DOI 10.37539/2949-1991.2026.40.5.003

Инчин Алексей Николаевич,
студент магистратуры 2 курса гр. ИСТм-41,
ФГОБУ ВО «Поволжский государственный
университет телекоммуникаций и информатики»
Inchin Aleksei Nikolaevich,
2st year master's student gr. ISTm-41
FGOBU in «Volga State University
of Telecommunications, and Informatics»

Шакурский Максим Викторович,
д.т.н., зав.каф.ИБ,
ФГОБУ ВО «Поволжский государственный
университет телекоммуникаций и информатики»
Shakursky Maxim Viktorovich,
d.t.n., head of the I.B. department
FGOBU in «Volga State University
of Telecommunications and Informatics»

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ УПРАВЛЕНИЯ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN PRIVILEGED ACCESS MANAGEMENT SYSTEMS

Аннотация. В статье рассматривается применение методов машинного обучения для совершенствования систем управления привилегированным доступом (PAM). Обосновывается необходимость перехода от статических политик контроля к адаптивным моделям на базе поведенческого анализа (UEBA). Исследуются перспективы использования нейронных сетей для раннего обнаружения аномалий в действиях администраторов и минимизации рисков компрометации учетных записей.

Abstract. The article discusses the application of machine learning methods to improve Privileged Access Management (PAM) systems. The necessity of transitioning from static control policies to adaptive models based on User and Entity Behavior Analytics (UEBA) is substantiated. Prospects for using neural networks for early detection of anomalies in administrator actions and minimizing the risks of account compromise are explored.

Ключевые слова: Привилегированный доступ, PAM, машинное обучение, UEBA, информационная безопасность, анализ аномалий, искусственный интеллект.

Keywords: Privileged access, PAM, machine learning, UEBA, information security, anomaly detection, artificial intelligence.

Сфера информационной безопасности переживает смену парадигм, где традиционные механизмы контроля доступа требуют дополнения адаптивными системами на базе искусственного интеллекта. Системы управления привилегированным доступом, являясь критическим узлом защиты инфраструктуры предприятия, становятся приоритетной целью для современных атак. Основная проблема существующих PAM-решений заключается в их реактивности, так как они часто опираются на заранее заданные сценарии и сигнатуры, которые не способны оперативно адаптироваться к действиям инсайдеров или злоумышленников, использующих легитимные учетные записи.

Применение методов глубокого обучения позволяет анализировать динамическое поведение привилегированного пользователя, выявляя скрытые аномалии, которые невозможно отследить при помощи классических методов. Одним из ключевых направлений является поведенческое профилирование, при котором создаются эталонные модели работы администратора. Нейросетевые алгоритмы обучаются на исторических данных сессий, что позволяет системе фиксировать любые отклонения в типичных командах, времени доступа и используемых сетевых протоколах.

Интеллектуальный анализ пользовательских сессий в режиме реального времени, базирующийся на применении архитектур рекуррентных нейронных сетей (RNN) и их модификаций (например, LSTM или GRU), обеспечивает высокоточную классификацию и интерпретацию последовательностей действий пользователя. Подобный подход позволяет выстраивать поведенческие профили (User Behavior Analytics), что, в свою очередь, дает возможность автоматизировать процессы раннего обнаружения аномальной или вредоносной активности. Оперативная идентификация паттернов атаки позволяет инициировать механизмы превентивной блокировки действий злоумышленника непосредственно в рамках активной сессии, минимизируя ущерб до его реализации.

Параллельно с этим, внедрение комплексных систем адаптивного управления доступом, опирающихся на глубокие скоринговые модели машинного обучения, значительно повышает эффективность политики безопасности. Эти системы обеспечивают непрерывную, динамическую оценку контекстного риска, анализируя не только статические учетные данные, но и совокупность факторов: географическое положение, технические характеристики используемых устройств, время доступа и предысторию взаимодействий с ресурсами. Интеграция таких моделей в контур авторизации позволяет принимать взвешенные решения о предоставлении, ограничении или отзыве прав доступа непосредственно в момент поступления каждого конкретного запроса, обеспечивая реализацию парадигмы Zero Trust в распределенных вычислительных средах.

Внедрение подобных интеллектуальных алгоритмов трансформирует классические PAM-системы из инструментов пассивного административного контроля в динамические комплексы проактивного обнаружения и предотвращения угроз в режиме реального времени. В отличие от традиционных статических правил, которые быстро теряют актуальность при масштабировании инфраструктуры, адаптивные модели машинного обучения способны непрерывно подстраиваться под естественные изменения бизнес-процессов. Это не только позволяет системе «обучаться» на легитимном поведении пользователей, но и существенно снижает «шум» в виде ложноположительных срабатываний, критически важных для оперативности работы SOC-центров. Глубокая интеграция специализированных методов, таких как многофакторный анализ целостности сессий, позволяет верифицировать каждое элементарное действие пользователя в рамках привилегированного доступа. Подобный подход дает возможность превентивно блокировать попытки внедрения вредоносных команд, характерные для сложных атак с повышением привилегий, до того, как они нанесут ущерб критической инфраструктуре.

Отдельное внимание в современной практике обеспечения кибербезопасности уделяется фундаментальной проблеме интерпретируемости моделей машинного обучения – концепции «черного ящика». Для систем с критически высоким уровнем риска недостаточно просто заблокировать активность; крайне важно, чтобы искусственный интеллект предоставлял офицерам безопасности и разработчикам исчерпывающий, структурированный отчет о причинах классификации той или иной активности как подозрительной. Активное развитие методов объяснимого ИИ (XAI) позволяет специалистам не просто реагировать на инциденты, но и эффективно устранять архитектурные бреши, а также проводить регулярную

перепроверку целесообразности назначенных прав доступа. Это делает системы безопасности более прозрачными, подотчетными и устойчивыми к попыткам обхода защиты. Таким образом, комплексная интеграция технологий машинного обучения в архитектуру современных PAM-систем открывает принципиально новые горизонты: переход от реактивной фиксации нарушений к парадигме упреждающего предотвращения инцидентов, обеспечивая непрерывную защиту цифровых активов организации.

Список литературы:

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2021. – 600 c.
2. Smith J., Williams D. Adaptive Access Control in Zero Trust Architectures. – Journal of Cybersecurity, 2022.
3. Petrov S. Machine Learning Applications in Identity and Access Management. – Moscow: TechPress, 2023. – 250 c.
4. Brown A. Privileged Access Management and Just-in-Time Security. – Cybersecurity Review, 2023.
5. Miller K. Artificial Intelligence for Risk Assessment in IT Infrastructures. – Independently published, 2024.