РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРБЕЗОПАСНОСТИ

АХРОРОВ Одилжон Алимжонович
Преподаватель Военно-оборонного
Университета Республики Узбекистан.

Аннотация. С ростом киберугроз и угроз безопасности в цифровой среде важность роли искусственного интеллекта в кибербезопасности становится все более очевидной. Эффективное использование алгоритмов машинного обучения, автоматизация обнаружения и реагирования на кибератаки, решение этических вопросов, связанных с использованием искусственного интеллекта в этой сфере, являются ключевыми аспектами современной кибербезопасности. В данной статье рассматривается роль и влияние искусственного интеллекта на кибербезопасность, определяются преимущества и проблемы, а также обсуждаются этические аспекты этого вопроса.

Ключевые слова. Информационная безопасность; Киберугрозы; Информационная безопасность; Защита данных.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

AXROROV Odiljon Alimjonovich
Lecturer at the Military Security and Defense University
of the Republic of Uzbekistan

Annotation. With the rise of cyber and security threats in the digital environment, the importance of the role of artificial intelligence in cybersecurity is becoming increasingly clear. Effective use of machine learning algorithms, automation of detection and response to cyberattacks, and resolution of ethical issues associated with the use of artificial intelligence in this area are key aspects of modern cybersecurity. This article examines the role and impact of artificial intelligence on cybersecurity, identifies advantages and challenges, and discusses the ethical aspects of this issue.

Keywords: Information security; Cyber threats; Information Security; Data protection.

Введение.

В современном цифровом мире, где технологии становятся все более сложными, а киберугрозы - все более активными, роль искусственного интеллекта (ИИ) в обеспечении кибербезопасности становится ключевой [1]. Искусственный интеллект внедряется в сферу кибербезопасности с целью не

только обнаружения и предотвращения угроз, но и эффективного реагирования на них.

Одним из важных аспектов является автоматизация процесса кибербезопасности с использованием искусственного интеллекта. Алгоритмы машинного обучения позволяют системам автоматически анализировать большие объемы данных, выявлять и предсказывать возможные кибератаки [2]. Это позволяет оперативно реагировать и незамедлительно предотвращать угрозы до того, как они нанесут ущерб систему (сети). Технологии машинного обучения также способствуют созданию интеллектуальных систем, способных адаптироваться к новым видам угроз [3]. Системы, оснащенные искусственным интеллектом, могут обучаться на основе новых данных и улучшать свою эффективность с течением времени.

Это особенно важно в контексте появления всё более сложных кибератак. Кроме того, искусственный интеллект применяется для создания интеллектуальных систем анализа угроз и решения сложных киберзадач [4]. Такие системы могут обрабатывать данные в реальном времени, выявлять нестандартное поведение пользователей, анализировать сетевой трафик и обнаруживать скрытые угрозы.

Однако, вместе с усилением киберзащиты, искусственный интеллект также становится инструментом для создания более сложных кибератак. Атакующие могут использовать технологии машинного обучения для создания интеллектуальных и трудновыявляемых угроз. Это подчеркивает необходимость постоянного совершенствования методов кибербезопасности и адаптации к новым вызовам. Одним из значительных аспектов обсуждения являются этические вопросы, связанные с использованием искусственного интеллекта в кибербезопасности [5]. Вопросы конфиденциальности, ответственности за принятие решений, а также создание стандартов и регулирование в этой области становятся все более актуальными.

В современном мире, где технологии играют огромную роль в нашей повседневной жизни, кибербезопасность становится все более значимым аспектом. Угрозы виртуального пространства постоянно эволюционируют, и потому необходимо развивать инновационные методы и инструменты для борьбы с киберпреступностью [6]. В этом контексте, искусственный интеллект (ИИ) играет все более важную роль в обеспечении кибербезопасности. Искусственный интеллект обладает потенциалом преобразовывать современные методы обнаружения и реагирования на киберугрозы.

Автоматическое обнаружение инцидентов, анализ больших объемов данных, прогнозирование потенциальных уязвимостей - все это является областью применения ИИ в кибербезопасности. Это позволяет

идентифицировать и отражать атаки быстрее, чем это возможно для человека. Повышение кибербезопасности имеет решающее значение в современном цифровом мире.

Предлагаются несколько предложений по улучшению кибербезопасности:

Обучение и осведомленность сотрудников: 1. Проведение регулярных обучений сотрудников кибербезопасности, в целях выявлениях новых потенциальных угроз. 2. Развитие культуру заботы кибербезопасности сотрудников в целях оперативно сообщать о подозрительных действиях.

Надежные меры аутентификации: 1. Обеспечение использования надежных и уникальных паролей для всех учетных записей. 2. Внедрение многофакторную аутентификацию (MFA), в целях обеспечения дополнительного уровня безопасности.

Сетевая безопасность: 1. Использование брандмауэров для мониторинга и контроля входящего и исходящего сетевого трафика. 2. Использование системы обнаружения и предотвращения вторжений для выявления потенциальных угроз и обеспечение автоматического реагирования сети на них [7].

Помимо этого Искусственный интеллект также способен усилить процессы аутентификации и авторизации. Аутентификация на основе ИИ, будь то сканирование отпечатков пальцев и ладони, намного безопаснее, и система может сканировать их надежно. Когда биометрические логины связаны с паролями, вероятность взлома данных пользователя становится значительно ниже. Технологии распознавания лиц и голоса, могут предоставить более надежные способы идентификации пользователей. Благодаря ИИ, можно создать системы, которые могут автоматически обнаруживать необычную активность в сети и применять меры безопасности для предотвращения возможных атак. Кроме того, ИИ может быть использован для разработки сильных систем противодействия фишингу и вредоносному программному обеспечению.

Алгоритмы машинного обучения могут анализировать тысячи электронных писем, обнаруживая подозрительные и небезопасные ссылки, а также прикрепленные файлы. Такие системы способны улучшить процессы фильтрации на самом раннем этапе, что помогает предотвратить многие кибератаки [8]. Искусственный интеллект также может использоваться для разработки системы мониторинга, которая анализирует активность в сети и идентифицирует любые подозрительные действия. Это позволяет предупреждать потенциальные угрозы и принимать меры для их нейтрализации. Однако, несмотря на все преимущества, ИИ также несет некоторые риски. ИИ может быть использован для защиты, он может быть использован и

злоумышленниками для создания более сложных и усовершенствованных атак. Соответственно, необходимы такие же сильные системы искусственного интеллекта для борьбы с этими угрозами.

Заключение.

В заключение можно отметить что, роль искусственного интеллекта в кибербезопасности является основополагающей и стремительно развивающейся. Он способен улучшить обнаружение и реагирование на киберугрозы, сделать процессы аутентификации и авторизации более надежными, а также предотвратить фишинги и внедрение вредоносных программных обеспечений. Однако, важно развивать соответствующие механизмы искусственного интеллекта для борьбы с растущими угрозами. Взаимодействие между ИИ и людьми становится ключевым фактором для обеспечения кибербезопасности в нашем цифровом обществе. Роль искусственного интеллекта в кибербезопасности неотъемлема в современном цифровом обществе. ИИ позволяет усиливать защиту от киберугроз, но также предъявляет новые вызовы, требующие внимания к аспектам безопасности и этики.

Список использованной литературы.

[1]. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. (2022). Искусственный интеллект и кибербезопасность. International Journal of Open Information Technologies, 10(9), 135-147.

[2]. Афанасьева Д.В. (2020). Применение искусственного интеллекта в обеспечении безопасности данных. Известия Тульского государственного университета. Технические науки, 2, 151-154.

[3]. Власенко А.В., Киселёв П.С., Склярова Е.А. (2021). Искусственный интеллект и проблемы кибербезопасности. Технология Deepfake. Молодой ученый, (21), 81-86.

[4]. Basnet, Ram, Srinivas Mukkamala, and Andrew H. Sung. "Detection of phishing attacks: A machine learning approach." Soft computing applications in industry. Springer, Berlin, Heidelberg, 2008. 373-383.

[5]. Divakaran, Dinil Mon, and Adam Oest. "Phishing Detection Leveraging Machine Learning and Deep Learning: A Review." arXiv preprint arXiv:2205.07411 (2022). [15] Shenfield, Alex, David Day, and Aladdin Ayesh. "Intelligent intrusion detection systems using artificial neural networks." Ict Express 4.2 (2018): 95-99.

[6]. Mishra, Preeti. "A detailed investigation and analysis of using machine learning techniques for intrusion detection." IEEE Communications Surveys & Tutorials 21.1 (2018): 686-728.

[7]. Noor, Umara. "A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories." Future Generation Computer Systems 95 (2019): 467-487.

[8]. Dmitry, Namiot, Ilyushin Eugene, and Chizhov Ivan. "On a formal verification of machine learning systems." International Journal of Open Information Technologies 10.5 (2022): 30-34.