервал [0,1], в котором должны лежать все значения нормированной среднеквадратической ошибки, если на вход фильтра поступает только ожидаемый процесс и шум. Это является признаком наличия аномалии в обрабатываемом трафике.

Данный эксперимент соответствует рассмотрению одного локально-стационарного периода в сетевом трафике, статистические характеристики которого могут, например, представлять сценарий использования сети в рабочее время. Результаты моделирования позволяют говорить о том, что отклонение значения среднеквадратической ошибки фильтрации может указывать на наличие аномального источника трафика в сети, то есть использоваться в качестве критерия обнаружения аномалии.

В дальнейшем следует рассмотреть АКФ реального самоподобного трафика, исследовать влияние на статистические свойства трафика аномалий, действующих не на всем периоде наблюдений, а лишь на некоторой его части, а также разработать методику оценки флуктуаций трафика в разные дни и недели (шума наблюдений) на основе наблюдения нормального трафика.

Литература

1. *Li M.* Long-Range Dependence and Self-Similarity of Teletraffic with Different Protocols at the Large Time Scale of Day in the Duration of 12 Years: Autocorrelation Modeling // Physica Scripta. 2020. Vol. 95. No. 6. Art. no. 065222. DOI: 10.1088/1402-4896/ab82c4

2. *Шелухин О.И., Сакалема Д.Ж., Филинова А.С.* Обнаружение вторжений в компьютерные сети (сетевые аномалии) / под ред. О.И. Шелухина. М. : Горячая линия – Телеком, 2018. ISBN 978-5-9912-0323-4.

3. *Земзеров П.А., Суворов С.В.* Анализ и визуализация сетевого трафика на основе технологии экспорта потоков NetFlow // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2020. № 1. С. 78–86. URL: http://www.nauteh-journal.ru/files/78e4c74c-290a-4100-af6f-53af911d895c (дата обращения: 22.03.2023).

4. *Huang H., Al-Azzawi H., Brani H.* Network Traffic Anomaly Detection // arXiv. Cornell University. 2014. DOI: 10.48550/arXiv.1402.0856

5. *Ndong J., Salamatian K.* Signal Processing-based Anomaly Detection Techniques: A Comparative Analysis // Internet 2011: Proc. 2011 3rd International Conference on Evolving Internet. 2011. P. 32–39.

URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.862.8520&rep=rep1&type=pdf (дата обращения: 22.03.2023).

6. *Басараб М.А., Строганов И.С.* Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4 (7). С. 30–40. URL: https://cyberrus.com/wp-content/uploads/2015/01/vkb_05_04.pdf (дата обращения: 22.03.2023).

7. *Левин Б.Р.* Теоретические основы статистической радиотехники. Кн. 2. 2-е изд. М. : Советское радио, 1975. 390 с.

8. *Haykin S.S.* Adaptive Filter Theory. 4th edition. Upper Saddle River, N.J. : Prentice Hall, 2002.

9. *Шелухин О.И., Тенякшев А.М., Осин А.В.* Моделирование информационных систем / под ред. О.И. Шелухина. М. : Сайнс-Пресс, Радиотехника, 2005. 367 с. ISBN 5-93108-072-4.

10. *Crouse M., Baraniuk R.G.* Fast, Exact Synthesis of Gaussian and nonGaussian Long-Range-Dependent Processes // IEEE Transactions on Information Theory, 1999. URL: https://scholarship.rice.edu/bitstream/handle/1911/21941/fastLRD-TREE9913.pdf (дата обращения: 22.03.2023).

References

1. Li M. (2020) Long-Range Dependence and Self-Similarity of Teletraffic with Different Protocols at the Large Time Scale of Day in the Duration of 12 Years: Autocorrelation Modeling. *Physica Scripta.* Vol. 95. No. 6. Art. no. 065222. DOI: 10.1088/1402-4896/ab82c4

2. Sheluhin O.I., Sakalema D.Zh., Filinova A.S. (2018) *Obnaruzhenie vtorzhenii v komp'yuternye seti (setevye anomalii)* [Network intrusion detection (network anomalies)]. Moscow : Goryachaya liniya – Telekom Publishing. ISBN 978-5-9912-0323-4. (In Russian).

3. Zemzerov P.A., Suvorov S.V. (2020) Analiz i vizualizatsiya setevogo trafika na osnove tekhnologii eksporta potokov [Analysis and visualization of network traffic based on NetFlow export technology]. *Modern Science: Actual Problems of Theory and Practice. Series: Natural and Technical Sciences*. No. 1. URL: http://www.nauteh-journal.ru/files/78e4c74c-290a-4100-af6f-53af911d895c (accessed 22.03.2023). (In Russian).

4. Huang H., Al-Azzawi H., Brani H. (2014) Network Traffic Anomaly Detection. *arXiv*. *Cornell University.* DOI: 10.48550/arXiv.1402.0856

5. Ndong J., Salamatian K. (2011) Signal Processing-based Anomaly Detection Techniques: A Comparative Analysis. *Internet 2011: Proc. 2011 3rd International Conference on Evolving Internet*. Pp. 32–39. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.862.8520&rep=rep1&type=pdf (accessed 22.03.2023).

6. Basarab M.A., Stroganov I.S. (2014) Obnaruzhenie anomalii v informatsionnykh protsessakh na osnove mul'tifraktal'nogo analiza [Anomaly detection in information processes based on multifractal analysis]. *Voprosy kiberbezopasnosti*. No. 4 (7). Pp. 30–40. URL: https://cyberrus.com/wp-content/uploads/2015/01/vkb_05_04.pdf (accessed 22.03.2023). (In Russian).

7. Levin B.R. (1975) *Teoreticheskie osnovy statisticheskoi radiotekhniki* [Theoretical Foundations of Statistical Radio Engineering.]. 2nd edition. Vol. 2. Moscow : Sovetskoe radio Publishing. 390 p. (In Russian).

8. Haykin S.S. (2002) *Adaptive Filter Theory*. 4th edition. Upper Saddle River, N.J. : Prentice Hall.

9. Sheluhin O.I., Tenyakshev A.M., Osin A.V. (2005) *Modelirovanie informatsionnykh sistem* [Information systems modeling]. Ed. by O.I. Sheluhin. Moscow : Science-Press, Radiotehnika Publishing. 367 p. ISBN 5-93108-072-4. (In Russian).

10. Crouse M., Baraniuk R.G. (1999) Fast, Exact Synthesis of Gaussian and nonGaussian Long-Range-Dependent Processes. *IEEE Transactions on Information Theory*. URL: https://scholarship.rice.edu/bitstream/handle/1911/21941/fastLRD-TREE9913.pdf (accessed 22.03.2023).