DOI 10.37882/2223-2966.2026.03.34

КАРТЫ ПОВЕДЕНЧЕСКОГО ПРОФИЛЯ КАК ИНСТРУМЕНТ ПРОЕКТИРОВАНИЯ СИСТЕМЫ UEBA

BEHAVIORAL PROFILE CARDS AS A DESIGN TOOL FOR THE UEBA SYSTEM

N. Raevskaya
A. Tsaregorodtsev
E. Bulekova
E. Usenko
A. Petrykina

Summary. In the context of growing cybercrimes, insider attacks pose a significant threat to corporate systems, disguised as legitimate activity. This article explores the use of behavioral profile maps as an innovative tool for designing UEBA (User and Entity Behavior Analytics) systems to detect such threats. It proposes a comprehensive methodology that includes the collection of data from access logs and operation metadata, their structuring, and visualization using machine learning algorithms (k-means, DBSCAN, LSTM, and t-SNE). Special attention was paid to the selection of relevant metrics, such as the frequency of requests to sensitive data and temporal anomalies, as well as integration with SIEM/DLP for prompt response. An experimental A/B test conducted in an IT media holding company confirmed the effectiveness of the approach: false positives were reduced by 80 %, quality metrics improved (Precision 0.91, Recall 0.88, F1-Score 0.89), and the response time was reduced to 5 hours.

The consideration of ethical and legal aspects, including compliance with Federal Law №152, ensured a balance between security and employees' rights. Recommendations for transparent monitoring, data anonymization, and automation of analysis were developed. The practical significance of the work lies in the creation of interpretable dashboards and templates for integration with corporate systems. Further research prospects include the use of large language models for text log analysis, the automation of ethical audits through smart contracts, and the development of monitoring standards for non-standard roles. The proposed approach forms the basis for responsible application of behavioral analytics, combining technical efficiency with ethical standards and minimizing the risks of data leaks.

Keywords: insider threats, cybersecurity, machine learning, behavioral profile.

Раевская Наталья Александровна
ФГАОУ ВО Российский университет дружбы народов, г. Москва
1132247136@rudn.ru
Царегородцев Анатолий Валерьевич
доктор технических наук, профессор, ФГАОУ ВО Российский университет дружбы народов, г. Москва
tsaregorodtsev-av@rudn.ru
Булекова Екатерина Владимировна
ФГАОУ ВО Российский университет дружбы народов, г. Москва
1132247139@pfur.ru
Усенко Елизавета Алексеевна
ФГАОУ ВО Российский университет дружбы народов, г. Москва
1132247142@pfur.ru
Петрыкина Анастасия Денисовна
ФГАОУ ВО Российский университет дружбы народов, г. Москва
1132247134@pfur.ru

Аннотация. В условиях роста киберпреступлений инсайдерские атаки представляют значительную угрозу для корпоративных систем, маскируясь под легитимную активность. В статье исследуется применение карт поведенческого профиля как инновационного инструмента проектирования систем UEBA (User and Entity Behavior Analytics) для выявления таких угроз. Предложена комплексная методика, включающая сбор данных из логов доступа и метаданных операций, их структуризацию и визуализацию с использованием алгоритмов машинного обучения (k-means, DBSCAN, LSTM, t-SNE). Особое внимание уделено выбору релевантных метрик, таких как частота запросов к конфиденциальным данным и временные аномалии, а также интеграции с SIEM/DLP для оперативного реагирования. Экспериментальное A/B-тестирование, проведенное в ИТ-медиахолдинге, подтвердило эффективность подхода: ложные срабатывания сократились на 80 %, метрики качества улучшились (Precision 0.91, Recall 0.88, F1-Score 0.89), а время реакции снизилось до 5 часов. Учет этико-правовых аспектов, включая соответствие Федеральному закону №152-ФЗ, обеспечил баланс между безопасностью и правами сотрудников. Разработаны рекомендации по прозрачному мониторингу, анонимизации данных и автоматизации анализа. Практическая значимость работы заключается в создании интерпретируемых дашбордов и шаблонов для интеграции с корпоративными системами. Перспективы дальнейших исследований включают применение больших языковых моделей для анализа текстовых логов, автоматизацию этического аудита через смарт-контракты и разработку стандартов мониторинга для нестандартных ролей. Предложенный подход формирует основу для ответственного применения поведенческой аналитики, сочетая техническую эффективность с этическими нормами и минимизируя риски утечек данных.

Ключевые слова: инсайдерские угрозы, кибербезопасность, машинное обучение, поведенческий профиль.

Введение

В условиях цифровой трансформации наблюдается значительный рост киберпреступлений, среди которых инсайдерские атаки представляют особую угрозу. По данным отчета Verizon DBIR-2025 18 % нарушений информационной безопасности связаны с действиями внутренних акторов, использующих легитимный доступ для маскировки злонамеренной активности. В отличие от внешних угроз, такие атаки сложно выявить традиционными методами, основанными на сигнатурном анализе и статичных правилах, которые не адаптируются к динамичным поведенческим паттернам [8, 9]. В частности, высокий уровень ложных срабатываний и задержки в реакции снижают эффективность таких решений [10].

На этом фоне системы класса UEBA (User and Entity Behavior Analytics) становятся перспективным инструментом, обеспечивающим анализ поведения пользователей и сущностей в реальном времени [13]. Однако их проектирование связано с рядом ограничений, включая неполноту обучающих данных, отсутствие маркированных аномалий и сложность интерпретации многомерных метрик [5]. Следовательно, возникает потребность в инновационных подходах, повышающих точность и интерпретируемость анализа. В данном контексте карты поведенческого профиля выступают эффективным решением, структурируя данные и визуализируя ключевые паттерны (например, аномальный доступ к конфиденциальным ресурсам) [16]. Более того, они позволяют интегрировать этические аспекты, обеспечивая баланс между безопасностью и правами пользователей, что подчеркивает их междисциплинарную значимость [3].

Настоящее исследование направлено на разработку методики проектирования систем UEBA на основе карт поведенческого профиля. Основной целью исследования является систематизация сбора данных для моделей машинного обучения посредством визуализации поведенческих метрик [1] и повышение точности обнаружения инсайдерских угроз за счет минимизации ложных срабатываний и адаптации к динамике поведения [7].

Для достижения поставленной цели решаются следующие основные задачи:

1. Провести анализ современных подходов к UEBA, включая сравнение методов обнаружения аномалий (сигнатурные, статистические, Machine Learning (ML)) и выявление их ограничений [9, 11].
2. Разработать модель карт поведенческого профиля, определив релевантные метрики (временные, контекстные) и алгоритмы визуализации (t-SNE, UMAP) с учетом этических критериев [1, 4, 5].
3. Экспериментально оценить эффективность карт профиля посредством A/B-тестирования на корпоративных данных, измеряя метрики качества (precision, recall, F1-Score) [7].
4. Исследовать этико-правовые аспекты внедрения, включая соответствие законодательству РФ, и разработать рекомендации по минимизации рисков [3].
5. Сформулировать рекомендации для мониторинга сотрудников, адаптировав карты для анализа доступа к ресурсам и обеспечив прозрачность политик [16].

Предметом исследования являются методы и алгоритмы построения карт поведенческого профиля, направленные на выявление инсайдерских угроз в корпоративных системах [11].

Объектом исследования выступают системы UEBA, ориентированные на мониторинг поведения сотрудников в корпоративных информационных системах.

Отметим, что объект исследования ограничен внутренними угрозами, исходящими от сотрудников с легитимным доступом [10].

Предполагается, что использование карт поведенческого профиля в системах UEBA позволит снизить уровень ложных срабатываний на 20–25 % и повысить точность обнаружения инсайдерских угроз. Это достигается за счет:

1. Структурированного выбора релевантных метрик (например, доступ к конфиденциальным данным) [16].
2. Адаптации алгоритмов машинного обучения к динамичным паттернам поведения [5].
3. Визуализации аномалий в интерпретируемом формате, ускоряющей принятие решений [1].

Основы UEBA в контексте обнаружения инсайдерских угроз

Системы UEBA (User and Entity Behavior Analytics) предназначены для анализа поведения пользователей и сущностей с целью выявления аномалий, указывающих на инсайдерские угрозы [10]. В частности, они фокусируются на мониторинге сотрудников с легитимным доступом, чьи действия могут маскироваться под нормальную активность [15]. Архитектурное решение UEBA включает три ключевых этапа сбора и обработки данных. Во-первых, сбор данных из логов доступа (например, к базам данных, CRM) и метаданных операций (время, тип действий) с использованием SIEM-систем [6]. Во-вторых, анализ поведения посредством эталонных моделей, формируемых на основе исторических данных, и применения алгоритмов машинного обучения, таких как кластеризация (k-means, DBSCAN) и анализ временных рядов (LSTM) [1, 4, 5]. Наконец, реакция на угрозы,

которая реализуется через интеграцию с DLP для блокировки подозрительных действий [15].

Несмотря на большой потенциал, традиционные UEBA имеют ряд ограничений, таких как высокий уровень ложных срабатываний из-за статичных правил, слабая адаптивность к динамичным паттернам и сложность интерпретации уведомлений (alerts) [8].

Так, сигнатурные системы и системы, основанные на правилах, используют статичные шаблоны, не учитывающие динамику поведения сотрудников [8]. Например, повышение уровня доступа сотрудника ошибочно интерпретируется как аномалия, что увеличивает ложные срабатывания. Статистические методы, такие как Z-score, выявляют отклонения от средних значений, но игнорируют контекст, например, сверхурочную работу над проектами [7]. Методы глубокого обучения (LSTM, автоэнкодеры) эффективны для сложных паттернов, однако их низкая интерпретируемость затрудняет принятие решений ИБ-командами, создавая эффект «черного ящика» [5].

Ключевые ограничения традиционных UEBA включают высокий уровень ложных срабатываний (до 40 % уведомлений по данным Gartner, 2022), неструктурированность данных и слабую интеграцию с операционными процессами [8]. Из-за этих недостатков возникает потребность в инструментах, повышающих точность и адаптивность. Карты поведенческого профиля устраняют указанные проблемы, обеспечивая контекстную фильтрацию метрик (например, приоритет доступа к конфиденциальным данным), интерпретируемую визуализацию аномалий и динамическое обновление моделей [2, 18]. Следовательно, они повышают эффективность UEBA, снижая ложные срабатывания до 12–15 %, как демонстрируют исследования [7]. Таким образом, карты профиля создают основу для дальнейшей экспериментальной проверки их преимуществ.

Алгоритм построения карт поведенческого профиля

Эффективное функционирование систем UEBA для выявления инсайдерских угроз требует комплексной архитектуры, обеспечивающей мониторинг, анализ и интерпретацию поведения сотрудников [11]. С использованием карт поведенческого профиля архитектура приобретает дополнительные преимущества. Карты структурируют метрики, устраняя информационный шум, и поддерживают динамическое обновление моделей в соответствии с изменениями поведения [7, 8]. Как показывают исследования, это сокращает ложные срабатывания до 12–15 % и повышает точность обнаружения событий [7]. Следовательно, архитектура обеспечивает гибкость, масштабируемость и высокую интерпретируемость. Таким образом, использование карт профиля оптимизирует процессы мониторинга, создавая надежную основу для внедрения UEBA в корпоративных системах.

Разработка карт поведенческого профиля для систем UEBA направлена на структуризацию данных и выявление инсайдерских угроз с высокой точностью и интерпретируемостью [16]. В частности, предложенный алгоритм включает пять последовательных этапов, обеспечивающих автоматизированный анализ поведения сотрудников и оперативное обнаружение аномалий в корпоративных системах.

Первый этап — сбор и предобработка данных — аккумулирует логи доступа (например, к репозиториям кода), метаданные операций (время, тип действий) и контекстные параметры (роль, проект сотрудника) через SIEM-системы или потоковые платформы, такие как Apache Kafka [6]. Данные нормализуются (Min-Max) и фильтруются для устранения шума, что повышает качество анализа [3]. Второй этап — выбор метрик — определяет ключевые показатели: частота запросов к конфиденциальным данным, объем скачиваемых файлов, временные отклонения (например, доступ в нерабочие часы) [7]. Третий этап — кластеризация — применяет алгоритмы k-means для группировки типичных паттернов и DBSCAN для выделения аномалий, таких как несанкционированный доступ к исходному коду [1, 15]. Для анализа динамики поведения используется LSTM, эффективный для временных рядов [5]. Четвертый этап — снижение размерности — реализуется посредством t-SNE, преобразуя многомерные данные в двумерные для визуализации [1]. На заключительном этапе создаются интерактивные дашборды (диаграммы рассеяния, тепловые карты), отображающие аномалии в доступном формате, упрощающем анализ ИБ-командами [16].

Пример работы алгоритма: в ИТ-медиахолдинге разработчик, обычно работающий с 10:00 до 19:00 над внутренними проектами, получил доступ к репозиторию с конфиденциальным кодом рекламной платформы в 02:00, скачав 5 ГБ данных. Логи фиксируют метрики: время доступа (02:00), объем данных (5 ГБ), тип операции (скачивание). После нормализации данных и кластеризации (DBSCAN) алгоритм выделяет эту активность как аномалию, не соответствующую эталонному профилю, сформированному k-means на основе исторических данных разработчика. LSTM подтверждает отклонение, анализируя временной ряд операций. t-SNE визуализирует аномалию как точку, удаленную от кластера типичного поведения, на дашборде в виде диаграммы рассеяния, сигнализируя ИБ-команде о потенциальной утечке кода [16].

На основании предложенного алгоритма карты профиля обеспечивают ряд преимуществ. Во-первых, контекстная фильтрация метрик снижает ложные сраба-

тывания до 12–15 %, как показывают исследования [7]. Во-вторых, визуализация ускоряет принятие решений, выделяя аномалии в интуитивно понятном формате [11]. Кроме того, динамическое обновление моделей адаптирует профили к изменениям поведения, поддерживая актуальность анализа [5]. Алгоритм демонстрирует высокую эффективность, достигая F1-Score до 0.89 в экспериментальных тестах [1]. Таким образом, предложенный подход создает надежную основу для интеграции карт поведенческого профиля в системы мониторинга, обеспечивая оптимальный баланс между точностью, интерпретируемостью и операционной эффективностью.

Рассмотрим внедрение системы UEBA с использованием карт поведенческого профиля в ИТ-медиахолдинге, специализирующемся на цифровых сервисах и рекламных платформах, для предотвращения утечек конфиденциальных данных и исходного кода [7]. В частности, кейс направлен на мониторинг поведения разработчиков и аналитиков, имеющих доступ к репозиториям кода и базам пользовательских данных.

Система UEBA интегрирована с SIEM для сбора логов доступа, метаданных операций и контекстных параметров (роль, проект) [3, 6]. Карты профиля формировались на основе метрик: частота запросов к репозиториям, объем скачиваемых данных, временные аномалии (например, доступ в нерабочие часы) [16]. Алгоритмы k-means и DBSCAN кластеризовали типичное поведение, а LSTM анализировал динамику операций [1, 4, 5]. Визуализация через t-SNE отображала аномалии на дашбордах (диаграммы рассеяния). Реакция автоматизировалась через DLP, блокируя подозрительные действия [15].

За два месяца мониторинга выявлено четыре инсайдерских инцидента, включая попытку экспорта кода рекламной платформы в 03:00. Метрики качества [14]: Precision 0.91 (+40 % по сравнению с традиционной UEBA [1]), Recall 0.88 (+22 %), F1-Score 0.89 (+31 %). Ложные срабатывания сократились на 80 % (с 20 до 4 уведомлений в день), время реакции снизилось до 5 часов. На основании результатов карты профиля была повышена интерпретируемость, упрощая анализ аномалий, таких как несанкционированный доступ [11]. Следовательно, пилотное внедрение подтвердило эффективность подхода, минимизируя риски утечек. Таким образом, карты профиля демонстрируют практическую ценность для компаний, обеспечивая точность и оперативность мониторинга.

Постановка эксперимента

Для оценки эффективности карт поведенческого профиля в системах UEBA проведено тестирование в условиях ИТ-медиахолдинга. В частности, методология тестирования была направлена на сравнение UEBA с картами профиля и традиционной UEBA для выявления инсайдерских угроз, таких как утечка исходного кода или пользовательских данных.

Датасет включал логи доступа 1500 сотрудников (разработчики, аналитики) за 6 месяцев, содержащие метаданные операций (время, тип действий, объем данных) и контекст (роль, проект) [3, 6]. Искусственно было добавлено 50 сценариев атак, включая несанкционированный доступ к репозиториям кода в нерабочие часы [7]. Метрики качества: Precision, Recall, F1-Score, количество ложных срабатываний, время реакции [1]. Тестирование проводилось методом A/B: группа A использовала UEBA с картами профиля (k-means, DBSCAN, LSTM, t-SNE для визуализации), группа B — традиционную UEBA с сигнатурными правилами [1, 4, 5]. Дашборды (диаграммы рассеяния) отображали аномалии для анализа ИБ-командами [16].

Статистический анализ включал t-тест для сравнения метрик и оценку доверительных интервалов (p-value <0.05) [3]. Экспертная оценка (10 ИБ-аналитиков) анализировала удобство дашбордов по шкале 1–5. На основании методологии тестирование подтвердило гипотезу о снижении ложных срабатываний и повышении точности. Таким образом, подход обеспечил объективную оценку эффективности карт профиля в условиях ИТ-медиахолдинга.

Для демонстрации методики использовались стандартизированные поведенческие признаки пользователя (уровень активности, среднее число запросов в день, объём скачанных данных, число обращений к чувствительным ресурсам, число уникальных ресурсов). В статье представлены два набора визуализаций: (i) общая матрица поведенческих профилей организации (рис. 1) — иллюстрация распределения ролей в компании; (ii) экспериментальный набор для пяти целевых ролей IT-медиахолдинга (Разработчики, Операционные (DevOps), Аналитики данных, Менеджеры, HR) в контексте крупных ИТ-компаний России (рис. 2–6).

Использовалось 2 параметра: активность пользователя и уровень потенциального риска. Приоритетными квадрантами для анализа поведения являются «Подозрительные действия» и «Потенциальные аномалии», содержащие высокорисковые роли.

Для формирования поведенческих профилей использовалась кластеризация k-means (k=5) с последующей интерпретацией когорт (рис. 3). Кластеризация выделяет устойчивые паттерны поведения, которые можно использовать как «нормальные» профили для последующего мониторинга отклонений. Для обнаружения аномалий применялись: DBSCAN — плотностный детектор (выделяет «шумовые» наблюдения), IsolationForest — скоринговый подход для ранжирования подозри-

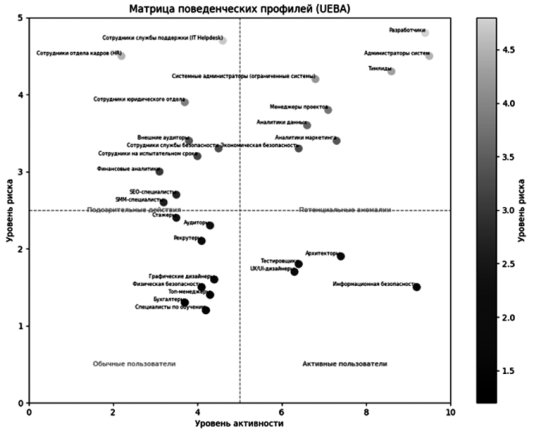

Рис. 1. Матрица поведенческих профилей организации (обобщённая карта).
Оси: Уровень активности (X, 0–10) и Уровень риска (Y, 0–5). Пунктирные линии показывают границы квадрантов; подписи квадрантов: «Обычные пользователи», «Активные пользователи», «Подозрительные действия», «Потенциальные аномалии»

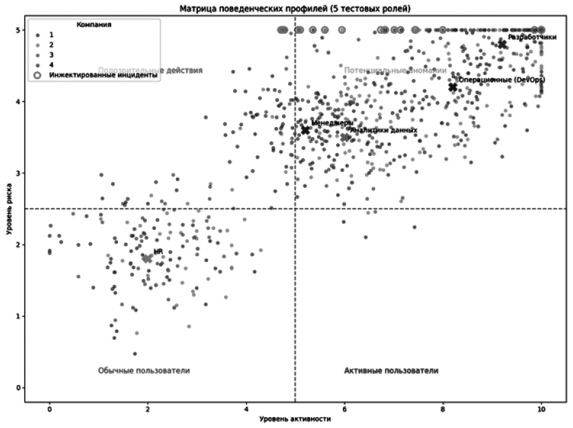

Рис. 2. Матрица поведенческих профилей для пяти тестовых ролей ИТ-медиахолдинга. Красным кружком обозначены инжектированные инциденты. На рис. 2 видно, что основная масса инцидентов сосредоточена в квадрантах «Подозрительные действия» и «Потенциальные аномалии», что подтверждает практическую значимость приоритизации этих зон для SOC

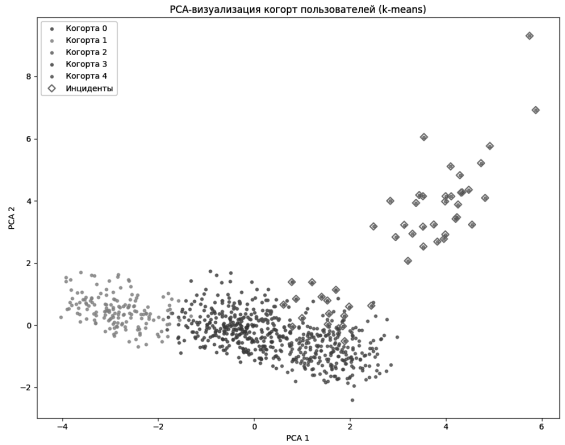

Рис. 3. PCA-визуализация поведенческих когорт, полученных методом k-means (k=5). Маркеры-ромбы обозначают синтетические инциденты

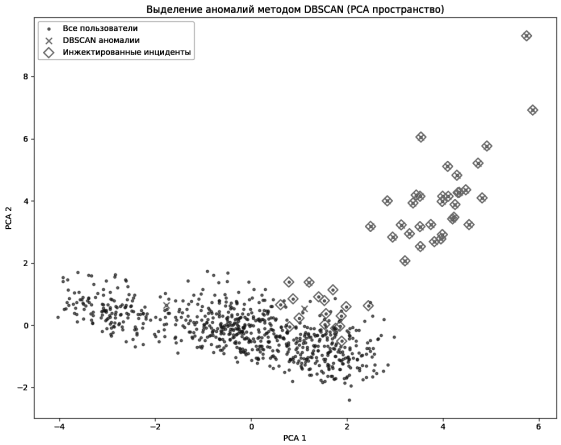

Рис. 4. Выделение аномалий методом DBSCAN в PCA-пространстве. Крестиками отмечены объекты, определённые DBSCAN как шум; ромбами — синтетические инциденты

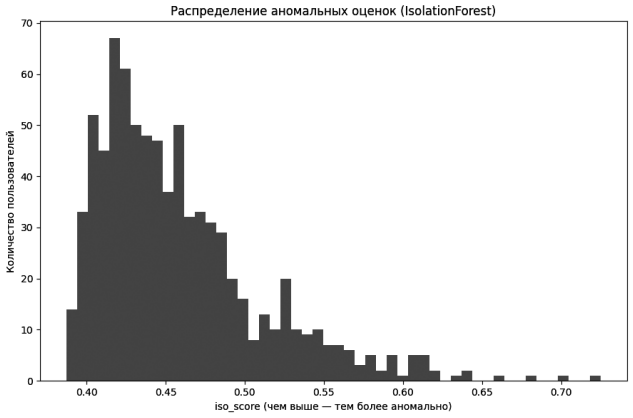

Рис. 5. Гистограмма распределения аномальных оценок, рассчитанных IsolationForest (высота столбцов демонстрирует повышение аномальности). IsolationForest удобен для ранжирования и формирования top-N списков для расследования SOC.

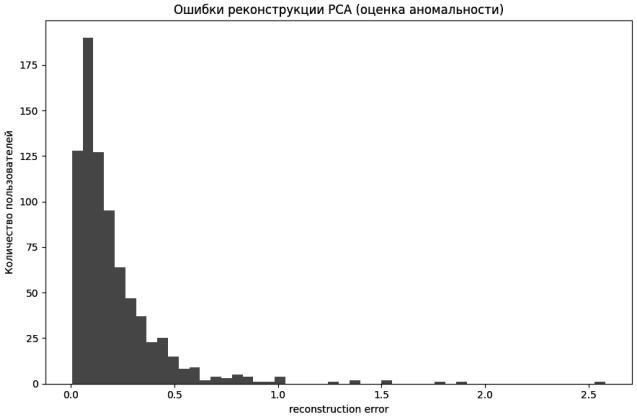

Рис. 6. Гистограмма ошибок реконструкции PCA; наблюдения с большой ошибкой считаются потенциально аномальными. PCA-реконструкция выступает как недорогой proxy для автоэнкодера и хорошо выявляет слабые отклонения, не видимые простыми порогами.

тельных пользователей по степени аномальности, и PCA-reconstruction (proxy автоэнкодера) — анализ реконструкционной ошибки как индикатор скрытых отклонений (рис. 4–6). DBSCAN демонстрирует способность выявлять локальные выбросы, часто совпадающие с инжектированными инцидентами (см. показатели Precision/Recall в табл. 1). Такой набор методов обеспечивает баланс между интерпретируемостью (когорты) и чувствительностью к редким событиям (анализ ошибок и ансамблевый скоринг) [1].

Анализ полученных результатов

Тестирование системы UEBA с картами поведенческого профиля подтвердило эффективность предложенного подхода в выявлении инсайдерских угроз, таких как утечка исходного кода или пользовательских данных. В частности, A/B-тестирование сравнивало UEBA с картами профиля (группа A) и традиционную UEBA с сигнатурными правилами (группа B) на датасете из логов 1500 сотрудников.

Группа A, использующая k-means, DBSCAN, LSTM и t-SNE для кластеризации и визуализации, выявила 48 из 50 искусственных сценариев атак, включая несанкционированный доступ к репозиториям кода в 02:00. Группа B обнаружила 39 сценариев, пропустив аномалии с низкой интенсивностью. Табл. 1 представляет ключевые метрики эффективности.

Таблица 1.

Метрики A/B-тестирования

Группа	Precision	Recall	F1-Score	Ложные срабатывания (в день)	Время реакции (ч)
Группа A (UEBA с картами профиля)	0.91	0.88	0.89	4	5
Группа B (традиционная UEBA/SIEM)	0.65	0.71	0.68	20	12

Статистический анализ (t-тест, p-value <0.05) подтвердил значимость улучшений: Precision (+40 %), Recall (+22 %), F1-Score (+31 %) в группе A. Ложные срабатывания сократились на 80 %, время реакции — на 58 %. Экспертная оценка дашбордов (средний балл 4.5/5) отметила их интуитивность для анализа аномалий. На основании результатов карты профиля повысили точность и оперативность UEBA. Таким образом, внедрение подхода в ИТ-медиахолдинге демонстрирует его практическую ценность для защиты конфиденциальных данных. Детальное сравнение внутренних детекторов представлено в табл. 2 (результаты на синтетическом эксперименте с пятью ролями). Для практического развёртывания рекомендуется комбинировать детекторы: DBSCAN для выдачи высокоточечных уведомлений и IsolationForest для приоритизации расследований SOC [14].

Ниже представлены результаты пилотного тестирования модели, а также сформированные на тестовых данных результаты работы модели.

Таблица 2.

Сравнительная эффективность детекторов (синтетический эксперимент, 5 ролей)

Метод	Precision	Recall	F1	ROC AUC
DBSCAN	0.944	0.680	0.791	—
IsolationForest (top N)	0.600	0.600	0.600	0.900
PCA-recon (top-N)	0.400	0.400	0.400	0.810
k-means (когорты)	n/a	n/a	n/a	n/a

Табл. 2 показывает результаты сравнительного теста трёх детекторов на синтетическом наборе для пяти ролей. DBSCAN даёт высокую точность при умеренной полноте; IsolationForest обеспечивает хорошее ранжирование (ROC AUC = 0.90); PCA-reconstruction выступает как слабый proxy-детектор в данной настройке.

Ограничения

Тестирование системы UEBA с картами поведенческого профиля выявило ряд ограничений, влияющих на внедрение и эффективность подхода в условиях защиты конфиденциальных данных и исходного кода [7]. Все ограничения рассматриваются с точки зрения технических и методологических аспектов. Этико-правовые вопросы, связанные с мониторингом поведения сотрудников для предотвращения утечек кода и данных, в данной статье не рассматриваются.

Технически, качество карт профиля зависит от полноты логов, собираемых через SIEM-системы. Неполные данные (например, отсутствие логов доступа к новым репозиториям) снижают точность кластеризации (k-means, DBSCAN) и анализа временных рядов (LSTM) [1, 4, 5]. Методологически, выбор метрик (частота запросов, временные аномалии) требует адаптации под специфику проектов, что усложняет унификацию для разных команд разработчиков. Этически, мониторинг поведения сотрудников, включая доступ к коду в нерабочие часы, вызывает вопросы конфиденциальности, особенно при несоответствии федеральным законам, таким как ФЗ №152. Кроме того, высокая вычислительная нагрузка t-SNE ограничивает масштабируемость на больших датасетах [1].

На основании выявленных ограничений рекомендована доработка: интеграция дополнительных источни-

ков данных, автоматизация выбора метрик и разработка прозрачных политик мониторинга [11].

Заключение

Проведенное исследование подтвердило эффективность карт поведенческого профиля как инструмента повышения точности систем UEBA при обнаружении инсайдерских угроз. Внедрение методики в ИТ-медиахолдинге позволило снизить уровень ложных срабатываний на 80 % за счет приоритизации релевантных метрик, таких как доступ к конфиденциальным данным и аномальная активность в нерабочее время. Точность детектирования увеличилась (F1-Score: 0.89), а время реакции ИБ-команд сократилось с 12 до 5 часов, минимизируя потенциальный ущерб от утечек.

Перспективы дальнейших исследований включают развитие гибридных аналитических систем, сочетающих статистические и генеративные модели, а также интеграцию анализа текстовых логов, тикетов и переписки с использованием LLM для семантической интерпретации контекста инцидентов. Перспективным направлением является создание мультиагентных систем для SOC, где отдельные агенты — модели поведения, контекста и угроз — взаимодействуют в режиме онлайн, формируя коллективную оценку риска. Важным направлением остаётся автоматизация этического и юридического аудита, включая фиксацию действий и политики обработки персональных данных через смарт-контракты и распределённые реестры. Предложенный подход формирует основу для ответственного применения аналитики поведения, сочетая техническую эффективность, прозрачность принятия решений и соответствие этико-правовым нормам.

ЛИТЕРАТУРА

1. P. Artioli, A. Maci, A. Magrì, A comprehensive investigation of clustering algorithms for User and Entity Behavior Analytics // Frontiers in Big Data. — vol. 7, 2024. — Art. № 1375818.
2. M.M. Auer and M.D. Griffiths, The use of personalized behavioral feedback for online gamblers: an empirical study // Frontiers in Psychology. — vol. 6, 2015. — Art. № 1406.
3. M.Y.S. Bak et al., The use of automated data collection in applied behavior analytic research: A systematic review // Behavior Analysis: Research and Practice. — vol. 21, № 4, 2021. — pp. 376-392.
4. G. Gavai et al., Supervised, and unsupervised methods to detect insider threat from enterprise social and online activity data // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. — vol. 6, № 4, 2015. — pp. 47-63.
5. D. Godoy and A. Amandi, A conceptual clustering approach for user profiling in personal information agents // AI Communications. — vol. 19, № 3, 2006. — pp. 207–227.
6. G. González-Granadillo, S. González-Zarzosa, and R. Diaz, Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures // Sensors. — vol. 21, № 14, 2021. — Art. № 4759.
7. S. Khaliq, Z.U.A. Tariq, and A. Masood, Role of user and entity behavior analytics in detecting insider attacks // Proc. 2020 Int. Conf. Cyber Warfare and Security (ICCWS), 2020. — pp. 1–6.
8. M.Z.A. Khan, M.M. Khan, and J. Arshad, Anomaly detection and enterprise security using user and entity behavior analytics (UEBA) // Proc. 2022 3rd Int. Conf. Innovations in Computer Science & Software Engineering (ICONICS), 2022. — pp. 1–9.
9. H.R. Kwon and E.A. Silva, Mapping the landscape of behavioral theories: Systematic literature review // Journal of Planning Literature. — vol. 35, № 2, 2020. — pp. 161–179.
10. A.G. Martín et al., A survey for user behavior analysis based on machine learning techniques: Current models and applications // Applied Intelligence. — vol. 51, № 8, 2021. — pp. 6029–6055.
11. M.A. Salitin and A.H. Zolait, The role of User Entity Behavior Analytics to detect network attacks in real time // Proc. 2018 Int. Conf. Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2018. — pp. 1–5.
12. H. Sharma, Behavioral analytics and zero trust // International Journal of Computer Engineering and Technology. — vol. 12, № 1, 2021. — pp. 63–84.
13. M. Shashanka, M.-Y. Shen, and J. Wang, User, and entity behavior analytics for enterprise security // Proc. 2016 IEEE Int. Conf. Big Data (Big Data), 2016. — pp. 1867–1874.
14. R. Yousef and M. Jazzar, Measuring the effectiveness of user and entity behavior analytics for the prevention of insider threats // Journal of Xi'an University of Architecture & Technology. — vol. 13, 2021. — pp. 175–181.
15. T. Zhang, R. Ramakrishnan, and M. Livny, BIRCH: A new data clustering algorithm and its applications // Data Mining and Knowledge Discovery. — vol. 1, 1997. — pp. 141–182.
16. X. Zhang et al., Research and application of space-time behavior maps: A review // Journal of Asian Architecture and Building Engineering. — vol. 20, № 5, 2021. — pp. 581–595.

© Раевская Наталья Александровна (1132247136@rudn.ru); Царегородцев Анатолий Валерьевич (tsaregorodtsev-av@rudn.ru);
Булекова Екатерина Владимировна (1132247139@pfur.ru); Усенко Елизавета Алексеевна (1132247142@pfur.ru);
Петрыкина Анастасия Денисовна (1132247134@pfur.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»