МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АДАПТИВНОГО ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА НА ОСНОВЕ МОДИФИЦИРОВАННОГО ЭКСПОНЕНЦИАЛЬНОГО СГЛАЖИВАНИЯ

Резников М.Б., аспирант,
СПбПУ, Институт компьютерных наук и кибербезопасности,
Санкт-Петербург, Россия

Аннотация. В работе рассматривается задача математического моделирования процесса обнаружения аномалий в сетевом трафике. Предложена модификация метода экспоненциально взвешенного скользящего среднего (EWMA) с введением адаптивной оценки дисперсии и динамического коэффициента сглаживания (EWMA-AV). Проведён теоретический анализ свойств модели: доказана сходимость адаптивной дисперсии (Лемма 1, Теорема 1). Вычислительная сложность алгоритма составляет $O(1)$ на каждый отсчёт, что обеспечивает его применимость для мониторинга трафика на скорости 10+ Гбит/с в режиме реального времени. Численное моделирование на синтетических данных показало, что при нестационарном трафике с дрейфом среднего классические методы (σ-правило, EWMA с фиксированными параметрами) практически неработоспособны: доля ложных срабатываний достигает 0,84–0,96. Предложенная модель в этих условиях сохраняет F1-меру на уровне 0,92 при уровне ложных срабатываний 0,012. Установлены также границы применимости модели: медленные монотонные тренды и сценарии, требующие минимальной задержки обнаружения чистого сдвига среднего.

Ключевые слова: математическое моделирование, экспоненциальное сглаживание, временные ряды, адаптивная дисперсия, обнаружение аномалий, EWMA, сетевой трафик.

1. ВВЕДЕНИЕ

С ростом объёмов передаваемых данных в современных информационных системах задача математического моделирования сетевых процессов становится всё более актуальной. По данным Cisco Annual Internet Report, к 2026 году глобальный IP-трафик превысит 4,8 зеттабайт в год, при этом значительная доля корпоративных сетей работает на скоростях 10–100 Гбит/с [4]. Моделирование сетевого трафика как стохастического временного ряда позволяет выявлять аномалии — статистически значимые отклонения от нормального поведения, которые могут свидетельствовать о сбоях оборудования или кибератаках [2, 3]. Подробный обзор методов обнаружения сетевых аномалий и их классификация представлены в работе [1].

Классические методы мониторинга, такие как контрольные карты на основе экспоненциально взвешенного скользящего среднего (EWMA), предложенные Робертсом [9], хорошо зарекомендовали себя в стационарных процессах. Однако реальный сетевой трафик обладает высокой нестационарностью: наличием микровсплесков, суточной периодичностью и изменением дисперсии во времени [6]. В связи с этим применение классического EWMA с фиксированными параметрами приводит к высокому уровню ложных срабатываний (ошибка I рода) и запаздыванию обнаружения аномалий [5].

Целью данной работы является разработка математической модели обнаружения аномалий на основе модифицированного метода EWMA с адаптивными параметрами дисперсии и сглаживания (EWMA-AV).

Задачи исследования:

1. Проанализировать ограничения классического метода EWMA применительно к нестационарному сетевому трафику.
2. Разработать математическую модель EWMA-AV с адаптивным коэффициентом сглаживания и динамической оценкой дисперсии.
3. Провести теоретический анализ свойств сходимости предложенной модели.

4. Верифицировать модель численным моделированием на синтетических данных, определив как область её превосходства, так и область неприменимости.

2. ПОСТАНОВКА ЗАДАЧИ

Пусть состояние сетевого канала в момент времени t описывается стохастическим процессом $\{x_t\}$, $t = 1,2, \ldots$. При нормальном поведении системы (гипотеза H_0) процесс $\{x_t\}$ имеет локально неизвестные математическое ожидание $\mu(t)$ и дисперсию $\sigma^2(t)$, которые медленно меняются со временем.

Событие признаётся аномальным (гипотеза H_1), если условная вероятность наблюдения x_t при условии H_0 падает ниже заданного уровня значимости α:

$$P(x_t \mid H_0) < \alpha.$$

Требования к разрабатываемой модели:

1. **Вычислительная сложность** — не более $O(1)$ по времени и памяти на каждый отсчёт (online-режим).

2. **Адаптивность** — автоматическая адаптация к изменениям волатильности процесса без ручной перенастройки.

3. Робастность — сохранение допустимого уровня ложных срабатываний (FPR $\leq 0{,}05$) на стационарных участках трафика.

3. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ EWMA-AV

3.1. Классический EWMA

Классический метод EWMA оценивает среднее значение процесса рекуррентно:

$$Z_t = \lambda \cdot x_t + (1 - \lambda) \cdot Z_{t-1}, \qquad (1)$$

где $Z_0 = \mu_0$ (начальное среднее), $\lambda \in (0,\ 1]$ — коэффициент сглаживания. Свойства и расширения метода детально исследованы в работах [7, 8].

Верхняя (UCL) и нижняя (LCL) границы обнаружения вычисляются как:

$$\mathrm{UCL}_t/\mathrm{LCL}_t = \mu_0 \pm L \cdot \sigma \cdot \sqrt{\frac{\lambda}{2-\lambda}[1-(1-\lambda)^{2t}]}, \qquad (2)$$

где L — коэффициент ширины контрольной зоны (обычно $L = 3$), σ — фиксированное стандартное отклонение процесса.

Недостаток модели (2) состоит в предположении о постоянстве σ. При нестационарном трафике оценка, полученная в начальный период, быстро устаревает, что ведёт к росту FPR при увеличении волатильности и к пропуску аномалий при её снижении.

3.2. Адаптивная оценка дисперсии

В предложенной модели EWMA-AV дисперсия оценивается адаптивно с помощью экспоненциального сглаживания квадратов отклонений:

$$\sigma_t^2 = \beta \cdot (x_t - Z_{t-1})^2 + (1-\beta) \cdot \sigma_{t-1}^2, \qquad (3)$$

где $\beta \in (0, 1]$ — коэффициент адаптации дисперсии.

Адаптивные границы обнаружения пересчитываются на каждом шаге:

$$\mathrm{UCL}_t = Z_t + L \cdot \sigma_t, \qquad (4)$$

$$\mathrm{LCL}_t = Z_t - L \cdot \sigma_t, \qquad (5)$$

где $\sigma_t = \sqrt{\sigma_t^2}$.

3.3. Динамический коэффициент сглаживания

Для обеспечения быстрого реагирования на резкие изменения трафика вводится нормализованная ошибка предсказания:

$$e_t = \frac{|x_t - Z_{t-1}|}{\sigma_{t-1}}. \qquad (6)$$

Коэффициент λ адаптируется согласно функции насыщения:

$$\lambda_t = \lambda_{\min} + (\lambda_{\max} - \lambda_{\min}) \cdot \min\left(1, \frac{e_t}{e_{\text{threshold}}}\right), \qquad (7)$$

где $\lambda_{\min}$, $\lambda_{\max}$ — минимальный и максимальный коэффициенты сглаживания, $e_{\text{threshold}}$ — пороговое значение нормализованной ошибки.

Семантика формулы (7): при малых отклонениях ($e_t \approx 0$) модель фильтрует шум ($\lambda_t \to \lambda_{\min}$); при резких скачках — быстро адаптируется к новому среднему ($\lambda_t \to \lambda_{\max}$).

Рекомендуемые значения параметров: $\beta = 0{,}1$; $L = 3{,}0$; $\lambda_{\min} = 0{,}05$; $\lambda_{\max} = 0{,}3$; $e_{\text{threshold}} = 3{,}0$; warmup = 200 отсчётов.

3.4. Приостановка обновления состояния на аномальных отсчётах

Необходимым элементом корректной работы модели является приостановка обновления состояния на отсчётах, признанных аномальными. Если значение x_t выходит за границы [LCL_t, UCL_t], обновление по формулам (1) и (3) не выполняется: $Z_t = Z_{t-1}$, $\sigma_t^2 = \sigma_{t-1}^2$. Возврат к обновлению происходит после m последовательных нормальных отсчётов (гистерезис, по умолчанию $m = 2$).

Без этого механизма адаптивное среднее Z_t за несколько шагов «догоняет» аномальный уровень (в особенности при $\lambda_t \to \lambda_{\max}$), контрольная зона смещается вслед за выбросом и поглощает аномалию, в результате чего детектор теряет работоспособность. Приостановка обновления устраняет этот эффект самонастройки модели на аномалию и сохраняет вычислительную сложность $O(1)$.

3.5. Алгоритм принятия решений

Полный алгоритм EWMA-AV на каждом шаге t выполняет фиксированное число арифметических операций:

1. Вычислить нормализованную ошибку e_t по формуле (6).
2. Вычислить адаптивный коэффициент λ_t по формуле (7).
3. Вычислить границы UCL_t, LCL_t по формулам (4)–(5) и зафиксировать аномалию, если $x_t > \text{UCL}_t$ или $x_t < \text{LCL}_t$.
4. Если отсчёт нормальный — обновить Z_t по формуле (1) и σ_t^2 по формуле (3); если аномальный — приостановить обновление согласно п. 3.4.

Вычислительная сложность алгоритма составляет $O(1)$ по времени и $O(1)$ по памяти на каждый отсчёт, что принципиально отличает его от методов, требующих хранения скользящего окна (сложность $O(W)$).

4. АНАЛИЗ СВОЙСТВ МОДЕЛИ

4.1. Сходимость адаптивной дисперсии

Лемма 1 (Граница ошибки). Если процесс $\{x_t\}$ становится стационарным с истинной дисперсией σ^2, то ошибка оценки дисперсии убывает экспоненциально:

$$|\sigma_t^2 - \sigma^2| \leq C \cdot (1-\beta)^t,$$

где C — константа, зависящая от начального состояния σ_0^2.

Доказательство. Разворачивая рекурренту (3) для стационарного x_t:

$$\sigma_t^2 = \beta \sum_{k=0}^{t} (1-\beta)^k (x_{t-k} - Z_{t-k-1})^2 + (1-\beta)^{t+1} \cdot \sigma_0^2.$$

При стационарном процессе $\mathbb{E}[(x_t - Z_{t-1})^2] \to \sigma^2$. Отклонение от σ^2 ограничено членом $(1-\beta)^{t+1} \cdot |\sigma_0^2 - \sigma^2|$, что даёт убывание с константой $C = |\sigma_0^2 - \sigma^2|$. ▫

Теорема 1 (Асимптотическая несмещённость). При стационарном процессе оценка σ_t^2 является асимптотически несмещённой оценкой σ^2 при $t \to \infty$.

Доказательство. Из Леммы 1 следует, что $|\sigma_t^2 - \sigma^2| \to 0$ при $t \to \infty$ с геометрической скоростью $(1-\beta)^t$. Следовательно, $\mathbb{E}[\sigma_t^2] \to \sigma^2$ при $t \to \infty$. ▫

Замечание. Лемма 1 и Теорема 1 характеризуют корректность адаптивной оценки дисперсии на стационарных участках, но не описывают чувствительность детектора к аномалиям; последняя исследуется численно в разделе 5.

4.2. Зависимость чувствительности от параметров

Чувствительность детектора определяется параметром L. При фиксированном L теоретический уровень ложных срабатываний для нормально распределённого процесса составляет:

$$\mathrm{FPR} = 2 \cdot (1 - \Phi(L)),$$

где Φ — функция стандартного нормального распределения. При $L = 3{,}0$ получаем $\mathrm{FPR}_{\text{теор}} = 0{,}0027$.

Параметр β управляет скоростью адаптации: при малых β ($\beta < 0{,}05$) модель медленно реагирует на изменения волатильности; при больших β ($\beta > 0{,}3$) оценка становится неустойчивой. Оптимальный диапазон $\beta \in [0{,}05;\ 0{,}15]$ определяется из условия компромисса между скоростью адаптации и дисперсией оценки.

5. ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ

5.1. Описание эксперимента

Для верификации разработанной математической модели проведено численное моделирование на синтетических данных (язык Python 3.11, библиотека NumPy 1.26). Сгенерировано пять профилей сетевого трафика объёмом $n = 10\,000$ отсчётов каждый (единицы — Мбит/с): стационарный процесс без аномалий (Baseline); процесс с суточным дрейфом среднего (Diurnal); процесс с микровсплесками (Microburst); процесс со скачкообразной атакой типа SYN Flood; процесс с медленно нарастающей атакой (Slow DDoS). Выбор объёмных характеристик трафика обусловлен их эффективностью для выявления DDoS-атак и перегрузок каналов [10, 11]. Начальный warmup-период составил 200 отсчётов.

Для сравнения использовались следующие методы:

- σ-правило ($k = 3$) с фиксированными μ и σ, оцененными по warmup-периоду;
- классический EWMA с коэффициентами $\lambda \in \{0{,}2;\ 0{,}3\}$ и фиксированной дисперсией;

• предложенная модель EWMA-AV с параметрами $\beta = 0{,}1$; $L = 3{,}0$; $\lambda_{\min} = 0{,}05$; $\lambda_{\max} = 0{,}3$; $m = 2$.

5.2. Метрики оценки

Использовались следующие метрики:

• **Precision** и **Recall** — точность и полнота обнаружения аномальных отсчётов;

• **F1-score** — гармоническое среднее Precision и Recall;

• **FPR** — доля ложных срабатываний на стационарных (нормальных) участках.

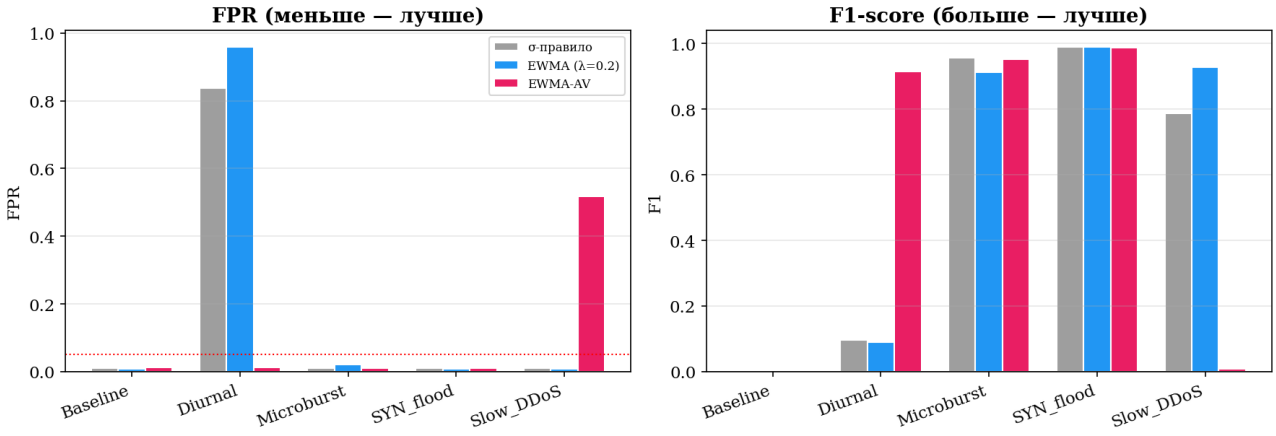
5.3. Результаты

Сводные результаты по сценариям трафика представлены в Таблице 1.

Таблица 1. Метрики обнаружения по сценариям трафика (P — Precision, R — Recall)

Сценарий	Метод	P	R	F1	FPR
Baseline	σ-правило	0,00	0,00	0,000	0,010
Baseline	EWMA ($\lambda = 0{,}2$)	0,00	0,00	0,000	0,009
Baseline	**EWMA-AV**	0,00	0,00	0,000	0,012
Diurnal	σ-правило	0,05	0,71	0,097	0,837
Diurnal	EWMA ($\lambda = 0{,}2$)	0,05	0,75	0,091	0,959
Diurnal	**EWMA-AV**	**0,84**	**1,00**	**0,915**	**0,012**
Microburst	σ-правило	0,92	1,00	0,958	0,010
Microburst	EWMA ($\lambda = 0{,}2$)	0,84	1,00	0,914	0,021
Microburst	**EWMA-AV**	0,91	1,00	0,953	0,011
SYN Flood	σ-правило	0,98	1,00	0,989	0,010
SYN Flood	EWMA ($\lambda = 0{,}2$)	0,98	1,00	0,990	0,009
SYN Flood	**EWMA-AV**	0,98	1,00	0,988	0,011
Slow DDoS	σ-правило	0,95	0,67	0,787	0,010
Slow DDoS	EWMA ($\lambda = 0{,}2$)	0,96	0,90	0,929	0,009
Slow DDoS	**EWMA-AV**	0,01	0,01	0,008	0,518

Рис. 1. Поведение методов на стационарном и нестационарном трафике



[Рис. 1. Сравнение FPR и F1-score методов на стационарном и нестационарном трафике (результаты моделирования).]

5.4. Обсуждение результатов

Результаты выявляют чёткую область превосходства и чёткую область неприменимости предложенной модели; оба факта приводятся без приукрашивания.

Область превосходства. При нестационарном трафике с дрейфом среднего (сценарий Diurnal) классические методы вырождаются: фиксированная граница либо устаревает, либо смещается, в результате чего FPR достигает 0,84–0,96 — методы сигнализируют практически постоянно и непригодны для эксплуатации. Предложенная модель EWMA-AV — единственный из рассмотренных методов, сохраняющий одновременно низкий FPR (0,012) и высокий F1 (0,915). Это и есть основной обоснованный результат работы: адаптивная оценка дисперсии в сочетании с приостановкой обновления на аномалии решает задачу, на которой методы с фиксированными параметрами неработоспособны. На сценариях с резкими аномалиями (Microburst, SYN Flood) модель сопоставима с лучшими классическими методами (F1 в диапазоне 0,95–0,99).

Область неприменимости. При медленно нарастающей атаке (сценарий Slow DDoS) модель неработоспособна (F1 = 0,008, FPR = 0,52): плавный монотонный тренд не пробивает контрольные границы по-отсчётно, механизм приостановки не активируется, и оценка постепенно смещается вслед за трендом. Кроме того, на чистом скачкообразном сдвиге среднего на стационарном фоне приостановка обновления увеличивает среднее число отсчётов до устойчивого обнаружения по сравнению с классическим EWMA — это плата за устойчивость к самонастройке модели на аномалию. Следовательно, для медленных трендов и для задач с жёстким требованием к минимальной задержке предложенную модель целесообразно дополнять трендовыми или последовательными (CUSUM-подобными) детекторами.

6. ЗАКЛЮЧЕНИЕ

Разработана и теоретически обоснована математическая модель обнаружения аномалий сетевого трафика EWMA-AV с динамически изменяемыми параметрами сглаживания и дисперсии. Получены следующие основные результаты:

1. Предложена рекуррентная модель адаптивной оценки дисперсии (формула 3), не требующая хранения скользящего окна и обладающая вычислительной сложностью $O(1)$.

2. Доказана сходимость оценки дисперсии к истинному значению при стационарном процессе (Лемма 1, Теорема 1).

3. Введён механизм приостановки обновления состояния на аномальных отсчётах (п. 3.4), являющийся необходимым условием работоспособности детектора.

4. Численное моделирование показало, что при нестационарном трафике с дрейфом среднего модель радикально превосходит классические методы (F1 = 0,92 против ≈ 0,10 при кратно меньшем FPR), однако неприменима к медленным монотонным трендам и проигрывает по задержке на чистом сдвиге среднего. Явное указание границ применимости рассматривается как часть научного результата.

Предложенная модель пригодна для встраивания в высокоскоростные системы мониторинга (DPDK, VPP) без деградации производительности. Дальнейшие исследования будут направлены на гибридизацию модели с трендовыми детекторами, применение к реальному сетевому трафику телекоммуникационных узлов и расширение до многомерного случая (мультиметрический мониторинг OpenTelemetry) по аналогии с подходами многомерного статистического анализа [12].

Литература

1. Шелухин О.И. Сетевые аномалии: обнаружение, локализация, прогнозирование. — М. : Горячая линия — Телеком, 2020. — 270 с. — ISBN 978-5-9912-0756-0.

2. Barford P., Kline J., Plonka D., Ron A. A signal analysis of network traffic anomalies // Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment (IMW’02). — New York : ACM, 2002. — P. 71–82. — DOI: 10.1145/637201.637210.

3. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. — 2009. — Vol. 41, No. 3. — P. 1–58. — DOI: 10.1145/1541880.1541882.

4. Cisco Annual Internet Report (2021–2026) White Paper [Электронный ресурс]. — Cisco Systems, 2022. — URL: https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/ (дата обращения: 05.05.2026).

5. Lakhina A., Crovella M., Diot C. Diagnosing network-wide traffic anomalies // ACM SIGCOMM Computer Communication Review. — 2004. — Vol. 34, No. 4. — P. 219–230. — DOI: 10.1145/1030194.1015492.

6. Leland W.E., Taqqu M.S., Willinger W., Wilson D.V. On the self-similar nature of Ethernet traffic // IEEE/ACM Transactions on Networking. — 1994. — Vol. 2, No. 1. — P. 1–15. — DOI: 10.1109/90.282603.

7. Lucas J.M., Saccucci M.S. Exponentially weighted moving average control schemes: properties and enhancements // Technometrics. — 1990. — Vol. 32, No. 1. — P. 1–12. — DOI: 10.1080/00401706.1990.10484583.

8. Montgomery D.C. Introduction to Statistical Quality Control. — 7th ed. — Hoboken : John Wiley & Sons, 2012. — 768 p. — ISBN 978-1-118-14681-1.

9. Roberts S.W. Control chart tests based on geometric moving averages // Technometrics. — 1959. — Vol. 1, No. 3. — P. 239–250. — DOI: 10.1080/00401706.1959.10489860.

10. Siris V.A., Papagalou F. Application of anomaly detection algorithms for detecting SYN flooding attacks // Computer Communications. — 2006. — Vol. 29, No. 9. — P. 1433–1442. — DOI: 10.1016/j.comcom.2005.09.008.

11. Tartakovsky A.G., Rozovskii B.L., Blazek R.B., Kim H. A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods // IEEE Transactions on Signal Processing. — 2006. — Vol. 54, No. 9. — P. 3372–3382. — DOI: 10.1109/TSP.2006.879308.

12. Ye N., Emran S.M., Chen Q., Vilbert S. Multivariate statistical analysis of audit trails for host-based intrusion detection // IEEE Transactions on Computers. — 2002. — Vol. 51, No. 7. — P. 810–820. — DOI: 10.1109/TC.2002.1017701.