УДК 004.7

Ализода С.С.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

Научный руководитель:
Лихачевский Д.В.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ СЕТЕВОЙ БЕЗОПАСНОСТИ

Аннотация. Использование искусственного интеллекта (ИИ) в сетевой безопасности позволяет эффективно обнаруживать и предотвращать атаки, а также анализировать угрозы в реальном времени. ИИ помогает в

автоматизации процессов защиты и реагировании на инциденты. В работе рассматриваются методы применения ИИ, такие как машинное обучение и анализ больших данных, а также возможные риски.

Ключевые слова: ИИ, сетевая безопасность, искусственный интеллект, машинное обучение, защита от атак, аномалии, автоматизация, прогнозирование угроз, киберзащита, безопасность сетей.

В условиях стремительного роста числа кибератак и усложнения методов вторжения традиционные средства защиты компьютерных сетей оказываются недостаточно эффективными [1]. С увеличением объемов передаваемой информации и масштабом атакующих воздействий возникает необходимость в системах, способных адаптироваться к новым условиям и угрозам. В этом контексте технологии искусственного интеллекта (ИИ) становятся ключевым инструментом в арсенале средств кибербезопасности. Их применение позволяет не только оперативно реагировать на инциденты, но и предотвращать атаки еще до того, как они наносят ущерб. В данной статье рассматриваются основные направления использования ИИ в обеспечении сетевой безопасности, а также оцениваются вызовы и перспективы, связанные с этой технологией.

Ранее системы обеспечения сетевой безопасности были в основном основаны на сигнатурных методах – они эффективно справлялись с известными угрозами [2], но были практически бесполезны против новых, неизвестных атак. Такая модель не позволяла вовремя адаптироваться к стремительно меняющемуся ландшафту угроз. Появление систем, использующих поведенческий анализ, стало первым шагом в сторону интеллектуальной безопасности. Однако настоящим прорывом стало внедрение методов машинного обучения и искусственного интеллекта, которые позволили не только фиксировать уже произошедшие инциденты, но и предсказывать потенциальные угрозы на основе большого количества данных.

ИИ способен анализировать сетевой трафик в реальном времени, выявлять аномалии и подозрительную активность, которая не укладывается в рамки стандартного поведения пользователей или систем [3]. Таким образом, он становится активным элементом защиты, а не просто пассивным наблюдателем.

Одним из ключевых направлений применения ИИ в сетевой безопасности является интеллектуальное обнаружение вторжений. Алгоритмы машинного обучения анализируют поведение пользователей, систем и приложений, выявляя отклонения, которые могут свидетельствовать о попытке взлома, заражении вредоносным ПО [4] или компрометации учетной записи. Такие системы непрерывно обучаются, что позволяет им распознавать все более сложные атаки.

Важно отметить, что искусственный интеллект также активно используется в системах автоматического реагирования на инциденты.

После выявления угрозы соответствующая система может в реальном времени изолировать подозрительное устройство, прекратить определенный сетевой процесс или уведомить администратора. Это позволяет значительно сократить время между атакой и началом контрмер, тем самым снижая возможный ущерб.

Кроме того, ИИ находит применение в прогнозировании угроз – на основе исторических данных и текущих трендов формируются модели, позволяющие предугадывать потенциальные сценарии атак [5] и заранее укреплять защиту.

Использование искусственного интеллекта в кибербезопасности дает значительные преимущества. Это прежде всего скорость обработки данных и реагирования, способность обнаруживать ранее неизвестные атаки, а также снижение зависимости от человеческого фактора [6]. В отличие от специалистов, ИИ не устает, не отвлекается и может обрабатывать огромные объемы данных круглосуточно.

Однако существуют и определенные ограничения. Алгоритмы машинного обучения могут быть подвержены ошибкам – например, выдавать ложные срабатывания или, наоборот, пропускать опасные события. Кроме того, существует риск, что злоумышленники начнут использовать ИИ против самих систем безопасности, создавая вредоносные программы, способные обходить интеллектуальные фильтры. Необходимо также учитывать этические аспекты использования ИИ, в том числе вопросы конфиденциальности данных, возможность предвзятости алгоритмов и ограниченность прозрачности в принятии решений.

В ближайшие годы ИИ, скорее всего, станет неотъемлемой частью всех этапов обеспечения сетевой безопасности – от аутентификации пользователей до анализа логов и автоматизации принятия решений. Особое внимание будет уделяться усиленной интеграции ИИ в существующие архитектуры безопасности и повышению его объяснимости – способности «объяснить», почему система приняла то или иное решение. Ожидается также рост интереса к гибридным моделям, сочетающим ИИ с традиционными методами и экспертными системами. Кроме того, начнется активное развитие технологий защиты самих моделей машинного обучения от манипуляций и атак, направленных на подмену или искажение данных, на которых они обучаются.

Таким образом, искусственный интеллект в ближайшем будущем будет не только усиливать существующие системы, но и формировать новые подходы к безопасности, где превентивный характер защиты выйдет на первый план.

Искусственный интеллект уже сегодня занимает важное место в системе обеспечения сетевой безопасности. Он способен существенно повысить эффективность защиты, снизить риски и ускорить реагирование на инциденты. Однако для полной реализации его потенциала необходимо учитывать технические, этические и организационные аспекты. Только

гармоничное сочетание человеческого опыта и машинной точности позволит создать устойчивую и адаптивную систему кибербезопасности, готовую к вызовам цифровой эпохи.

Список использованных источников:

1. Buczak A.L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 2016.

2. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010.

3. Garcia-Teodoro P., Diaz-Verdejo J., Maciá-Fernández G., Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 2009.

4. Bhuyan M.H., Bhattacharyya D.K., Kalita J.K. Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials, 2014.

5. Chio C., Freeman D. Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media, 2018.

6. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. Springer, 2012.

Alizoda S.S.
Belarusian State University of
Informatics and Radioelectronics, Minsk

Scientific supervisor:
Likhachevsky D.V.
Belarusian State University of
Informatics and Radioelectronics, Minsk

THE ROLE OF ARTIFICIAL INTELLIGENCE IN NETWORK SECURITY

Abstract. The use of artificial intelligence (AI) in network security enables efficient detection and prevention of attacks, as well as real-time threat analysis. AI helps automate protection processes and respond to incidents. The paper discusses AI methods like machine learning and big data analysis, as well as potential risks.

Keywords: AI, network security, artificial intelligence, machine learning, attack protection, anomalies, automation, threat forecasting, cybersecurity, network safety.