

И. В. Махорин¹✉

Метод адаптивной оконной фильтрации при расчете квантильного порога в задачах обнаружения инсайдерской активности

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: ilyamakhorin@mail.ru

Аннотация. В статье рассматривается задача обнаружения инсайдерской активности в корпоративных вычислительных сетях в условиях нестационарности поведенческих данных. Показано, что использование квантильных порогов на скользящем окне фиксированного размера приводит к снижению устойчивости методов обнаружения аномалий при изменении характеристик входного потока. Предложен метод адаптивной оконной фильтрации, в котором размер окна определяется динамически на основе локальной вариативности и интенсивности данных. Представлена математическая формализация метода и приведено вероятностное обоснование его устойчивости. Анализ показывает, что предложенный подход позволяет повысить устойчивость оценки квантильного порога и улучшить адаптацию к изменяющимся условиям. Метод ориентирован на потоковую обработку данных и может быть применен в системах UEBA и других задачах кибербезопасности.

Ключевые слова: обнаружение инсайдерских угроз, квантильный порог, адаптивное окно, поведенческий анализ, UEBA, кибербезопасность

I. V. Makhorin¹✉

Adaptive window filtering method for quantile threshold estimation in insider threat detection

¹National Research Nuclear University «MEPhI», Moscow, Russian Federation
e-mail: ilyamakhorin@mail.ru

Abstract. This paper addresses the problem of insider threat detection in corporate information systems under conditions of non-stationary behavioral data. It is shown that the use of quantile thresholds based on a fixed-size sliding window leads to reduced robustness of anomaly detection methods when the characteristics of the input data stream change. An adaptive window filtering method is proposed, in which the window size is dynamically adjusted based on local variability and event intensity. A mathematical formulation of the method is presented, along with a probabilistic justification of its robustness. The analysis shows that the proposed approach improves the stability of quantile threshold estimation and enhances adaptation to changing conditions. The method is designed for streaming data processing and can be applied in UEBA systems and other cybersecurity tasks.

Keywords: insider threat detection, quantile threshold, adaptive window, behavioral analysis, UEBA, cybersecurity

Введение

В современных корпоративных вычислительных сетях задача обнаружения инсайдерских угроз приобретает особую актуальность в связи с ростом объемов

обрабатываемых данных и усложнением поведенческих паттернов пользователей. В отличие от внешних атак, инсайдерская активность характеризуется наличием легитимных прав доступа, что существенно затрудняет ее выявление традиционными средствами информационной безопасности. В этой связи все большее распространение получают методы поведенческого анализа и обнаружения аномалий, лежащие в основе систем класса User and Entity Behavior Analytics (UEBA) [1–3]. Современные исследования также демонстрируют активное применение методов машинного обучения и глубокого обучения для анализа поведения пользователей и выявления скрытых признаков инсайдерской активности [4]. При этом отдельное внимание уделяется развитию UEBA-моделей, ориентированных на выявление аномалий в корпоративных вычислительных сетях [5].

Одним из распространенных подходов к обнаружению аномалий является использование статистических порогов, в частности квантильных оценок распределения наблюдаемых признаков [6, 7]. Пусть задан временной ряд наблюдений, отражающий интенсивность или характеристики активности пользователя. Тогда аномальные события могут определяться как значения, превышающие некоторый квантильный порог, вычисляемый на основе исторических данных. Однако на практике такие методы сталкиваются с существенными ограничениями [8, 9].

Во-первых, поведение пользователей в корпоративной сети является нестационарным: распределение признаков может изменяться во времени под влиянием рабочих процессов, сезонных факторов и внешних условий [10, 11]. Во-вторых, интенсивность событий может значительно варьироваться, что приводит к нестабильности оценок квантилей при использовании фиксированного окна наблюдения. В результате возникают ситуации, когда порог либо избыточно чувствителен (что увеличивает число ложноположительных срабатываний), либо, наоборот, теряет способность выявлять аномалии. Исходя из этого, возникает необходимость в разработке методов, способных адаптироваться к изменяющимся характеристикам входных данных и обеспечивать устойчивую оценку пороговых значений. Одним из перспективных направлений является использование адаптивных оконных методов, в которых параметры окна наблюдения (размер, положение) изменяются в зависимости от текущих свойств временного ряда [12–14].

В данной работе предлагается метод адаптивной оконной фильтрации при расчете квантильного порога, направленный на повышение устойчивости и точности обнаружения аномальной активности. В отличие от классических методов, основанных на использовании фиксированного окна наблюдения, в предлагаемом подходе размер окна определяется динамически на основе локальных статистических характеристик временного ряда. Это позволяет учитывать нестационарность процесса и адаптировать оценку квантильного порога к текущим условиям функционирования системы.

Методы и материалы

В рамках настоящего исследования рассматривается стохастический процесс наблюдений:

$$X_{t=1}^T, \quad (1)$$

где $X_t \in R$ представляет собой значение признака, характеризующего активность пользователя или системы в момент времени t . Предполагается, что процесс является локально нестационарным, то есть распределение случайной величины X_t задается семейством функций распределения $F_t(x)$, изменяющихся во времени. Для обнаружения аномальной активности используется квантильный подход. Квантиль уровня $\alpha \in (0,1)$ определяется как:

$$q_\alpha(t) = \inf \inf \{ x \in R: F_t(x) \geq \alpha \}, \quad (2)$$

и служит пороговым значением, превышение которого интерпретируется как потенциальная аномалия. Поскольку истинное распределение $F_t(x)$ неизвестно, используется его эмпирическая оценка, построенная по выборке наблюдений. В классическом подходе применяется скользящее окно фиксированного размера, однако в условиях нестационарности такой подход приводит к компромиссу между смещенностью и дисперсией оценки. Для устранения данного ограничения в работе предлагается метод адаптивной оконной фильтрации, в рамках которого размер окна наблюдения изменяется во времени в зависимости от локальных характеристик процесса.

Пусть окно наблюдения переменной длины w_t :

$$W_t = X_{t-w_t+1}, \dots, X_t. \quad (3)$$

Тогда эмпирическая функция распределения определяется как:

$$\hat{F}_t(x) = \frac{1}{w_t} \sum_{i=t-w_t+1}^t 1\{X_i \leq x\} \quad (4)$$

а оценка квантиля принимает вид:

$$\widehat{q}_\alpha(t) = \inf \{ x: \hat{F}_t(x) \geq \alpha \}. \quad (5)$$

Ключевым элементом предлагаемого метода является механизм адаптации размера окна. Размер окна определяется как функция локальной вариативности и интенсивности потока событий:

$$w_t = w_0 \cdot (1 + \beta \sigma_t)^{-1} \cdot (1 + \gamma \lambda_t)^{-1}, \quad (6)$$

где w_0 – базовый размер окна, β и γ – параметры чувствительности.

Локальная вариативность σ_t оценивается через стандартное отклонение значений в текущем окне, что позволяет учитывать степень разброса данных. Ин-

тенсивность потока событий λ_t определяется как среднее число наблюдений, удовлетворяющих заданному условию активности, в фиксированном интервале времени. Тем самым, при увеличении вариативности или плотности событий размер окна автоматически уменьшается, обеспечивая быструю реакцию на изменения, а при стабильном поведении увеличивается, снижая влияние случайных флуктуаций. Аномальная активность фиксируется при превышении текущим наблюдением адаптивного квантильного порога:

$$X_t > \hat{q}_\alpha(t). \quad (7)$$

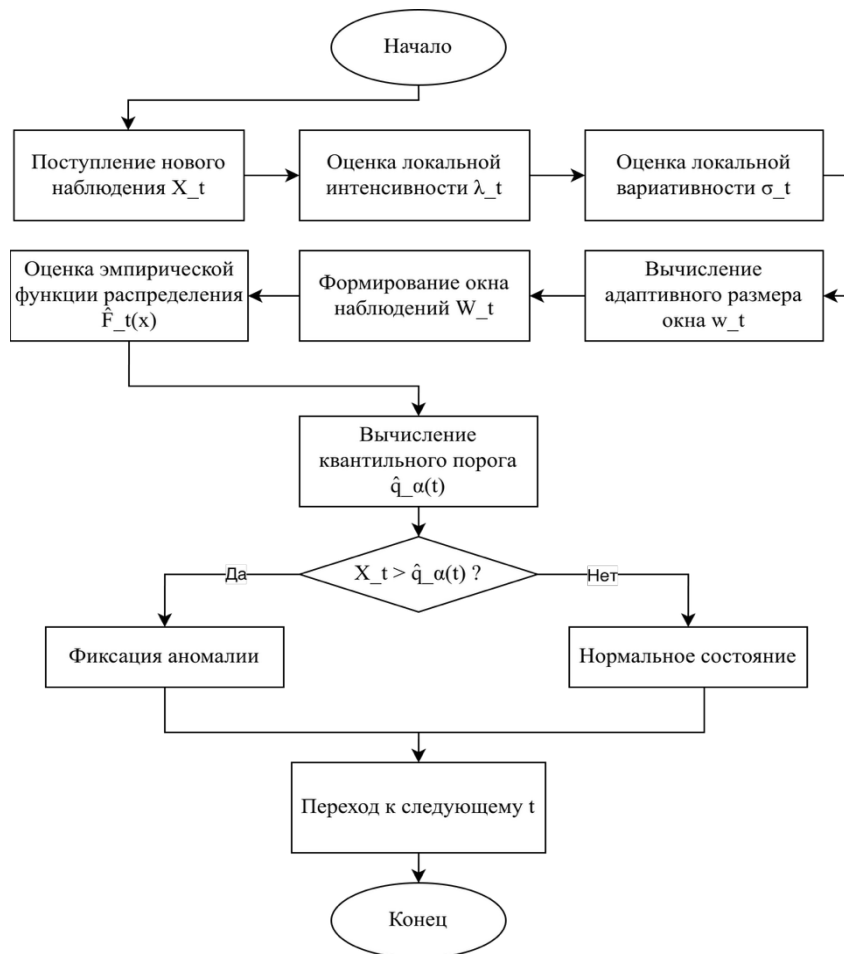


Рис. 1. Блок-схема метода адаптивной оконной фильтрации при расчете квантильного порога

Реализация метода осуществляется в виде последовательной обработки временного ряда, в рамках которого на каждом шаге производится оценка локальных характеристик, пересчет размера окна и обновление квантильного порога. Предложенный подход ориентирован на использование в потоковых системах анализа событий и не требует хранения полной истории наблюдений, что обеспечивает его вычислительную эффективность.

Визуализация метода представлена на рис. 1. На каждом шаге обработки входного потока данных производится оценка локальных характеристик временного ряда, на основе которых динамически определяется размер окна наблюдения. Далее формируется выборка для оценки эмпирической функции распределения и вычисляется квантильный порог. Принятие решения об аномалии осуществляется путем сравнения текущего значения с адаптивным порогом. Такой подход обеспечивает онлайн-обработку данных и позволяет оперативно реагировать на изменения в поведении системы.

Вероятностное обоснование устойчивости метода

Для анализа свойств предложенного метода рассмотрим ошибку оценки квантильного порога, определяемую как:

$$\varepsilon_t = |\widehat{q}_\alpha(t) - q_\alpha(t)|. \quad (8)$$

В классическом случае фиксированного окна w при предположении стационарности процесса выполняется сходимость оценки квантиля по вероятности. Однако в условиях локальной нестационарности возникает дополнительная ошибка, связанная с изменением распределения во времени. Суммарная ошибка может быть представлена в виде:

$$E[\varepsilon_t^2] = Bias^2(w_t) + Var(w_t), \quad (9)$$

где первая составляющая определяется скоростью изменения распределения $F_t(x)$, а вторая – объемом выборки.

При использовании фиксированного окна уменьшение дисперсии достигается за счет увеличения w , однако это приводит к росту смещенности в условиях нестационарности. В предложенном методе данный компромисс разрешается за счет адаптивного выбора размера окна.

Предположим, что семейство распределений $F_t(x)$ удовлетворяет условию Липшица:

$$|F_t(x) - F_{t-1}(x)| \leq L, \quad (10)$$

где L – константа, характеризующая скорость изменения процесса. Тогда оптимальный размер окна, минимизирующий среднеквадратичную ошибку, зависит от локальной скорости изменения распределения.

В предлагаемом методе эта зависимость аппроксимируется через локальную вариативность σ_t и интенсивность λ_t , что позволяет адаптивно приближаться к оптимальному значению w_t . В результате достигается снижение ошибки оценки квантиля по сравнению с фиксированным окном:

$$E[\varepsilon_t^2]_{adaptive} \leq E[\varepsilon_t^2]_{fixed}. \quad (11)$$

Таким образом, предложенный метод обеспечивает более устойчивую оценку порогового значения в условиях нестационарности данных.

Обсуждение

Проведенный анализ показал, что использование адаптивной оконной фильтрации при оценке квантильного порога обеспечивает более устойчивые результаты по сравнению с классическим подходом, основанным на фиксированном размере окна. Ключевое преимущество метода заключается в способности учитывать локальные изменения характеристик временного ряда, что особенно важно в условиях нестационарности поведенческих данных.

Анализ механизма адаптации демонстрирует, что при увеличении вариативности и интенсивности событий размер окна уменьшается, обеспечивая более оперативную реакцию на изменения распределения. В условиях стабильного поведения, напротив, окно увеличивается, что снижает влияние случайных флуктуаций. Таким образом, достигается баланс между чувствительностью метода и устойчивостью оценки квантильного порога.

Сравнение с классическим подходом показывает, что использование фиксированного окна может приводить к запаздыванию адаптации порогового значения и увеличению числа ложноположительных срабатываний, тогда как предложенный метод обеспечивает более гибкую реакцию на изменения данных. В то же время эффективность метода зависит от выбора параметров адаптации и способа оценки локальных характеристик временного ряда. Кроме того, практическая эффективность подобных методов во многом определяется качеством исходных данных, полнотой журналирования событий и архитектурой системы мониторинга, обеспечивающей непрерывный сбор и обработку телеметрии [15–17].

Заключение

В работе предложен метод адаптивной оконной фильтрации при расчёте квантильного порога для задач обнаружения инсайдерской активности. Показано, что предложенный подход позволяет повысить устойчивость оценки и улучшить адаптацию к изменяющимся условиям по сравнению с методами с фиксированным окном.

Практическая значимость метода заключается в возможности его применения в системах анализа поведения пользователей и сущностей (UEBA), а также в других задачах обнаружения аномалий в потоковых данных.

В качестве направлений дальнейших исследований целесообразно рассмотреть методы автоматической настройки параметров адаптации, а также расширение предложенного подхода на многомерные признаки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Kantchelian A., Neo C., Stevens R. Facade: High-precision insider threat detection using deep contextual anomaly detection //arXiv. – 2024. – С. 1–15.
2. Kamatchi K., Ramesh S. Insights into user behavioral-based insider threat detection: A systematic review //International Journal of Information Security. – 2025. – С. 1–20.

3. Parimalla S. Hunting the invisible: Harnessing UEBA to unmask insider threats //IntechOpen. – 2025. – С. 1–20.
4. Ofori H. K., Mensah K. Machine learning and deep learning for insider threat detection: A bibliometric review //Symmetry. – 2025. – Т. 17. – №. 10. – С. 1–20.
5. Song Y., Chen J. Insider threat detection based on UEBA models //Lecture Notes in Computer Science. – 2024. – С. 210–225.
6. Ibraheem I. O., Morufat A. T., Segbefia S. K. Detecting malicious insider threats through anomaly-based user behaviour analytics in enterprise networks //Southern African Journal of Security. – 2025. – С. 1–23.
7. Koli L., Kalra S., Thakur R. AI-driven insider risk management with adaptive scoring and behavioral analytics //arXiv. – 2025. – С. 1–18.
8. Feng W., Liu Y., Zhang X. Multi-granularity user anomalous behavior detection //Applied Sciences. – 2024. – Т. 15. – №. 1. – С. 128–140.
9. Ahmad W., Khan M. Leveraging machine learning for internal user behaviour analytics in cybersecurity //International Journal of Information Technology and Information Systems. – 2025. – С. 1–15.
10. Cain J., Beadles H. Mask-based window-level insider threat detection for campaign discovery //arXiv. – 2026. – С. 1–12.
11. Tian T., Li H., Zhou X. Insider threat detection for specific threat scenarios //Journal of Big Data. – 2025. – С. 1–18.
12. A-UEBA: An anomaly heterogeneity learning framework for user and entity behavior analytics //Proceedings of ACM Conference. – 2026. – С. 1–10.
13. Ye X., Zhang Y., Wang Z. Insider threat detection using hybrid deep learning models //Scientific Reports. – 2025. – Т. 15. – С. 1–12.
14. Huang Z., Tang X., Li H. TabSec: A collaborative framework for insider threat detection //arXiv. – 2024. – С. 1–14.
15. Muñoz D. A., Homoliak I. Dataset generation for insider threat detection systems //Computers & Security. – 2025. – С. 1–14.
16. Басыня Е. А., Худяков Д. С. Комплексный мониторинг информационной инфраструктуры предприятия //Защита информации. Инсайд. – 2020. – №. 6. – С. 28–33.
17. Стрельцов А. С., Французова Г. А., Басыня Е. А. Разработка системы сбора, обработки и анализа событий информационной инфраструктуры предприятия //Системы анализа и обработки данных. – 2023. – №. 1 (89). – С. 101–113.

© И. В. Махорин, 2026