

А. А. Цыганков¹✉

Анализ проблем в области выявления аномалий в действиях пользователей информационных систем на основе поведенческой аналитики

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

Аннотация. В статье рассматривается проблема выявления аномалий в действиях пользователей информационных систем с использованием методов поведенческой аналитики. Основная проблема исследований в данной области заключается в существующих ограничениях современных систем обнаружения инцидентов информационной безопасности, в частности высокая доля ложных срабатываний, дисбаланс данных и неспособность адаптации к изменениям в поведении. Целью работы является анализ проблем в области выявления аномалий в действиях пользователей информационных систем на основе поведенческой аналитики. В результате исследования определены фундаментальные проблемы существующих подходов, среди которых выделены: концептуальный сдвиг, острая нехватка качественных размеченных наборов данных, коллизии между сбором пользовательских метрик и правом на неприкосновенность частной жизни, а также проблема дисбаланса классов.

Ключевые слова: инсайдер, машинное обучение, кибербезопасность

A. A. Tsygankov¹✉

Analysis of problems in the field of detecting anomalies in user behavior within information systems based on behavioral analytics

¹National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: aatsygankov@mephi.ru

Abstract. The article considers the problem of detecting anomalies in the actions of information system users using behavioral analytics methods. The main problem of research in this area lies in the existing limitations of modern information security incident detection systems, in particular, a high rate of false positives, data imbalance, and the inability to adapt to changes in behavior. The objective of this work is the analysis of problems in the field of detecting anomalies in the actions of information system users based on behavioral analytics. As a result of the study, fundamental problems of existing approaches were identified, among which the following are highlighted: concept drift, an acute shortage of high-quality labeled datasets, conflicts between the collection of user metrics and the right to privacy, as well as the problem of class imbalance.

Keywords: insider, machine learning, cybersecurity

Введение

Современные сетевые операционные системы ежедневно генерируют значительные объемы журналов событий, включающих сотни тысяч записей, отражающих различные аспекты пользовательской активности: обращения к ресурсам, процессы аутентификации и деаутентификации, а также иные события, ре-

гистрируемые в соответствии с установленными политиками информационной безопасности. Накопление и анализ таких данных создают предпосылки для построения поведенческих моделей пользователей.

При наличии достаточного объема и качества данных становится возможным формирование профиля нормального поведения пользователя, который может быть использован в задачах классификации с применением методов и алгоритмов машинного обучения. Сравнение текущей активности с эталонной моделью позволяет выявлять отклонения, интерпретируемые как аномалии. Такие аномалии могут свидетельствовать о потенциальных инцидентах информационной безопасности, включая несанкционированный доступ или компрометацию учётных записей.

В рамках данного исследования рассматриваются существующие подходы и решения в области обнаружения аномалий пользовательского поведения в информационных системах. Анализируются их ограничения, такие как высокая доля ложных срабатываний, сложность адаптации к изменяющемуся поведению пользователей, требования к объёму обучающих данных и вычислительным ресурсам. На основе проведенного анализа формулируются ключевые научные и практические вызовы, стоящие перед современными системами обнаружения аномалий, а также обосновываются направления дальнейших исследований, направленных на повышение точности, интерпретируемости и масштабируемости таких систем.

Целью исследования является анализ проблем в области выявления аномалий в действиях пользователей информационных систем на основе поведенческой аналитики. Для ее решения была проведена декомпозиция на атомарные подзадачи, а именно:

- 1) исследование предметной области;
- 2) моделирование предметной области;
- 3) анализ проблематики предметной области.

Теоретическая значимость исследования заключается в развитии подходов к анализу журналируемых действий пользователей информационных систем. Практическая значимость определяется возможностью применения исследуемых методов в системах обеспечения информационной безопасности с целью обеспечения информационной безопасности.

Исследование предметной области

UEBA (англ. User and Entity Behavior Analytics) представляет собой направление в области поведенческой кибербезопасности, ориентированное на выявление аномалий в активности пользователей и сущностей (устройств, сервисов, учётных записей) на основе анализа их поведенческих паттернов. Формально задача UEBA сводится к задаче обнаружения аномалий (anomaly detection) и, в отдельных случаях, к задаче классификации или ранжирования событий по степени риска.

В современной научной литературе доминируют методы машинного обучения (ML) и глубокого обучения (DL) [1, 2]. В работах используются методы

опорных векторов для построения границы нормального поведения; методы главных компонент для снижения размерности и выявления аномалий через реконструкционную ошибку; алгоритм изолированного леса, используя который аномалии изолируются быстрее нормальных точек [3]. С развитием отрасли нейросетевых моделей расширяются и методы, применяемые в кибербезопасности. Например, в исследовании [4] рассматривается использование GNN (англ. Graph Neural Network), применяемые для моделирования сложных взаимосвязей между пользователями и сущностями. Помимо этого, активно используются генеративно-состязательные сети (GAN) для классификации поведения пользователей и автоматического подбора гиперпараметров, что позволяет адаптироваться к реальным системам с сохранением высокой точности [5].

Одной из фундаментальных проблем UEBA-систем является нехватка размеченных данных, особенно для редких или ранее неизвестных атак. Для решения этой проблемы активно исследуются методы выявления аномалий, использующие минимальное количество данных для начала функционирования. В частности, разрабатываются новые методы FSL (англ. Few-shot learning) [6] и ZSL (англ. Zero-shot learning) [7]. Первые используются для обучения моделей при наличии малого числа размеченных примеров. Интеграция же методов ZSL необходима для определения ранее не встречаемых классов, что в рамках кибербезопасности является критически важной возможностью.

Существуют также классические методы обнаружений аномального поведения пользователей, в частности использование подходов, основанных на правилах (англ. rule-based), ручной анализ журналов событий. Очевидно, что второй полностью исключает возможность определения инцидента информационной безопасности в момент совершения атаки. Подход, основанный на правилах, эффективен при детектировании известных атак или нарушений политики безопасности [8], однако, данный метод строго ограничен скоростью внедрения новых правил и абсолютно не защищает от атак нового типа, что в условиях активного развития киберпреступности является одним из ключевых факторов, на которых основываются специалисты при выборе системы защиты.

Моделирование предметной области

Процесс взаимодействия пользователя с информационной системой может быть формализован в виде стохастического процесса. Поведение пользователя может описываться последовательностью сессий S , каждая из которых содержит многомерный вектор признаков $\{e_1, e_2, \dots, e_n\}$. Каждый из признаков e_i может содержать временные метки, сетевые запросы, транзакции и многое другое. На рис. 1 показана BPMN-диаграмма (англ. Business Process Model and Notation) процесса трансформации пользовательской активности в векторы признаков для выявления аномалий.

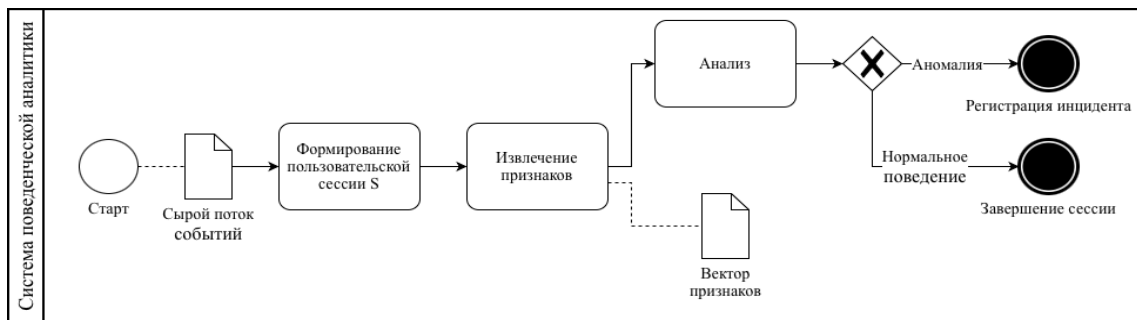


Рис. 1. BPMN-модель процесса трансформации пользовательской активности в векторы признаков для выявления аномалий

Изначально процесс инициализируется получением артефакта входных данных – сырого потока событий, который агрегирует сетевые запросы, процессы идентификации, временные метки и иные артефакты. На первом вычислительном этапе разрозненные события структурируются в рамках задачи формирования пользовательской сессии S . Далее следует этап извлечения признаков, результатом выполнения которого является многомерный вектор признаков $\{e_1, e_2, \dots, e_n\}$. Сформированный вектор передается в блок логического анализа, где модель оценивает степень отклонения текущего поведения от профиля нормального поведения пользователя. В случае, если выявленные отклонения трактуются алгоритмом как аномалия, процесс переходит по соответствующей ветви и инициирует терминальное событие — регистрацию инцидента информационной безопасности. В противном случае сессия завершается штатно.

Анализ проблематики предметной области

Важной проблемой в моделировании активности пользователя остается возможное образование концептуального сдвига (англ. *concept drift*) [9]. Он описывает непредсказуемые изменения в базовом распределении потоковых данных с течением времени. Например, смена формата работы, должности, переход к решению задач другого типа и многие другие перемены в жизни исследуемого пользователя могут изменить его поведение, что приведет к выявлению аномалии и, как следствие, ложноположительному срабатыванию.

Помимо этого, известной проблемой является дисбаланс данных (англ. *imbalanced data*). Например, в синтетическом датасете *CERT Insider Threat Dataset*, который был разработан научной группой Университета Карнеги – Меллона, на 1000 записей приходится всего 30 аномалий [10]. Проблема появляется именно тогда, когда экземпляры одного класса преобладают над экземплярами другого класса – в приведенном наборе данных, например, лишь 3% данных должны быть корректно определены как аномалии. В таких ситуациях модели зачастую снижают точность выявления аномалий и происходит смещение.

Фундаментальной проблемой во всей области детекции аномалий в действиях пользователей является исключительная редкость датасетов, на которых можно строить и обучать модели [11]. Организации, разрабатывающие собствен-

ные решения, зачастую не публикуют собственные журналы событий с размеченными данными по понятным причинам: такие данные содержат конфиденциальную информацию сотрудников и, конечно, могут использоваться злоумышленниками для получения чувствительной информации. В свою очередь синтетические датасеты, используемые в большинстве исследований, обладают недостатками любых синтетических данных: они в лучшем случае не полностью отражают реальность.

Строго говоря, проблемой является даже сам по себе анализ поведения пользователей, поскольку он зачастую вступает в прямое противоречие с законами о защите персональных данных. Это значит, что система детекции аномалий в пользовательском поведении должна не просто собирать максимальное количество требуемой ей для обучения информации, но и при этом не нарушать право сотрудников на неприкосновенность частной жизни.

Заключение

В ходе проведенного исследования был выполнен комплексный анализ проблем выявления аномалий в действиях пользователей информационных систем с использованием методов поведенческой аналитики. Установлено, что классические подходы, основанные на правилах и ручном анализе журналов, обладают критическими ограничениями, так как не способны выявлять новые типы кибератак в момент их совершения. Помимо этого, определены фундаментальные проблемы, существенно ограничивающие эффективность современных систем обнаружения аномалий, а именно:

- 1) естественные изменения в поведении сотрудников приводят к высокому уровню ложноположительных срабатываний;
- 2) преобладание записей нормального поведения над аномалиями приводит к смещению алгоритмов и снижению точности детекции;
- 3) отсутствие реальных (не синтетических) корпоративных датасетов делает невозможным качественное обучение моделей;
- 4) необходимость сбора максимального объема метрик для профилирования вступает в прямое противоречие с правом пользователей на неприкосновенность частной жизни и законами о защите персональных данных.

Основным направлением дальнейших исследований в данной области должна стать разработка и интеграция подходов, не требующих больших объемов обучающих выборок. В частности, развитие методов FSL и ZSL, что позволит системам обеспечения информационной безопасности эффективно классифицировать ранее неизвестные инциденты. Решение выявленных проблем позволит существенно повысить точность, интерпретируемость и масштабируемость систем поведенческой аналитики.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Mizanur M. et al. Machine learning-based anomaly detection for cyber threat prevention //Journal of Primeasia. – 2025. – Т. 6. – №. 1. – С. 1-8.

2. Mihailescu M. I. et al. Unveiling threats: Leveraging user behavior analysis for enhanced cybersecurity //2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). – IEEE, 2023. – C. 01-06.
3. Lanuwabang L., Sarasu P. Detection of Anomalies Based on User Behavioral Information: A Survey //International Journal of Wireless and Microwave Technologies (IJWMT). – 2025. – T. 15. – №. 3. – C. 54-65.
4. Ares-Robledo F., Rifà-Pous H., Clarisó R. Graph neural networks for anomaly detection: a systematic review of dynamic temporal approaches //Artificial Intelligence Review. – 2026.
5. Xia X. et al. GAN-based anomaly detection: A review //Neurocomputing. – 2022. – T. 493. – C. 497-535.
6. Gamal M. et al. Few-shot learning for discovering anomalous behaviors in edge networks //Computers, Materials and Continua. – 2021. – T. 69. – №. 2. – C. 1823-1837.
7. Demirel D. Y., Sandikkaya M. T. Web based anomaly detection using zero-shot learning with CNN //IEEE Access. – 2023. – T. 11. – C. 91511-91525.
8. Alzaabi F. R., Mehmood A. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods //IEEE Access. – 2024. – T. 12. – C. 30907-30927.
9. Lu J. et al. Learning under concept drift: A review //IEEE transactions on knowledge and data engineering. – 2018. – T. 31. – №. 12. – C. 2346-2363.
10. Bin Sarhan B., Altwaijry N. Insider threat detection using machine learning approach //Applied Sciences. – 2022. – T. 13. – №. 1. – C. 259.
11. Manoharan P. et al. Insider threat detection using supervised machine learning algorithms //Telecommun. Syst. – 2024. – T. 87. – №. 4. – C. 899-915.

© A. A. Цыганков, 2026