УДК 004.056

РАЗВИТИЕ АЛГОРИТМОВ ИИ ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК

Яковишин А.Д.

магистр,

Камчатский государственный технический университет

Петропавловск-Камчатский, Россия

Аннотация

В статье рассматривается актуальный вопрос об использовании алгоритмов искусственного интеллекта (ИИ) в борьбе с киберугрозами. Основное внимание уделяется анализу современных тенденций в разработке и применении алгоритмов машинного (Machine Learning, ML, МО) и глубокого (Deep Learning, DL) обучения в контексте кибербезопасности. Исследование охватывает важность прогнозирования и предотвращения кибератак на ранних стадиях, обеспечение защиты информационных систем и данные о применении ИИ в кибератаках. Подчеркивается необходимость разработки новых методов и подходов в области кибербезопасности для противодействия кибератакам.

Ключевые слова: искусственный интеллект, кибербезопасность, машинное обучение, глубокое обучение, кибератаки, алгоритмы ИИ.

DEVELOPMENT OF AI ALGORITHMS FOR DETECTION AND PREVENTION OF CYBER ATTACKS

Yakovishin A.D.

Master's degree,

Kamchatka State Technical University

Petropavlovsk-Kamchatsky, Russia

Abstract

This article addresses the critical theme of using artificial intelligence (AI) algorithms to combat cyber threats. It focuses on analyzing current trends in the development and application of machine learning and deep learning algorithms within the context of cybersecurity. The study encompasses the importance of predicting and preventing cyber attacks at early stages, securing information systems, and data on the use of AI in cyber attacks. The necessity of developing new methods and approaches in cybersecurity to counteract cyber attacks is emphasized.

Keywords: artificial intelligence, cybersecurity, machine learning, deep learning, cyber attacks, AI algorithms.

Введение

Появление направления борьбы с кибератаками возникло из-за угроз, связанных с развитием Интернета, а также растущего объема данных в сети. Считается, что дал толчок к развитию инцидент 2017 года: в ходе атаки программы-вымогателя WannaCry пострадало более 200 000 компьютеров из 150 стран. В последние годы число подобных программ и степень нанесенного ими ущерба стремительно растет. В связи с этим коммерческие и базовые инфраструктуры сталкиваются с повышенными рисками утечки данных и сопутствующими финансовыми потерями.

Целью данной статьи является анализ современных тенденций в области разработки алгоритмов искусственного интеллекта (ИИ), предназначенных для борьбы с кибератаками. Исследование направлено на выявление текущих ограничений и возможностей использования технологий ИИ в контексте обеспечения информационной безопасности. Учитывая все более сложный характер киберугроз, особое внимание уделяется развитию алгоритмов машинного (Machine Learning, ML, МО) и глубокого обучения (Deep Learning), которые могут эффективно анализировать большие объемы данных, выявлять скрытые угрозы и прогнозировать возможные атаки.

Актуальность исследования также обусловлена необходимостью поиска решений в сфере кибербезопасности. В условиях постоянно развивающихся технологий и возрастающей угрозы кибератак, разработка и применение алгоритмов ИИ в сфере кибербезопасности становится ключевым фактором защиты цифровых активов как отдельных компаний, так и целых государств.

Основная часть

Современные алгоритмы ИИ, например, МО, используются и активно развиваются для проведения расширенного анализа данных, выявления признаков и паттернов кибератак, что позволяет в дальнейшем прогнозировать и предотвращать их на ранних стадиях.

Развитие и применение алгоритмов ИИ в сфере кибербезопасности

Использование ИИ для проведения предикативного анализа в области кибербезопасности является критически важным для предугадывания и предотвращения потенциальных кибератак. Этот подход, известный названием Threat Intelligence, признали 96% международных экспертов по информационной безопасности как фундаментальный в современной борьбе с киберугрозами [1]. Американская компания IBM, используя свое инновационное решение IBM Watson for Cybersecurity, анализирует широкий спектр данных для прогнозирования возможных киберугроз. Отчеты Watson за 2023 год указывают на значительное улучшение в области обнаружения и реагирования на угрозы, сокращая время реагирования с нескольких дней до нескольких минут [2]. Это не только уменьшает количество успешных кибератак, но и существенно облегчает рабочую нагрузку на специалистов в области кибербезопасности, освобождая их ресурсы для сосредоточения на других ключевых задачах. Таким образом, интеграция ИИ в системы кибербезопасности значительно повышает их эффективность, обеспечивая более быстрое и точное обнаружение угроз, что является неотъемлемым элементом защиты в цифровую эпоху.

Автоматизация процессов с помощью ИИ в сфере информационной безопасности значительно улучшает эффективность автоматического обнаружения и реагирования. Примером такой инновации является система EDR (Endpoint Detection and Response) от американской компании CrowdStrike, которая сократила время обнаружения угроз с нескольких дней до одного часа. Такой результат был достигнут благодаря автоматизированному анализу данных безопасности из разных источников, что не только ускоряет реакцию на угрозы, но и снижает затраты на их устранение. По данным исследования [3], такой подход может снизить стоимость затрат на последствия кибератак на 1,5 миллиона долларов. Данный пример подчеркивает значимость интеграции ИИ в кибербезопасность для повышения ее эффективности.

Использование систем ИИ также применяется для кодирования и декодирования данных. Внедрение подобных систем является важным шагом в обеспечении кибербезопасности, поскольку они помогают защищать информацию от несанкционированного доступа. В 2023 году американская компания Enveil разработала систему ZeroReveal, которая использует подходы гомоморфного шифрования для защиты данных на всех этапах. Такая система позволила проводить вычисления непосредственно на зашифрованных данных, не раскрывая их содержания. Enveil удалось защитить данные клиентов в ходе нескольких кибератак: киберпреступники не смогли получить доступ к данным даже в случаях успешного проникновения в систему [4].

Технология глубокого обучения Deep Learning в ИИ играет важную роль в анализе больших объемов данных в реальном времени, выявлении аномалий, обнаружении вредоносных активностей и прогнозировании возможных кибератак. Так, японская компания Fujitsu в 2023 году значительно усовершенствовала меры кибербезопасности благодаря применению технологии на основе глубокого обучения [5]. Это позволило компании не только существенно сократить количество успешных кибернападений, но и

уменьшить операционные затраты, повысив при этом эффективность работы своей команды по обеспечению цифровой безопасности. Внедрение таких технологий демонстрирует, как инновации в области ИИ могут быть эффективно использованы для укрепления кибербезопасности на глобальном уровне, в частности в странах с высоким уровнем технологического развития – таких как Япония.

Использование технологий ИИ для осуществления кибератак

В эпоху, когда киберугрозы становятся всё более сложными и изощренными, применение ИИ в сфере кибербезопасности выступает как мощный инструмент защиты. ИИ способен оперативно анализировать огромные объемы данных, выявляя и предотвращая кибератаки на ранних стадиях [6].

Повышение эффективности алгоритмов ИИ в кибербезопасности не остается незамеченным злоумышленниками. Вместе с увеличением количества известных уязвимостей и дефектов безопасности систем, регистрируемых в библиотеке CVE (Common Vulnerabilities and Exposures), наблюдается рост применения технологий ИИ для создания более сложных кибератак. Эти атаки могут включать сложные манипуляции с данными, автоматическое обнаружение и эксплуатацию уязвимостей, а также использование МО для повышения эффективности фишинговых и других видов социальной инженерии.

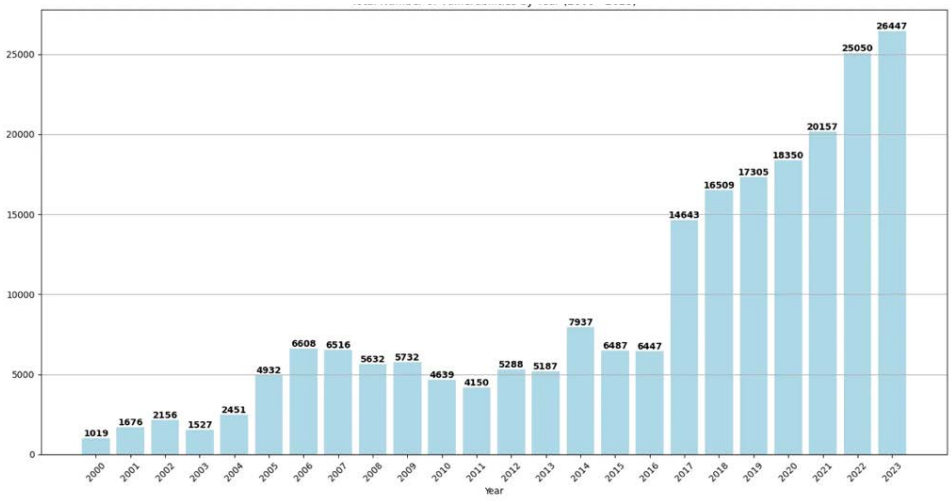

Рис.1 – Общее количество уязвимостей по годам (2000–2023) [7]

Из графика выше (рис. 1) следует, что общее количество уязвимостей, зафиксированных в базе CVE за 2023 год, достигло 26,447 случаев. Такая цифра является рекордной и свидетельствует о том, что потенциал для разработки и проведения кибератак, в т. ч. основанных на ИИ, продолжает расширяться.

Применение технологий ИИ при кибератаках породило потребность в разработке более продвинутых методов обнаружения и предотвращения угроз. К примеру, использование алгоритмов глубокого обучения для анализа поведенческих паттернов и выявления аномалий в системах становится все более актуальным [8].

Выводы

Алгоритмы ИИ, предназначенные для обнаружения и предотвращения кибератак активно развиваются, создавая все более продвинутые и надежные системы кибербезопасности. С учетом актуальности кибербезопасности и растущей сложности угроз, можно ожидать, что это направление будет продолжать активно развиваться в будущем.

Важно также подчеркнуть роль МО, глубокого обучения, искусственных нейронных сетей и алгоритмов кодирования данных в усилении защиты информационных систем. Путем интеграции этих технологий и разработкой

новых методов можно сделать значительный вклад в обеспечение кибербезопасности на глобальном уровне.

Библиографический список

1. Shin, Bongsik, and Paul Benjamin Lowry. "A review and theoretical explanation of the ‘Cyberthreat-Intelligence (CTI) capability’that needs to be fostered in information security practitioners and how this can be accomplished." Computers & Security 92 (2020): 101761.
2. Opara, Emmanuel, Hayden Wimmer, and Carl M. Rebman. "Auto-ML cyber security data analysis using Google, Azure and IBM Cloud Platforms." 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET). IEEE, 2022.
3. Bobovnikova A., Zrazhevskiy A. MODERN LEAN MANAGEMENT TRENDS IN THE US MARKET// Proceedings of the XXX International Multidisciplinary Conference «Innovations and Tendencies of State-of-Art Science». Mijnbestseller Nederland, Rotterdam, Nederland. 2023.
4. More, Stefan, and Lukas Alber. "YOU SHALL NOT COMPUTE on my data: Access policies for privacy-preserving data marketplaces and an implementation for a distributed market using MPC." In Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1-8. 2022.
5. Wang, W., Vos, K., Taylor, J., Jenkins, C., Bala, B., Whitehead, L., & Peng, Z. (2023). Is deep learning superior to traditional techniques in machine health monitoring applications. The Aeronautical Journal, 127(1318), 2105-2117.
6. Кенджаев Д.А. Революция в образовании: AR как средство повышения эффективности обучения / Д.А. Кенджаев // Инновационные подходы в современной науке: сб. ст. по материалам CLVII Международной

научно-практической конференции «Инновационные подходы в современной науке». – № 1(157). – М., Изд. «Интернаука», 2024.
7. Sasi, Tinshu, Arash Habibi Lashkari, Rongxing Lu, Pulei Xiong, and Shahrear Iqbal. "A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges." Journal of Information and Intelligence (2023).
8. Appiah, G., Amankwah-Amoah, J., & Liu, Y. L. (2020). Organizational architecture, resilience, and cyberattacks. IEEE Transactions on Engineering Management, 69(5), 2218-2233.

Оригинальность 89%