Инженерный вестник Дона, №1 (2026)
ivdon.ru/ru/magazine/archive/n1y2026/10690

Анализ методов обнаружения редкой аномальной активности пользователей информационных систем

О.И. Шелухин

Московский технический университет связи и информатики

Аннотация: Проведен аналитический обзор релевантных научных публикаций в области обнаружения аномальной активности пользователей при работе с информационными системами. Анализируются методы повышения эффективности противодействия инсайдерам в информационных системах с помощью построения адекватной модели аномального поведенческого профиля пользователей системы управления взаимоотношениями с клиентами. Обоснована целесообразность использовании методов машинного обучения и обработки больших данных для обнаружения инсайдеров в компьютерной сети.
Ключевые слова: информационные системы, информационная безопасность, инсайдер, аномальная активность, поведенческий профиль, кластерное соседство.

Введение

В условиях роста числа внутренних и внешних угроз информационной безопасности особое значение приобретает задача своевременного обнаружения аномальной активности пользователей при работе с информационными системами [1,2]. Под аномальной активностью понимается нетипичная активность, выходящая за пределы привычных временных, географических или функциональных паттернов, наблюдаемых ранее у конкретного пользователя. Анализ аномального поведения базируется на понятии поведенческого профиля пользователя. Система должна быть способна отличать профиль "нормальной" активности от отклоняющегося.

Одной из категорий редкого аномального поведения (аномальной активности) пользователей является инсайдерская угроза — *деятельность сотрудника, сознательно или неосознанно нарушающего внутренние политики безопасности, или на внешнюю атаку, имитирующую действия легитимного пользователя [3-5].*

Инсайдерские угрозы представляют собой одну из наиболее сложных задач в области обеспечения информационной безопасности организаций. Они исходят от лиц, обладающих законным доступом к критически важным данным, включая сотрудников, подрядчиков и иных уполномоченных пользователей. Основная сложность выявления таких угроз заключается в том, что инсайдеры хорошо осведомлены о внутренних процессах, что позволяет им незаметно совершать вредоносные действия.

Согласно классификации, представленной в [1] инсайдеров можно условно разделить на четыре категории:

- Невольные нарушители, совершающие ошибки по незнанию или неосторожности.
- Злонамеренные лица, преднамеренно наносящие ущерб организации.
- Сотрудники, испытывающие неудовлетворённость и проявляющие враждебность к работодателю.
- Внешние специалисты, получившие доступ к внутренним ресурсам.

Среди аномалий в поведении пользователей на рабочих станциях в части кибербезопасности можно выделить следующие:

- Подозрительная активность в нерабочее время - попытки входа, подключение к корпоративным ресурсам или запуск приложений в ночное время или в выходные дни;
- Множественные неудачные попытки входа — частые неудачные попытки входа в систему с одного IP-адреса или учетной записи;
- Попытки подключения к незнакомым или запрещенным ресурсам - обращения к ресурсам в интернете, облачным хранилищам или зарубежным сайтам, не связанным с рабочими задачами;
- Необычно большой исходящий или входящий трафик, множественные подключения к внешним ресурсам;

- Активность пользователя на нестандартных портах - попытки входа, подключение к корпоративным ресурсам или запуск приложений в ночное время или выходные дни;
- Нетипичный характер удаленного доступа сотрудника, source ip, географическое расположение, нетиповое устройство доступа;
- Нетипичные для пользователя действия — выполнение действий, не характерных для профиля пользователя;
- Подозрительные действия с файлами — создание, удаление или изменение большого количества файлов, особенно в нетипичных для пользователя директориях;
- Попытки обхода средств защиты — действия, направленные на отключение антивируса, host-based firewall, EDR или других средств безопасности;
- Действия под учетной записью с редкой активностью.

Для обеспечения высококачественной работы с клиентской базой, оптимизации бизнес-процессов и повышение качества принимаемых управленческих решений, активно внедряются системы управления взаимоотношениями с клиентами (Customer Relationship Management, CRM). Основная задача CRM-систем заключается в консолидации информации о клиентах, автоматизации взаимодействия с ними, а также в анализе истории взаимодействия с клиентом для последующей персонализации предлагаемых услуг и увеличения уровня удовлетворённости. В силу своей функциональной ценности и насыщенности чувствительной информацией CRM-системы представляют собой приоритетную цель для злоумышленников. Наличие доступа к CRM позволяет получить сведения о клиентах, что может быть использовано в мошеннических схемах, конкурентной разведке, фишинговых атаках или шантаже. Внешние угрозы по отношению к CRM-системе охватывают широкий спектр техник: от

подбора или компрометации учётных данных через фишинг и вредоносное ПО до эксплуатации уязвимостей веб-интерфейса, сетевых сервисов или слабых конфигураций доступа.

Для внешнего нарушителя успешная атака на CRM-систему требует значительных ресурсов и высокой квалификации, а также зачастую сопряжена с преодолением многоуровневой защиты и высокой вероятностью обнаружения.

Иная ситуация наблюдается в контексте внутренних угроз, под которыми понимаются действия штатных сотрудников или подрядчиков, обладающих санкционированным доступом к информационным системам организации. В отличие от внешнего нарушителя, инсайдер обладает не только техническим доступом к CRM-системе, но и контекстным пониманием бизнес-процессов, корпоративной структуры и слабых мест в организации процедур безопасности. Его действия, как правило, не вызывают подозрения, так как осуществляются в рамках выданных прав и соответствуют привычной нагрузке. Кроме того, инсайдер может использовать социальную инженерию, недокументированные возможности или слабости административного контроля. Всё это делает инсайдерскую активность особенно сложной для своевременного выявления и нейтрализации. Наличие априорного преимущества в виде легитимного доступа ставит перед специалистами по информационной безопасности задачу перехода от периметральной модели защиты к модели мониторинга поведения и выявления нетипичных, но формально допустимых действий пользователей.

Как известно, периметральные системы охраны (ПСО) являются наиболее эффективными средствами защиты от несанкционированного проникновения и прекрасно подходят для организации современной системы охраны. Нарушитель, воздействуя на пространство или предметы, составляющие часть

периметра, формирует возмущения, которые и можно зарегистрировать специальными датчиками.

Целью работы является анализ методов построения адекватной модели поведенческого профиля аномальной активности пользователей при работе с информационными системами, на основе которой можно оценить, насколько текущая активность пользователя отличается от ожидаемой.

Современные методы выявления инсайдерских угроз

Одним из ключевых достоинств машинного обучения является умение выявлять аномалии в поведении, не имеющие явно выраженных признаков нарушения, но отличающиеся от типичных моделей активности статистически значимым образом [6].

Работа [7] посвящена противодействию неумышленному инсайдингу, ведущему к нарушениям информационной безопасности в организациях. В качестве уязвимости организации рассматривается «неустойчивость» регламентов деятельности сотрудников (инструкций), а в качестве источника угрозы безопасности информационных ресурсов – девиация поведения сотрудников, вследствие чего происходит отклонение от шагов инструкции.

В [8] предложена модель комбинирования различных способов выявления инсайдеров. Предложено экспертное и теоретическое комбинирование пар способов, позволившее получить оценки успешности подобного комбинирования.

В условиях ограничений существующих подходов к решению задачи выявления аномального поведения пользователей особую значимость приобрели методы искусственного интеллекта, в частности алгоритмы машинного обучения. Подобные методы способны адаптироваться к многообразию поведения пользователей и выявлять скрытые закономерности без необходимости ручного задания правил. Применение интеллектуальных

методов в рамках развитие концепции анализа поведения пользователей позволило перейти от жёстко заданных шаблонов к вероятностному описанию активности субъектов, опирающемуся на данные о структуре и временной динамике их действий [9].

В [10] для построения моделей нормального поведения пользователей, акцент сделан на применение рекуррентных нейросетей, в частности, архитектуры LSTM (Long Short-Term Memory). Одним из примеров является фреймворк LADOHD (LSTM-based Anomaly Detector Over High-dimensional Data) — фреймворк для обнаружения аномалий на основе LSTM). Предназначен для анализа отклонений временных зависимостей высокоразмерных последовательных данных, например, событий в компьютерных системах. Учитывая, как краткосрочные, так и долгосрочные связи между действиями, данная модель позволяет эффективно обнаруживать признаки продолжительных атак. Подход с использованием LSTM-Autoencoder позволяет анализировать пользовательские сессии, начиная от момента входа в систему до выхода, что обеспечивает целостный контекст. Модель обучается на нормальных данных без аномалий, оптимизируя метрику ошибки реконструкции, что способствует выявлению нетипичных действий при минимальном уровне ложных срабатываний (примерно 9%).

Современные методы обнаружения инсайдерских угроз всё чаще основываются на объединении различных подходов. Так, в работе [9] описан гибридный метод, сочетающий машинное и глубокое обучение. Он использует уровень слияния (Fusion Layer) для интеграции результатов различных моделей и механизм адаптации к новым данным, что снижает количество ложных тревог и увеличивает до 98,5% точность идентификации пользователей.

Модель SPCAGAN (Sparse Principal Component Analysis Generative Adversarial Networks), представленная в [11], представляет собой модифицированную генеративно-состязательную нейронную сеть, способную генерировать синтетические данные для решения проблемы дисбаланса. Интеграция обучения многообразий и специальной функции потерь позволяет повысить устойчивость модели и точность классификации аномалий. Метод CATE (Convolutional Attention and Transformer Encoder) [12] совмещает статистические и последовательные методы анализа действий пользователей внутри организации. Это позволяет учесть как особенности распределения данных, так и временные зависимости, обеспечивая более глубокое понимание поведения сотрудников и своевременное выявление угроз. Подход, описанный в [13], объединяет поведенческий анализ на уровне сети и конечных устройств. Используемые в работе модели глубоких нейронных сетей в виде автокодировщиков (AE, Autoencoder) и вариационных автокодировщиков (VAE, Variational Autoencoder) обеспечивают обнаружение отклонений сетевых и хостовых данных с высокой точностью, особенно при комбинированной обработке.

В [14] обсуждается разработка модельно-методического аппарата для обнаружения инсайдеров в сети на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных. Эффективность таких решений подтверждается низким уровнем ложных срабатываний и высокой чувствительностью к нестандартным действиям. Тем не менее, для обеспечения устойчивости моделей в условиях постоянно изменяющихся угроз необходима их регулярная адаптация и дополнение актуальными данными.

В [15] анализируется построение адекватной модели поведенческого профиля, на основе которой оценивается, на сколько текущая активность пользователя отличается от ожидаемой. Для уточнения характера поведения

применяется многомерный анализ кластерного окружения, основанный на комбинациях признаков и разной плотности кластеризации. Полученные кластерные соседства сравниваются с эталонными множествами как нормальных, так и аномальных образцов, которые включены в эталонную матрицу, используемую для построения кластерных соседств.

Вышеизложенное обуславливает целесообразность подхода для обнаружения инсайдеров в компьютерной сети, основанного на использовании методов машинного обучения и обработки больших данных, что позволяет с одной стороны учитывать множество, на первый взгляд, трудно связанных друг с другом параметров, а с другой стороны - автоматизировать этот процесс.

Выводы

Несмотря на вышеперечисленные очевидные преимущества применения машинного обучения в задачах поведенческого анализа, практика их внедрения в корпоративных системах демонстрирует ряд критически важных ограничений, напрямую связанных с качеством и полнотой обучающих выборок. В условиях дефицита размеченных данных, особенно характерного для внутреннего мониторинга, где инциденты имеют низкую частоту и разнообразие, применение даже проверенных моделей сопровождается высоким уровнем ложноположительных или ложноотрицательных срабатываний. Аппроксимация нормального поведения на ограниченном наборе наблюдений приводит к переобучению моделей на шум, или, напротив, к чрезмерному сглаживанию поведенческих паттернов, в результате чего система либо теряет чувствительность к аномалиям, либо генерирует избыточное количество тревожных сигналов.

В условиях высокой вариативности поведения и организационных изменений, характерных для современных CRM-систем, возникает необходимость регулярного переобучения моделей с учётом актуального

контекста. Поддержание релевантности таких моделей требует как вычислительных, так и экспертных ресурсов.

В условиях высокой неопределённости и ограниченности данных требуется создать переход к гибридным архитектурам, в которых интеллектуальные методы подкрепляются корректирующими механизмами, что позволит повысить устойчивость системы, обеспечить контролируемость вывода и упростить эксплуатацию аналитических решений.

Публикация выполнена в рамках гранта на реализацию отраслевой научно-педагогической школы МТУСИ "Современные технологии исследования аномалий в информационной безопасности" по проекту "Обнаружение и прогнозирование редких аномальных событий для обеспечения информационной безопасности" (Пр. 93-х от 25.04.2025).

Литература

1. Rida N., Mehreen A., Rabita L.F., et al. Behavioral Based Insider Threat Detection Using Deep Learning // IEEE Access. 2021. pp. 143266 - 143274.

2. Villarreal-Vasquez M., Modelo-Howard G., Dubee tS., al. Hunting for Insider Threats Using LSTM-Based Anomaly Detection // IEEE TDSC. 2023. VOL. 20, NO. 1. pp. 451-462.

3. Bertrand S., Desharnais J., Tawbi N. Unsupervised User-Based Insider Threat Detection Using BGMM // 20th Annual International Conference on Privacy, Security and Trust (PST) 2023. pp.1-10.

4. Al-Shehari T.,Al-Razgan M.,Tana A., et al. Insider Threat Detection Using Isolation Forest // IEEE Access. Master’s thesis work carried out at Elastic Mobile Scandinavia AB and Lund University. 2023. pp.1-62.

5. Teng H., Weina N., Xiaosong Z., et al. Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning Security and Communication Networks. 2019. pp. 1-12.

6. Xiao H., Zhang W., Lu H. A Comprehensive Framework for Insider Threat Detection Based on Statistical and Sequential Analysis // J. Inf. Secur. Appl. 2023. Vol. 75. URL: researchgate.net/publication/376667112_Unveiling_shadows_A_comprehensive_framework_for_insider_threat_detection_based_on_statistical_and_sequential_analysis

7. Буйневич М. В., Власов Д. С. Комбинирование способов выявления инсайдеров больших информационных систем // Вопросы кибербезопасности. 2024, № 3(61). С. 2-13.

8. Буйневич М. В., Моисеенко Г. Ю. Повышение «устойчивости» регламентов деятельности как способ противодействия неумышленному инсайдингу// Вопросы кибербезопасности. 2024. № 6(64). С. 108-116.

9. Sridevi D., Kannagi L., Vivekanandan G. Detecting Insider Threats in Cybersecurity Using Machine Learning and Deep Learning Techniques / International Conference on Communication, Security and Artificial Intelligence (ICCSAI). 2023. Page(s): pp. 871 – 875.

10. Zewdie M., Girma A. T., Sitote M. Deep Neural Networks for Detecting Insider Threats and Social Engineering Attacks / International Conference on Electrical, Computer and Energy Technologies (ICECET). 2024. pp. 1 – 8.

11. Sridevi D. , Kannagi L., Vivekanandan G. Detecting Insider Threats in Cybersecurity Using Machine Learning and Deep Learning Techniques / International Conference on Communication, Security and Artificial Intelligence (ICCSAI). 2023, pp. 871 – 875.

12. Xiao H., Zhang W., Lu H. Unveiling Shadows: A Comprehensive Framework for Insider Threat Detection Based on Statistical and Sequential Analysis // J. Inf. Secur. Appl. 2023. Vol. 75.

13. Zewdie M., Yigezu S., Liménih A. Deep Neural Networks for Detecting Insider Threats and Social Engineering Attacks // ICECET. 2024, pp. 184–189.

14.Ушаков И.А. Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий обработки больших данных. // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 38-43.

14. Шелухин О.И., Осин А.В., Хализев К.А. Обнаружение аномальной активности пользователей информационной системы на основе анализа кластерных соседств. Материалы 34-й научно-технической всероссийской конференции «Методы и технические средства обеспечения безопасности информации»: СПб: Изд-во Политехнического университета, 2025. С. 11-14.

References

1. Rida N., Mehreen A., Rabita L.F et al. IEEE Access. 2021. pp. 143266 - 143274.

2. Villarreal-Vasquez M., Modelo-Howard G., Dube S., et al. IEEE TDSC. 2023. VOL. 20, NO. 1, pp. 451-462.

3. Bertrand S., Desharnais J., Tawbi N. 20th Annual International Conference on Privacy, Security and Trust (PST). 2023, pp. 1-10.

4. Al-Shehari T., Al-Razgan M., Tana A., et al. IEEE Access. Master's thesis work carried out at Elastic Mobile Scandinavia AB and Lund University.2023, pp.1-62.

5. Teng Hu., Weina Niu., Xiaosong Z., et al. Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning Security and Communication Networks. 2019, pp. 1-12.

6. Xiao H., Zhang W, Lu H. A. J. Inf. Secur. Appl. 2023. Vol. 75. URL: researchgate.net/publication/376667112_Unveiling_shadows_A_comprehensive_framework_for_insider_threat_detection_based_on_statistical_and_sequential_analysis

7. Bujnevich M.V., Vlasov D. S. Voprosy` kiberbezopasnosti. 2024. № 3 (61), pp. 2-13.

8. Bujnevich, M. V.Moiseenko, G. YU. Voprosy` kiberbezopasnosti. 2024. № 6(64), pp. 108-116.

9. Sridevi D., Kannagi L. Vivekanandan G. International Conference on Communication, Security and Artificial Intelligence (ICCSAI). 2023, pp. 871 – 875.

10. Zewdie M., Girma A., Sitote T.M. International Conference on Electrical, Computer and Energy Technologies (ICECET). 2024, pp.1 – 8.

11. Sridevi D., Kannagi L., Vivekanandan G. International Conference on Communication, Security and Artificial Intelligence (ICCSAI). 2023, pp.871 – 875.

12. Xiao H., Zhang W., Lu H. J. Inf. Secur. Appl. 2023. Vol. 75.

13. Zewdie M., Yigezu S., Liménih A. ICECET. 2024, pp. 184–189.

14. Ushakov I.A. Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta texnologii i dizajna. Seriya 1: Estestvenny`e i texnicheskie nauki. 2019. № 4. pp. 38-43.

15. Sheluhin O.I., Osin A.V., Xalizev K.A. Materialy` 34-j nauchno-texnicheskoj vserossijskoj konferencii «Metody` i texnicheskie sredstva obespecheniya bezopasnosti informacii»: SPb: Izd-vo Politexnicheskogo universiteta, 2025, pp.11-14.

Автор согласен на обработку и хранение персональных данных.

Дата поступления: 4.11.2025

Дата публикации: 27.12.2025