Список использованных источников
1. Identity-Centric Cybersecurity Model. URL: https://identitymanagementinstitute.org/identity-centric-cybersecurity-model/ (дата обращения: 11.03.2026).

Поздняк Ирина Сергеевна, к.т.н., доцент, декан фак. кибербезопасности и управления, i.pozdnyak@psuti.ru.
Чифранов Георгий Николаевич, стар. препод. каф. информационной безопасности, chifranov.e@ya.ru.

УДК 004.056; 004.8

МНОГОФАКТОРНЫЙ НЕЙРОСЕТЕВОЙ АНАЛИЗ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМАХ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ

Е.А. Марченко, С.В. Жуков, В.А. Федосеев
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: DLP‑системы, обнаружение утечки данных, гибридные модели глубокого обучения, поведенческая аналитика.

Современные корпоративные информационные системы генерируют значительные объёмы разнородных данных о действиях пользователей, что усложняет своевременное выявление инсайдерских угроз и подготовительных сценариев утечки конфиденциальной информации. Традиционные подходы, основанные на правилах, и простые статистические методы не позволяют в полной мере учитывать разнообразие поведения конкретного пользователя, динамику его активности и контекст выполняемых операций. В результате возрастает потребность в интеллектуальных UEBA‑решениях, способных проводить именно персонализированный поведенческий анализ и оценивать риск не только на уровне событий, но и на уровне индивидуального профиля пользователя [1, 2].

Целью работы является разработка и экспериментальное обоснование многофакторного персонализированного подхода к поведенческому анализу пользователей на основе комбинации нейросетевых моделей в контексте DLP‑систем.

Для достижения цели предлагается двухуровневый подход, решающий две ключевые задачи:

1. Объективная оценка уровня риска поведения сотрудника.
2. Выявление степени отклонения поведения от индивидуального профиля сотрудника.

Для решения этих задач были сформированы наборы данных, состоящие из 47 признаков, агрегированных на уровне сессии

пользователей из трёх рабочих станций на основе файловой, сетевой и процессной активности. Наборы данных формировались на основе 24 синтетических сценариев реальных утечек с разметкой по уровням риска 0–6. Данные были разделены на обучающую выборку (1680 записей) и тестовую выборку (420 записей).

Для первой задачи применялась разработанная нами нейросетевая модель обучения с учителем, получившая название HADFM (Hybrid Attention Deep Factorization Machine). Она состоит из 4 компонентов:

1. Linear Component – линейная ветвь модели, учитывающая вклад отдельных признаков и моделирующая их линейное влияние на уровень риска.

2. Feature Factorization Component – факторизационный слой с латентными эмбеддингами признаков для моделирования взаимодействий признако.

3. Attention Component – механизм self-attention для моделирования контекстных зависимостей между поведенческими признаками и выявления значимых комбинаций признаков.

4. Deep Nonlinear Representation – многослойная нейросеть прямого распространения, выполняющая нелинейное преобразование признаков и моделирующая сложные зависимости между ними.

Финальная оценка риска по шкале от 0 до 6 формируется как взвешенная комбинация выходов всех компонентов через softmax-слой.

На тестовой части датасета HADFM достигла следующих метрик: Macro F1-score = 0,9952, Accuracy = 0,9971, Precision = 0,997. Модель эффективно категоризирует известные рискованные сценарии.

Для решения второй задачи – выявления степени отклонения поведения от индивидуального профиля сотрудника – использовалась модель Deep SVDD (Deep Support Vector Data Description) без учителя. Она обучается только на нормальных сценариях, строя гиперсферу типичного поведения в латентном пространстве. Степень отклонения поведения рассчитывается как нормированное евклидово расстояние до центра гиперсферы и выражается в процентах относительно максимального расстояния, наблюдаемого в обучающей выборке.

На тестовой части датасета модель Deep SVDD достигла высоких метрик: MSE = 0,000356, MAE = 0,0181 на нормальных данных и Recall = 0,9870 (98,7%) при обнаружении аномалий. Модель демонстрирует высокую чувствительность к отклонениям от индивидуальной нормы пользователя и минимальные ложные срабатывания за счёт персонализации.

Таким образом, предложенная архитектура объединяет многофакторную классификацию поведенческих сценариев и персонализированное обнаружение отклонений, что позволяет учитывать как комбинации признаков активности пользователя, так и индивидуальные особенности его поведения.

Проведённые эксперименты подтвердили высокую эффективность предложенного метода. Модель HADFM достигла значения Macro F1-score 0,9952 при классификации уровней риска, а модель Deep SVDD обеспечила Recall 98,7% при обнаружении аномалий. Совместное применение моделей обеспечивает точность выявления потенциально опасных действий пользователей на уровне 99,2%.

Полученные результаты подтверждают эффективность применения многофакторного анализа комбинаций поведенческих признаков в задачах выявления утечек данных и демонстрируют перспективность использования предложенного подхода при разработке интеллектуальных модулей UEBA и DLP-систем.

Список использованных источников

1.Owobu, W.O. Conceptual Framework for Deploying Data Loss Prevention and Cloud Access Controls in Multi-Layered Security Environments / W.O. Owobu, O.A. Abieba, P. Gbenle [et al] // International Journal of Multidisciplinary Research and Growth Evaluation. – 2022. – Vol. 3(1). – P. 850-860.

2.Савенков, П.А. Использование методов и алгоритмов анализа данных и машинного обучения в UEBA/DSS для поддержки принятия управленческих решений / П.А. Савенков, П.С. Трегубов // Моделирова-ние, оптимизация и информационные технологии. – 2020. – Т. 8(1). – С. 585-587.

3.Ruff, L. Deep One-Class Classification / L. Ruff, R.A. Vandermeulen, N. Gornitz [et al.] // Proceedings of the 35th International Conference on Machine Learning (ICML). – 2018. – P. 4393-4402.

Марченко Екатерина Александровна, студ. гр. 6133-010402D, ea_marchenko_dev@mail.ru.
Жуков Семён Викторович, старш. препод. каф. геоинформатики и информационной безопасности, svzhukov@ssau.ru.
Федосеев Виктор Андреевич, к.физ.-мат.наук, доцент, зав. каф. геоинформатики и информационной безопасности, fedoseev.va@ssau.ru.

УДК 004.056.5; 004.7

КВАНТОВО-ЗАЩИЩЁННЫЕ СЕТИ: ПЕРСПЕКТИВЫ РАЗВИТИЯ И ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ

А.А. Обласов, Д.В. Воропаев
ФГБОУ ВО «Комсомольский-на-Амуре государственный университет», г. Комсомольск-на-Амуре

Ключевые слова: квантово-защищённые сети, квантовые коммуникации, характеристики квантовых сетей.

Квантово-защищённые сети представляют сложную структуру, включающую несколько ключевых компонентов, каждый из которых играет важную роль в обеспечении надежной и безопасной передачи данных.