УДК 004.896

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРБЕЗОПАСНОСТИ

Ягубов Эмин Джалал оглу
Emin.yaqubov.03@bk.ru
Магистрант 1-го курса по специальности «Кибербезопасности»
Сумгаитский государственный
университет г.Сумгаит, Республика
Азербайджан Научный
руководитель – **Ахмедова С.М.**
к.т.н.,доцент

Стремительное развитие цифровых технологий привело к росту количества и сложности киберпреступлений. Такая ситуация создает серьезные угрозы для отдельных лиц, предприятий и правительств. Искусственный интеллект (ИИ) открывает новые возможности в сфере кибербезопасности и обеспечивает эффективные решения в борьбе с киберпреступностью. В данной статье рассматривается применение ИИ в кибербезопасности и его роль в снижении киберпреступности [1].

В ходе исследования было выявлено, что применение искусственного интеллекта в кибербезопасности выглядит следующим образом.

1. Обнаружение и анализ угроз

ИИ может быстро анализировать большие объемы данных и выявлять потенциальные угрозы в режиме реального времени. Алгоритмы машинного обучения обнаруживают аномалии в сетевом трафике и поведении пользователей, выявляя нарушения безопасности на ранней стадии [2,3].

2. Прогностическая аналитика

ИИ позволяет прогнозировать будущие атаки, анализируя исторические данные. Это позволяет организациям заранее выявлять потенциальные уязвимости и принимать соответствующие меры.

3. Автоматизированные системы реагирования

Системы на основе искусственного интеллекта автоматически реагируют на инциденты безопасности, минимизируя последствия атак. Например, при обнаружении подозрительной

активности эти системы могут изолировать затронутые устройства или блокировать вредоносный трафик [2,4].

4. Анализ поведения

ИИ отслеживает поведение пользователей и системы, определяет нормальные модели активности и обнаруживает отклонения от них. Это помогает своевременно выявлять внутренние угрозы или захваты счетов.

5. Оценка уязвимости

ИИ помогает выявлять потенциальные уязвимости в системах, расставляя приоритеты и устраняя их. Это позволяет организациям более эффективно использовать свои ограниченные ресурсы, сосредоточившись на наиболее критических уязвимостях [4].

Искусственный интеллект произвел революцию в кибербезопасности и стал мощным инструментом в борьбе с киберпреступностью. Применение ИИ в таких областях, как обнаружение угроз, предиктивная аналитика, автоматизированные системы реагирования и поведенческий анализ, значительно повышает обороноспособность организаций.

Список использованной литературы:

1. Goodman, M. (2015). Future Crimes: Inside the Digital Underground and the Battle for Our Connected World.
2. Brundage, M., Avin, S., Clark, J., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.
3. Sharma, T. (2021). Artificial Intelligence in Cybersecurity: Impact and Future Trends. Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing.