DOI 10.37539/2949-1991.2026.40.5.002

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 АДАПТИВНЫХ МОДЕЛЕЙ ДЛЯ ОПТИМИЗАЦИИ УПРАВЛЕНИЯ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ В КОРПОРАТИВНЫХ СЕТЯХ
USING ADAPTIVE MODELS FOR OPTIMIZING PRIVILEGED ACCESS MANAGEMENT IN CORPORATE NETWORKS

Аннотация. В статье исследуется концепция адаптивного управления привилегированным доступом с применением интеллектуальных систем оценки рисков. Рассматриваются подходы к переходу от модели постоянных прав доступа к динамической модели «Just-in-Time». Анализируются возможности использования машинного обучения для автоматизации предоставления доступа на основе контекстуальных данных.

Abstract. The article explores the concept of adaptive privileged access management using intelligent risk assessment systems. Approaches to shifting from permanent access rights to a «Just-in-Time» dynamic model are examined. Possibilities of using machine learning to automate access provisioning based on contextual data are analyzed.

Ключевые слова: Привилегированный доступ, Just-in-Time, кибербезопасность, адаптивное управление, оценка рисков, машинное обучение.

Keywords: Privileged access, Just-in-Time, cybersecurity, adaptive management, risk assessment, machine learning.

В условиях глобальной цифровизации и усложнения корпоративных ИТ-ландшафтов традиционные парадигмы кибербезопасности утрачивают свою эффективность. Современные стратегии защиты всё чаще опираются на концепцию нулевого доверия (Zero Trust Architecture), фундаментальным принципом которой является отказ от презумпции доверия к любому субъекту внутри или вне периметра сети. В рамках данной стратегии управление привилегированным доступом (PAM) играет ключевую, системообразующую роль. Традиционные модели управления, базирующиеся на модели постоянных административных полномочий, создают значительные уязвимости: избыточные права доступа (Over-privileged accounts) расширяют поверхность атаки, упрощая злоумышленникам процесс эскалации привилегий и закрепления в системе. Для нейтрализации этих рисков требуется переход к

динамическим моделям доступа, которые делегируют право принятия решений автоматизированным системам, предоставляющим полномочия исключительно на временной основе (Just-in-Time Access) с учетом контекстной безопасности.

Интеллектуальные системы управления привилегиями, использующие методы глубокого машинного обучения (Deep Learning) и поведенческой аналитики (User and Entity Behavior Analytics – UEBA), трансформируют процесс предоставления доступа из статичного регламента в адаптивный процесс. Вместо подверженного ошибкам ручного распределения прав, система в непрерывном цикле анализирует широкий спектр телеметрии: от состояния защищенности устройства, включая наличие актуальных обновлений безопасности и патчей, до ретроспективного анализа поведенческих паттернов пользователя, его текущей геолокации, IP-адресов и даже времени суток, характерного для выполнения конкретных операций. Интеграция с системами управления критичностью активов позволяет алгоритмам в режиме реального времени формировать динамический «скоринг риска». В зависимости от полученного показателя система принимает решение: одобрить запрос автоматически, потребовать дополнительную верификацию через многофакторную аутентификацию (MFA), или заблокировать действие и инициировать сигнал тревоги для центра мониторинга безопасности (SOC).

Критически важным аспектом эволюции этих систем является радикальное снижение влияния человеческого фактора на безопасность инфраструктуры. За счет внедрения моделей машинного обучения, способных распознавать бизнес-контекст, PAM-системы получают возможность автономно принимать решения о временном повышении привилегий (Privilege Elevation) в строгом соответствии с утвержденными бизнес-процессами. Это не только существенно сокращает операционные издержки и нагрузку на ИТ-департаменты, но и позволяет на практике реализовать принцип «минимально необходимых привилегий». Автоматизация гарантирует, что администратор получает доступ к ресурсу ровно на тот период, который требуется для решения задачи (например, проведения технического обслуживания), после чего права автоматически отзываются, исключая возможность использования устаревших или «сиротских» учетных записей для атак.

Помимо превентивного контроля, применение интеллектуальных аналитических инструментов является мощным средством обнаружения вторжений, в частности – попыток горизонтального перемещения (Lateral Movement) внутри сети. Адаптивные системы способны выявлять тонкие аномалии в цепочках запросов доступа, которые выходят за рамки нормативного профиля поведения (Baseline) конкретного администратора. Например, нестандартный путь доступа к критической базе данных или нехарактерная последовательность запуска административных команд мгновенно классифицируются как подозрительная активность. В таких сценариях автоматизированные средства безопасности способны инициировать процедуру мгновенного отзыва всех активных токенов и завершения сессий, купируя угрозу до того, как будет нанесен реальный ущерб инфраструктуре или произойдет эксфильтрация конфиденциальных данных.

Таким образом, переход к адаптивному интеллектуальному управлению доступом становится обязательным требованием для обеспечения киберустойчивости в современных ИТ-средах. Автоматизация оценки рисков и динамическое предоставление привилегий позволяют достичь необходимого компромисса между гибкостью рабочих процессов и бескомпромиссным уровнем информационной безопасности. Дальнейшие исследования в этой области направлены на углубление интеграции интеллектуальных PAM-решений в гибридные облачные среды (Hybrid Cloud) и мультиоблачные архитектуры, где управление доступом становится все более сложным из-за размытия границ безопасности. Разработка таких систем станет фундаментом для создания автономно защищающихся корпоративных сетей, способных эффективно противостоять угрозам нового поколения.

Список литературы:

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2021. – 600 с.
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 с.
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.