

Научная статья

DOI 10.66424/2071-8217-2026-3-8

УДК 004.056

ИНТЕГРАЦИЯ РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМ В АРХИТЕКТУРУ UEBA ДЛЯ ОБНАРУЖЕНИЯ ПОВЕДЕНЧЕСКИХ АНОМАЛИЙ

С. В. Логачева, Н. О. Москалев, Д. С. Лаврова*

Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия

✉ *lavrova_ds@spbstu.ru

ДЛЯ ЦИТИРОВАНИЯ

Логачева С. В., Москалев Н. О., Лаврова Д. С. Интеграция рекомендательных систем в архитектуру UEBA для обнаружения поведенческих аномалий // Проблемы информационной безопасности. Компьютерные системы. 2026. № 3. С. 110–119. DOI: 10.66424/2071-8217-2026-3-8

ПОСТУПИЛА 06.07.2026

ПРИНЯТА 03.08.2026

ОПУБЛИКОВАНА 13.10.2026

© Логачева С. В., Москалев Н. О., Лаврова Д. С.

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Исследование посвящено проблеме обнаружения поведенческих аномалий в корпоративных информационных системах, потенциально связанных с действиями внутренних нарушителей. Проведен анализ существующих систем UEBA (User and Entity Behavior Analytics). Выявленные недостатки известных решений подчеркивают необходимость создания новых подходов к анализу поведения пользователей. В качестве решения разработан подход к интеграции рекомендательных систем в архитектуру UEBA, основанный на переформулировании задачи обнаружения аномалий как задачи оценки типичности поведения пользователя на основе коллективного опыта. Целесообразность применения подхода обоснована теоретически и подтверждена экспериментально. Полученные результаты показывают превосходство предложенного подхода над базовыми методами по метрикам Precision и F1-score и могут быть использованы для создания новых защитных решений.

КЛЮЧЕВЫЕ СЛОВА

UEBA, рекомендательные системы, поведенческая аналитика, коллаборативная фильтрация, обнаружение аномалий, внутренние угрозы

Original article

DOI 10.66424/2071-8217-2026-3-8

INTEGRATION OF RECOMMENDER SYSTEMS INTO UEBA ARCHITECTURE FOR BEHAVIORAL ANOMALY DETECTION

S. V. Logacheva, N. O. Moskalev, D. S. Lavrova*

Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia

✉ *lavrova_ds@spbstu.ru

FOR CITATION

Logacheva S. V., Moskalev N. O., Lavrova D. S. Integration of

ABSTRACT

The work is devoted to the problem of detecting behavioral anomalies in corporate information systems that are potentially related to the

recommender systems into UEBA architecture for behavioral anomaly detection. *Problems of information security. Computer systems*. 2026. No. 3, pp. 110–119. DOI: 10.66424/2071-8217-2026-3-8 (In Russian)

RECEIVED 06.07.2026

ACCEPTED 03.08.2026

PUBLICATION 13.10.2026

actions of internal intruders. During the work, an analysis of existing UEBA (User and Entity Behavior Analytics) systems was conducted. The identified shortcomings of known solutions highlight the need to create new approaches to analyzing user behavior. As a solution, an approach to integrating recommendation systems into the UEBA architecture was developed, based on rephrasing the task of anomaly detection as a task of estimating the typicality of user behavior based on collective experience. The feasibility of this approach was theoretically justified and experimentally confirmed. The obtained results demonstrate the superiority of the proposed approach over the basic methods in terms of Precision and F1-score metrics and can be used to create new protective solutions.

KEYWORDS

UEBA, recommender systems, behavioral analytics, collaborative filtering, anomaly detection, insider threats

1. ВВЕДЕНИЕ

Современные корпоративные информационные системы характеризуются высокой сложностью архитектуры и значительными объемами обрабатываемых данных. В этих условиях традиционные средства защиты, ориентированные на сигнатурный анализ (межсетевые экраны, IPS, антивирусы), не обеспечивают должного уровня защиты от угроз внутреннего нарушителя и целенаправленных атак, использующих легитимные учетные данные [1–3].

Таким образом, получили развитие системы поведенческой аналитики пользователей и сущностей (User and Entity Behavior Analytics – UEBA), которые строят динамические профили «нормального» поведения и выявляют отклонения от них [4], но существующие UEBA-решения сталкиваются с рядом фундаментальных ограничений. Методы на основе статистических признаков и классического машинного обучения (Isolation Forest, Z-score) генерируют недопустимо высокий уровень ложноположительных срабатываний (FPR). В то же время модели глубокого обучения (RNN, LSTM, автоэнкодеры), обеспечивающие высокую чувствительность к многоэтапным атакам, обладают низкой интерпретируемостью – аналитик не получает объяснения, почему конкретное действие классифицировано как аномальное [5, 6].

Для решения данной проблемы предлагается интеграция механизмов рекомендательных систем (Recommender Systems) в архитектуру UEBA. Рекомендательные системы, изначально разработанные для задач персонализации в электронной коммерции, демонстрируют высокую результативность при анализе поведенческих паттернов и оценке типичности действий пользователей на основе коллективного опыта [7, 8]. Ключевое преимущество данного подхода заключается в том, что аномалия интерпретируется не как абстрактное отклонение от нормы, а как действие, не характерное для «похожих пользователей» – коллег с аналогичной ролью или отделом, что обеспечивает высокую интерпретируемость каждого оповещения.

Представлена формальная модель поведения пользователя, адаптированная для интеграции с рекомендательными алгоритмами, а также результаты экспериментального исследования предложенного подхода на синтетическом наборе данных CERT r4.2 [9].

2. ОБЗОР ПОДХОДОВ К МОДЕЛИРОВАНИЮ ПОВЕДЕНИЯ И РЕКОМЕНДАТЕЛЬНЫМ СИСТЕМАМ

В работах [4, 7] рассматриваются статистико-признаковые подходы к обнаружению

внутренних угроз на основе набора данных CERT r4.2: поведение пользователя описывается через агрегированные векторы активности, а для классификации применяются алгоритмы Random Forest, Naive Bayes и метод опорных векторов с автоматической генерацией признаков (Deer Feature Synthesis). В работах [5, 6] предлагается анализировать низкоуровневые паттерны взаимодействия пользователя с системой – динамику клавиатурного почерка, системные вызовы, последовательности действий – с использованием поведенческой биометрии и рекуррентных нейронных сетей (GRU-автоэнкодеров). Несмотря на высокую точность, данные методы либо требуют значительных усилий по ручной инженерии признаков, либо обладают низкой интерпретируемостью результатов.

В работах [8, 10] исследуются алгоритмы коллаборативной фильтрации (в частности Implicit ALS) для рекомендательных систем, работающих с неявными взаимодействиями «пользователь – элемент». Данные методы демонстрируют отличные результаты в работе с разреженными матрицами и способны выявлять скрытые зависимости между пользователями на основе коллективного опыта, но их применение в задачах информационной безопасности и, в частности в архитектуре UEBA, остается недостаточно изученным: в существующих работах рекомендательные системы рассматриваются преимущественно в контексте персонализации контента, а не оценки «ожидаемости» (типичности) поведения субъектов в корпоративной среде.

Таким образом, несмотря на наличие алгоритмов коллаборативной фильтрации (в частности Implicit ALS) в арсенале исследователей, их прямое применение для задач UEBA невозможно без доработки. Классические Recommender Systems решают задачу ранжирования, но UEBA требует бинарной классификации событий на основе отклонения от коллективного ролевого паттерна, а также механизма объяснения причин аномалии, что требует разработки новой архитектуры интеграции.

3. ФОРМАЛИЗАЦИЯ ПОДХОДА

Модель поведения пользователя. Поведение пользователя u в корпоративной информационной системе за период T описывается набором троек:

$$B_u = \{(a_i, r_i, c_i) | i = 1, \dots, n\},$$

где a_i – действие (например, access, сору, login); r_i – ресурс (файл, хост, БД); c_i – контекст (временная метка, роль, геолокация, тип устройства).

Ключевой шаг модели – интерпретация каждой такой тройки как взаимодействия «пользователь – ресурс» (u_i, r_i) . Это позволяет преобразовать историю действий в разреженную матрицу взаимодействий:

$$M \in \{0, 1\}^{|U| \times |R|},$$

где $M_{u,r} = 1$, если пользователь u когда-либо обращался к ресурсу r . Данная формализация напрямую соответствует входным требованиям алгоритмов коллаборативной фильтрации.

Предлагаемая на данном этапе формализация и бинарная матрица взаимодействий M фокусируются на выявлении ресурсно-ролевых аномалий. Временной контекст в текущей реализации матрицы свернут, что делает модель нечувствительной к нарушениям временных шаблонов. Учет хронологии и временных зависимостей требует применения Sequence-aware моделей, что запланировано в рамках дальнейших исследований.

Алгоритм обнаружения аномалий. В качестве базового алгоритма выбрана Implicit ALS (Alternating Least Squares для неявных взаимодействий), но ключевая доработка метода для задач UEBA заключается в отказе от классического ранжирования в пользу вычисления адаптивного порога аномальности и механизма пост-объяснения на основе латентного пространства [10].

Модель обучается генерировать латентные векторы для пользователей p_u и ресурсов q_r . Для нового события u, r вычисляется рекомендательная оценка (score):

$$s(u, r) = p_u^T q_r.$$

Чем выше оценка, тем более «ожидаемым» считается взаимодействие.

Обнаружение аномалий происходит с помощью адаптивного порога, рассчитываемого индивидуально для каждого пользователя:

$$\tau_u = \text{percentile}_5(\{s(u_i, r_i) | r_i \in R_u\}),$$

где R_u – множество ресурсов, с которыми пользователь взаимодействовал в обучающей выборке. Если $s(u, r_{\text{new}}) < \tau_u$, то событие помечается как аномальное.

Механизм интерпретации. Пусть пользователь X занимает должность бухгалтера (роль: accountant, отдел: finance). В обучающей выборке его поведение описывается множеством троек вида (access, file-finance, t_1), (copy, file-finance, t_2), (login, server, t_3) и т.д. Пользователь X взаимодействует только с ресурсами отделов финансов.

В матрице взаимодействий M строка, соответствующая пользователю X , имеет ненулевые значения в столбцах финансовых ресурсов. После обучения модели Implicit ALS латентный вектор пользователя X оказывается близок к латентным векторам других бухгалтеров и далек от латентных векторов, например, аналитиков, чьи векторы строятся на основе множества ресурсов по типу: (access, git-repo, t_1).

Далее зафиксировано новое событие: пользователь X в рабочее время инициирует действие (access, git-repo, t). Модель вычисляет рекомендательную оценку $s(X, \text{git-repo})$. Поскольку латентные векторы X и группы аналитиков принадлежат разным семантическим кластерам латентного пространства, значение оценки оказывается ниже адаптивного порога (пятый перцентиль оценок по историческим взаимодействиям пользователя X). Событие помечается как аномальное.

Для формирования объяснения система вычисляет косинусную близость между сравниваемыми латентными векторами и отбирает $k=5$ наиболее похо-

жих пользователей. Все они оказываются сотрудниками отдела финансов. Затем для каждого из k соседей вычисляется коэффициент Жаккара между множеством ресурсов пользователя X и соседа – значения оказываются высокими $J \approx 0,8-0,9$, что подтверждает однородность группы. При этом ни один из k соседей не имеет в истории взаимодействий ресурса git-repo.

В результате аналитику SOC формируется следующее объяснение: «Пользователь X (бухгалтер, отдел finance) пытается получить доступ к ресурсу git-repo, но ни один из пяти сотрудников с аналогичным профилем не взаимодействовал с этим ресурсом за последние 30 дней. Коэффициент Жаккара с ближайшим соседом (бухгалтер Y): $J=0,87$ ».

Это напрямую решает проблему «черного ящика» традиционных UEBA-систем.

4. ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ

Для оценки результатов предложенного подхода реализован прототип. Эксперименты проводились на синтетическом наборе данных CERT Insider Threat Dataset v4.2 [9], содержащем данные аутентификации, работы с файлами, HTTP-трафика и устройств [11]. В данные вписаны синтетические аномалии (например, доступ к чувствительным файлам в нерабочее время).

В качестве базовых моделей для сравнения выбраны:

- Isolation Forest – на признаках: количество действий в день, энтропия ресурсов, время, роль;
- Z-score – анализ частоты доступа к ресурсам;
- Rule-based – простое правило: доступ к ресурсам с 22:00 до 07:00 считается аномалией.

Поскольку модель работает со статической матрицей взаимодействий, она предназначена для обнаружения аномалий,

Таблица 1 | Результаты тестирования на базовом наборе данных

Table 1 | Test results on the base dataset

Модель	Precision	Recall	F1-score	AUC-PR	FPR	Интерпретируемость
Implicit ALS	0,86	0,79	0,82	0,90	0,08	Высокая
Isolation Forest	0,72	0,65	0,68	0,75	0,15	Средняя
Z-score	0,68	0,52	0,59	0,62	0,22	Низкая
Rule-based	0,55	0,88	0,68	0,58	0,45	Высокая

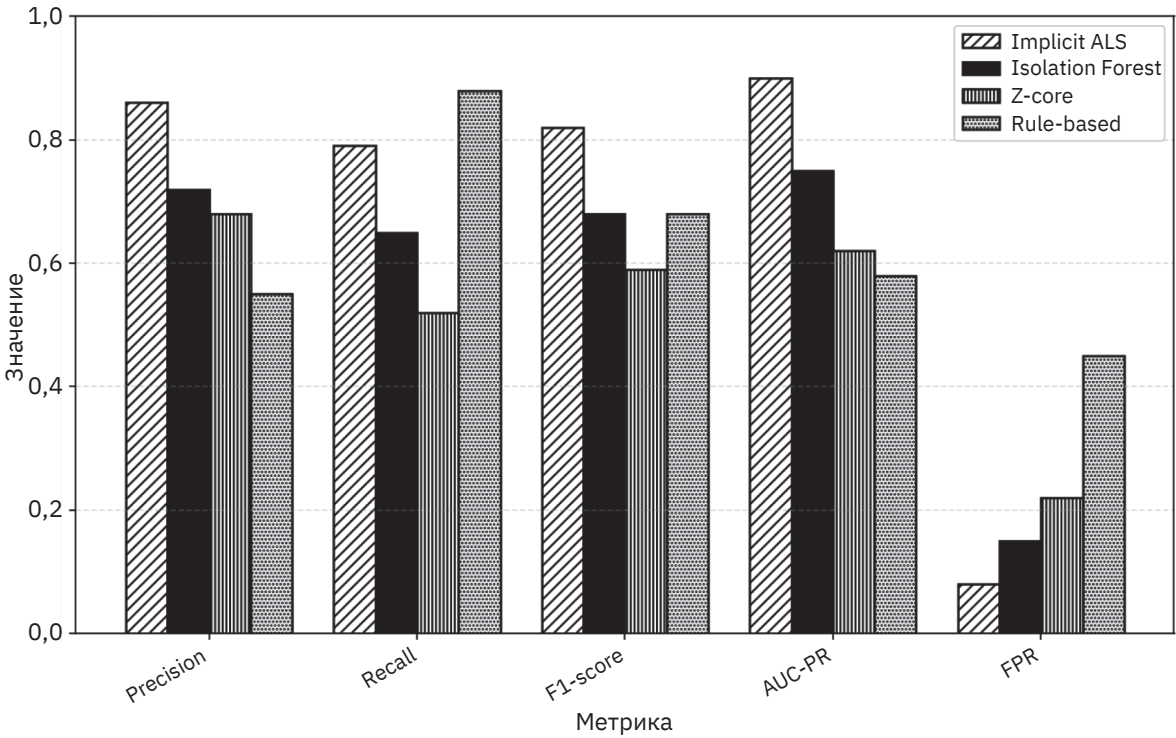


Рис. 1 | Сравнение метрик различных моделей в эксперименте на базовом наборе данных

Fig. 1 | Comparison of metrics for different models in the experiment on the baseline dataset

связанных с выходом за пределы семантического профиля. Выявление многоэтапных атак, проявляющихся в изменении последовательности действий при сохранении набора ресурсов, выходит за рамки данного исследования и требует интеграции с графовыми моделями.

Эксперимент 1. Базовый набор данных. Использовался синтетический набор данных на основе CERT r4.2: 1000 пользователей, 5000 ресурсов, 100 000 событий,

из которых 5 % – искусственные аномалии. Результаты тестирования представлены в табл. 1 и на рис. 1.

Предложенный подход на основе рекомендательной системы продемонстрировал наилучший баланс между точностью и полнотой, значительно превосходя простые статистические и эвристические методы. Особенно важно низкое значение FPR (8 %), что критично для практического применения в SOC, где большое количе-

Таблица 2 | Результаты тестирования при увеличенном размере данных
Table 2 | Test results with an increased data size

Модель	Precision	Recall	F1-score	AUC-PR	FPR	Интерпретируемость
Implicit ALS	0,85	0,78	0,81	0,89	0,09	Высокая
Isolation Forest	0,73	0,66	0,69	0,76	0,14	Средняя
Z-score	0,69	0,53	0,60	0,63	0,21	Низкая
Rule-based	0,56	0,87	0,69	0,59	0,44	Высокая

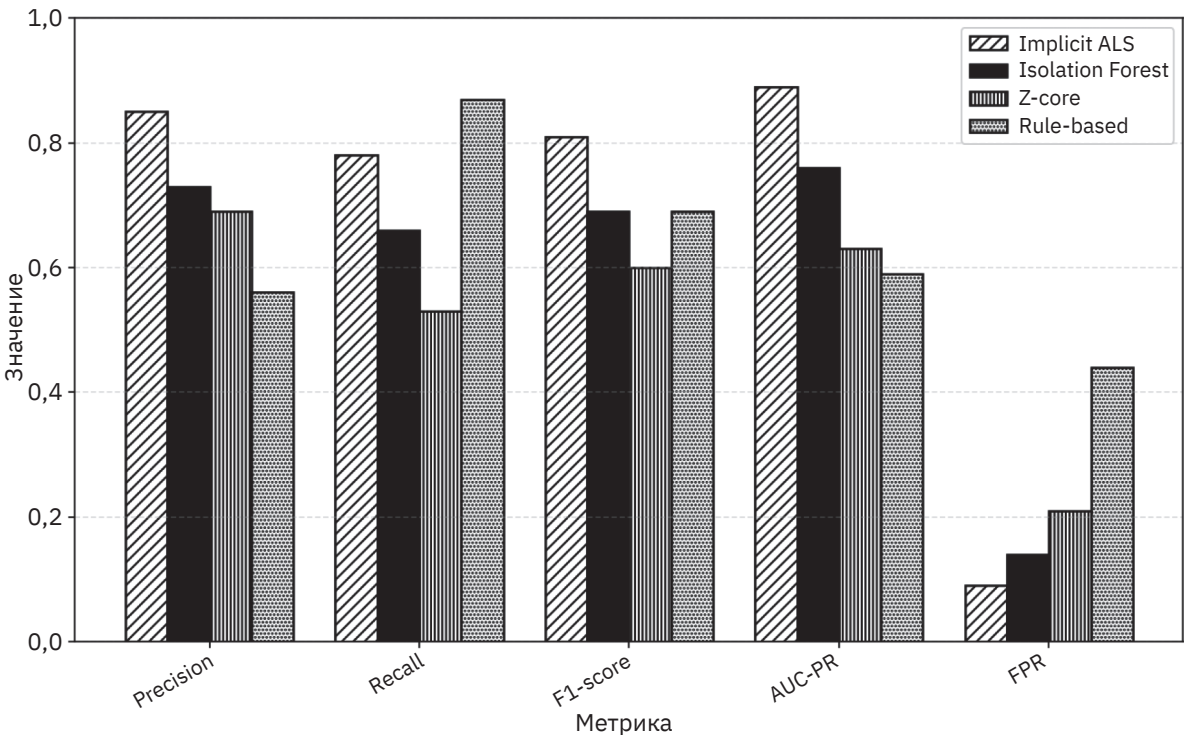


Рис. 2 | Сравнение метрик различных моделей в эксперименте при увеличенном размере данных
Fig. 2 | Comparison of metrics for various models in the experiment with an increased data size

ство ложных срабатываний снижает доверие аналитиков.

Эксперимент 2. Увеличенный размер данных. Для оценки масштабируемости модели проведен эксперимент на расширенном наборе данных (2 705 719 строк, 587 аномалий – около 0,02 % от общего числа). Результаты тестирования представлены в табл. 2 и на рис. 2.

Результаты подтверждают устойчивость предложенного подхода: метрики

практически не изменились при увеличении объема данных в 27 раз, что свидетельствует о хорошей масштабируемости модели.

Эксперимент 3. Изменение порога обнаружения. В третьем эксперименте изменена стратегия определения аномалий: вместо пятого перцентиля использован первый перцентиль, что повысило чувствительность модели. Результаты тестирования представлены в табл. 3 и на рис. 3.

Таблица 3 | Результаты тестирования при другом пороге обнаружения

Table 3 | Test results at a different detection threshold

Модель	Precision	Recall	F1-score	AUC-PR	FPR	Интерпретируемость
Implicit ALS	0,84	0,82	0,83	0,88	0,10	Высокая
Isolation Forest	0,71	0,68	0,69	0,74	0,16	Средняя
Z-score	0,67	0,55	0,60	0,61	0,67	Низкая
Rule-based	0,54	0,90	0,68	0,57	0,54	Высокая

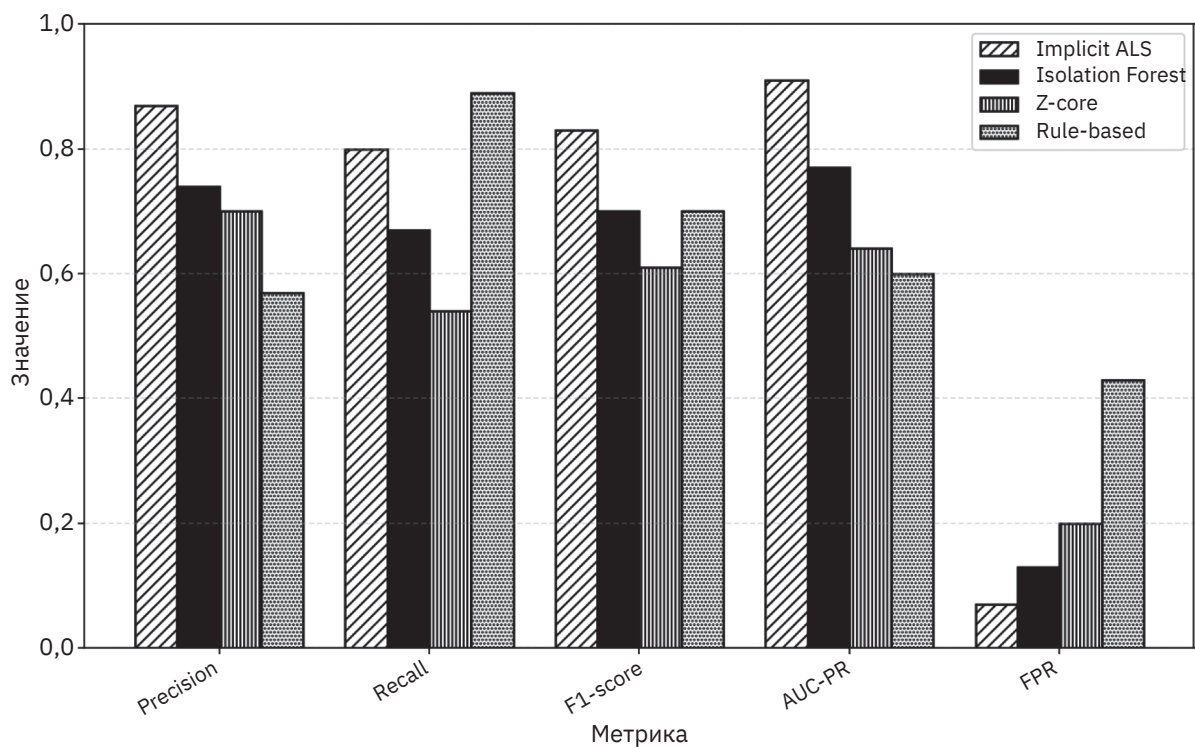


Рис. 3 | Сравнение метрик различных моделей в эксперименте с измененным порогом обнаружения

Fig. 3 | Comparison of metrics for different models in an experiment with a modified detection threshold

Снижение порога привело к росту Recall при незначительном снижении Precision, что демонстрирует гибкость адаптивного механизма обнаружения.

Результаты экспериментов подтверждают гипотезу: рекомендательные системы, адаптированные для задач UEBA, могут значительно повысить качество обнаружения аномалий по сравнению с традиционными методами.

Ключевые преимущества предложенного подхода:

- персонализация – модель учитывает индивидуальные паттерны каждого пользователя;
- устойчивость к шуму – благодаря использованию скрытых факторов и контекста, система игнорирует случайные отклонения;
- интерпретируемость – объяснения на основе «похожих пользователей» делают

оповещения понятными для аналитиков безопасности.

Ограничения:

1. Проблема «холодного старта». Модель полностью зависит от исторических данных. Для новых пользователей или новых ресурсов формирование латентного вектора невозможно без применения контентных эвристик (например, привязки к должности или отделу), что сужает применение в динамичных средах.

2. Уязвимость к «медленным» внутренним нарушителям. Поскольку модель формирует статический профиль на основе накопленной истории, злоумышленник, методично и постепенно расширяющий круг доступа к новым ресурсам в рамках своей роли, не будет обнаружен, так как модель адаптирует «нормальный профиль» под его действия. Для решения ограничения требуется внедрение механизмов скользящего окна (sliding window).

3. Ограниченность пакетного обучения. Модель Implicit ALS предполагает обучение на фиксированном наборе данных. В условиях реальной эксплуатации роли сотрудников и состав ресурсов эволюционируют. Без механизма онлайн-обновления латентных представлений модель будет генерировать ложные срабатывания на легитимные изменения в поведении, что требует дорогостоящего периодического переобучения.

5. ЗАКЛЮЧЕНИЕ

Решена актуальная задача повышения точности обнаружения аномалий системами поведенческой аналитики за счет интеграции механизмов рекомендательных систем. Ключевым научным результатом является разработка формальной модели поведения пользователя, основанной на переформулировании задачи обнаружения аномалий как задачи оценки семантической близости действий к ролевому паттерну. Представление активности в виде троек «действие – ресурс – контекст» позволило адаптировать алгоритмы коллаборативной фильтрации (Implicit ALS) для задач информационной безопасности, обеспечив высокую персонализацию профилей и учет коллективного опыта «похожих пользователей».

Проведенное экспериментальное исследование на синтетическом наборе данных CERT r4.2 включало три этапа и подтвердило гипотезу о результативности предложенного подхода. В базовом эксперименте модель продемонстрировала наилучший баланс между точностью и полнотой (Precision = 0,86, F1-score = 0,82) при критически низком уровне ложных срабатываний (FPR = 8 %), что значительно превосходит традиционные методы (Isolation Forest, Z-score, Rule-based). Второй эксперимент доказал масштабируемость решения: метрики практически не изменились при увеличении объема данных в 27 раз. Третий эксперимент показал гибкость адаптивного механизма обнаружения: снижение порога с пятого до первого перцентиля позволило повысить полноту (Recall) с минимальными потерями в точности.

Практическая значимость заключается в создании интерпретируемого механизма генерации оповещений. В отличие от моделей глубокого обучения, работающих как «черный ящик», предложенный подход предоставляет аналитикам SOC быстро интерпретируемые объяснения причин аномалии через поведение коллег, что напрямую снижает нагрузку на специалистов и ускоряет время расследования инцидентов (MTTD).

Несмотря на положительные результаты, текущая реализация имеет ряд ограничений, среди которых проблема «холодного старта» для новых пользователей и ресурсов, а также статичность модели после обучения. В качестве направлений дальнейших исследований планируется:

- интеграция Sequence-aware моделей (LSTM, Transformers) для учета хронологии событий и выявления многоэтапных атак;
- переход к инкрементальному онлайн-обучению для адаптации к динамическим изменениям ролей сотрудников и предотвращения ложных срабатываний при эволюции их поведенческих паттернов;
- использование графовых нейронных сетей (GNN) для структурного анализа взаимодействий в корпоративной сети;
- проведение пилотного внедрения и тестирования на реальных промышленных данных корпоративных SIEM-систем для оценки операционной нагрузки в условиях production-среды.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года. URL: <https://ptsecurity.com/research/analytics/> (дата обращения: 03.04.2026).
2. CODE RED 2026: Актуальные киберугрозы для российских организаций. URL: <https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/> (дата обращения: 03.04.2026).
3. Севастей Е. А. Интеллектуальные методы анализа поведения пользователей как инструмент раннего предсказания кибератак // Молодой ученый. 2025. № 45. С. 12–14.
4. Dosh M. Detecting insider threat within institutions using CERT dataset and different ML techniques // Periodicals of Engineering and Natural Sciences. 2021. Vol. 9. № 2. P. 873–884.
5. Yampolskiy R. V., Govindaraju V. Behavioural biometrics: a survey and classification // Int. J. Biometrics. 2008. Vol. 1. № 1. P. 81–113. DOI: 10.1504/IJBM.2008.018665.
6. Nepal S., Joshi B. User Behavior Analytics for Insider Threat Detection using Deep Learning // Proceedings of 10th IOE Graduate Conference. 2021. Vol. 10. P. 232–238.
7. Sarhan B. B., Altwaijry N. Insider Threat Detection Using Machine Learning Approach // Applied Sciences. 2023. № 13 (1). P. 259–278. DOI: 10.3390/app13010259
8. Курочкин А. И., Лобанов А. А. Сравнение подходов коллаборативной и контенто-ориентированной фильтрации в рекомендательных системах // Парадигма. 2025. № 6–1. С. 85–90.
9. InsiderThreatTestDataset. URL: https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247/1?file=24856766 (дата обращения: 03.04.2026).
10. Hu Y., Koren Y., Volinsky C. Collaborative filtering for implicit feedback datasets // 2008 Eighth IEEE International Conference on Data Mining, Pisa, Italy. 2008. P. 263–272. DOI: 10.1109/ICDM.2008.22.
11. UEBA: как анализ поведения помогает защищать данные. URL: <https://habr.com/ru/articles/878142/> (дата обращения: 03.04.2026).
12. Insider Threat Test Dataset. URL: https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247 (дата обращения: 03.04.2026).
13. Landauer M., Skopik F., Wurzenberger M. A User and Entity Behavior Analytics Log Data Set for Anomaly Detection in Cloud Computing // 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan. 2022. P. 4285–4294. DOI: 10.1109/BigData55660.2022.10020672.
14. Singh A. P., Sharma A. A systematic literature review on insider threats // arXiv:2212.05347. 2022.
15. What is the Cold Start Problem in Recommender Systems? URL: <https://www.freecodecamp.org/news/cold-start-problem-in-recommender-systems/> (дата обращения: 03.04.2026).

REFERENCES

1. Current cyber threats: Q4 2024 – Q1 2025. URL: <https://ptsecurity.com/research/analytics/> (accessed: 03.04.2026).
2. CODE RED 2026: Current cyber threats to Russian organizations. URL: <https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/> (accessed: 03.04.2026).
3. Sevastei E. A. Intelligent methods for analyzing user behavior as a tool for early prediction of cyberattacks. *Molodoj uchenyj*. 2025. No. 45, pp. 12–14.
4. Dosh M. Detecting insider threat within institutions using CERT dataset and different ML techniques. *Periodicals of Engineering and*

- Natural Sciences*. 2021. Vol. 9. No. 2, pp. 873–884.
5. **Yampolskiy R. V., Govindaraju V.** Behavioural biometrics: a survey and classification. *Int. J. Biometrics*. 2008. Vol. 1. No. 1, pp. 81–113. DOI: 10.1504/IJBM.2008.018665.
 6. **Nepal S., Joshi B.** User Behavior Analytics for Insider Threat Detection using Deep Learning. Proceedings of 10th IOE Graduate Conference. 2021. Vol. 10, pp. 232–238.
 7. **Sarhan B. B., Altwaijry N.** Insider Threat Detection Using Machine Learning Approach. *Applied Sciences*. 2023. No. 13 (1), pp. 259–278. DOI: 10.3390/app13010259.
 8. **Kurochkin A. I., Lobanov A. A.** Comparison of collaborative and content-based filtering approaches in recommender systems. *Paradigma*. 2025. No. 6–1, pp. 85–90.
 9. InsiderThreatTestDataset. URL: https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247/1?file=24856766 (accessed: 03.04.2026).
 10. **Hu Y., Koren Y., Volinsky C.** Collaborative filtering for implicit feedback datasets. 2008 Eighth IEEE International Conference on Data Mining, Pisa, Italy. 2008, pp. 263–272. DOI: 10.1109/ICDM.2008.22.
 11. UEBA: How behavior analysis helps protect data. URL: <https://habr.com/ru/articles/878142/> (accessed: 03.04.2026).
 12. Insider Threat Test Dataset. URL: https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247 (accessed: 03.04.2026).
 13. **Landauer M., Skopik F., Wurzenberger M.** A User and Entity Behavior Analytics Log Data Set for Anomaly Detection in Cloud Computing. 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan. 2022, pp. 4285–4294. DOI: 10.1109/BigData55660.2022.10020672.
 14. **Singh A. P., Sharma A.** A systematic literature review on insider threats. *arXiv:2212.05347*. 2022.
 15. What is the Cold Start Problem in Recommender Systems? URL: <https://www.freecodecamp.org/news/cold-start-problem-in-recommender-systems/> (accessed: 03.04.2026).

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

ЛОГАЧЕВА Светлана Викторовна – студент, Санкт-Петербургский политехнический университет Петра Великого, Россия, 195251, Санкт-Петербург, ул. Политехническая, д. 29
E-mail: logacheva_sv@edu.spbstu.ru

LOGACHEVA Svetlana V. – Student, Peter the Great St. Petersburg Polytechnic University, Russia, 195251, St. Petersburg, Polytechnicheskaya str., 29

МОСКАЛЕВ Никита Олегович – студент, Санкт-Петербургский политехнический университет Петра Великого, Россия, 195251, Санкт-Петербург, ул. Политехническая, д. 29
E-mail: moskalev.no@ibks.spbstu.ru

MOSKALEV Nikita O. – Student, Peter the Great St. Petersburg Polytechnic University, Russia, 195251, St. Petersburg, Polytechnicheskaya str., 29

ЛАВРОВА Дарья Сергеевна – д-р техн. наук, профессор, Санкт-Петербургский политехнический университет Петра Великого, Россия, 195251, Санкт-Петербург, ул. Политехническая, д. 29
E-mail: lavrova_ds@spbstu.ru
ORCID: 0000-0003-2849-4682

LAVROVA Daria S. – Doctor of Engineering Sciences, Professor, Peter the Great St. Petersburg Polytechnic University, Russia, 195251, St. Petersburg, Polytechnicheskaya str., 29