УДК 004.056.5

М.С. ЮРИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СИСТЕМАХ УПРАВЛЕНИЯ ИДЕНТИФИКАЦИЕЙ: НОВЫЕ ГОРИЗОНТЫ БЕЗОПАСНОСТИ

В условиях растущей киберугрозы системы управления идентификацией (IDM) нуждаются в улучшении безопасности и эффективности. Данная статья рассматривает возможности применения искусственного интеллекта (ИИ) для решения этих задач. В работе анализируются ключевые применения ИИ в IDM, такие как улучшенная аутентификация, авторизация, предотвращение несанкционированного доступа, а также оптимизация процессов управления идентификацией. В статье также рассматриваются вызовы и перспективы развития ИИ в IDM.

Введение

В условиях растущих киберугроз, традиционные системы управления идентификацией (IDM) сталкиваются с трудностями в обеспечении надежной защиты данных. Искусственный интеллект (ИИ) предлагает решение этой проблемы, повышая безопасность и эффективность IDM за счет улучшения обнаружения угроз, автоматизации задач, персонализации доступа и усовершенствования защиты от мошенничества.

Пути улучшения IDM при помощи ИИ

ИИ предлагает новые возможности для IDM. Он может анализировать поведение пользователей, их местоположение, тип устройства и другие факторы, чтобы строить динамические правила авторизации, предоставляя доступ только к необходимым ресурсам и минимизируя риски. Использование ИИ в IDM обеспечивает следующие преимущества [1]:

Аутентификация: ИИ позволяет создавать более надежные методы аутентификации, чем традиционные логин/пароль. Например, многофакторная аутентификация с использованием одноразовых паролей, биометрических данных и анализа поведения пользователя [2].

Авторизация: ИИ делает авторизацию более динамичной, учитывая контекст доступа пользователя (местоположение, тип устройства, поведение в системе), предоставляя только необходимый доступ и минимизируя риски.

Предотвращение несанкционированного доступа: ИИ анализирует поведение пользователей, выявляя аномалии, которые могут свидетельствовать о попытке несанкционированного доступа. Также ИИ

учится на данных о прошлых атаках, чтобы предсказывать и блокировать новые угрозы.

Для достижения высокого уровня безопасности в IDM используются конкретные методы ИИ, такие как:

Машинное обучение: выявление аномалий в поведении пользователей, что позволяет предсказывать и блокировать возможные угрозы. Например, методы обучения с учителем анализируют прошлые случаи атак и создают модели для предотвращения несанкционированного доступа [3].

Глубокие нейронные сети (Deep Learning): анализ сложных моделей поведения пользователей, что улучшает надежность биометрической аутентификации, включая распознавание лиц и отпечатков пальцев [4].

Алгоритмы обработки естественного языка (NLP): анализ текстовых данных, используемых для авторизации, например, при проверке ответов на вопросы безопасности или при анализе содержимого сообщений для выявления фишинга.

Заключение

В статье рассмотрено применение ИИ в системах управления идентификацией (IDM) для повышения их безопасности и эффективности. Ключевыми направлениями использования ИИ являются аутентификация, динамическая авторизация, обнаружение угроз и оптимизация процессов управления идентификацией. Также были рассмотрены вызовы, связанные с безопасностью данных, прозрачностью решений и этическими аспектами. Несмотря на эти трудности, ИИ открывает новые горизонты для улучшения IDM в условиях изменяющегося киберпространства.

Список литературы

1. «Ethical Considerations in Artificial Intelligence: A Guide for Policymakers and Businesses» // Brookings Institution, 2023. – URL: https://www.brookings.edu/research/ethical-considerations-in-artificial-intelligence-a-guide-for-policymakers-and-businesses/ (дата обращения 12.06.2024).

2. ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация. // Позитив текнолоджиз, 2020. – URL: https://docs.cntd.ru/document/1200130318 (дата обращения 12.06.2024).

3. Narayana, P., & Saxena, A. (2020). AI-Driven Cybersecurity in Identity Management Systems: A Comprehensive Review. International Journal of Computer Science. // Informational Fusion 97, 2023 – С. 16–19

4. Соков Б.Б. Создание прототипа системы биометрической аутентификации по геометрии лица с помощью методов машинного обучения //Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2018. – С. 175–179.