Анализ использования систем поддержки принятия решений на основе нейросетевых технологий

Капелькин Никита Александрович
Курсант КВВУ
E-mail: nik.kapelkin@mail.ru

Научный руководитель:
Петухов Андрей Юрьевич

В данной статье рассматриваются возможности и дальнейшие перспективы развития систем поддержки принятия решений в совместном использовании с нейросетевыми технологиями.

Система поддержки принятия решений, нейросетевые технологии, искусственный интеллект.

Технологии искусственного интеллекта (ИИ) стремительно развиваются. При этом, рост количества киберугроз, а также их виды и разнообразие, становятся с каждым днем все более изощреннее. Традиционные меры безопасности постепенно отходят на второй план, уступая своему новому конкуренту в лице «искусственного помощника». Кроме того, совместное использование систем поддержки принятия решений (СППР) и нейросетевых технологий позволяют повысить эффективность и качество принимаемых решений во многих областях, начиная от бизнеса до медицины и науки.

Искусственный интеллект — научное направление, в рамках которого ставятся и решаются задачи аппаратного или программного моделирования тех видов человеческой деятельности, которые традиционно считаются интеллектуальными [1].

В системе кибербезопасности машинное и глубокое обучение является составляющим компонентом ИИ в целом, однако ИИ имеет и свою индивидуальную цель.

Наилучшее использование систем на базе ИИ — применение самостоятельных решений, таким образом, чтобы ИИ вырабатывал наиболее результативный вариант развития событий, исключая запрограммированный сценарий на основе набора различных данных.

ИИ может эффективно детектировать сложные постоянные угрозы, такие как скрытное вредоносное ПО, которое без труда способно скрыться от лица киберспециалистов.

Облегчение работы киберспециалистов. Важно отметить одно из главных преимуществ применения ИИ в сфере информационной безопасности — автоматизация повседневных задач. Системы на базе ИИ анализируют журналы по безопасности, поведение людей и сетевой трафик. Таким образом, специалисты по кибербезопасности частично делегируют свои полномочия и располагают большим временем для решения более сложных стратегических задач.

Недостатками использования ИИ в кибербезопасности, являются Алгоритмы ИИ. Несмотря на преимущества использования ИИ в кибербезопасности, существуют и некоторые негативные аспекты. Так, например, один из недостатков связан со сложностью алгоритмов ИИ, который затрудняет их понимание специалистами по безопасности и вызывает некоторые сомнения.

Возможность манипуляции. Еще одной проблемой является возможность преднамеренного манипулирования системами ИИ, когда злоумышленники способны намеренно внедрять в систему искаженные данные, которые вводят в заблуждение и дестабилизируют защиту в целом.

Отсутствие человеческого суждения. Системы на базе ИИ невероятно умны и эрудированны,

однако «искусственный помощник» никогда не заменит человека в бытовых, морально-этических и творческих вопросах. Поэтому, в исключительных случаях, когда ИИ некомпетентен в некоторых постулатах, то обязательно требуется применение человеческого суждения для адекватной оценки контекста.

Рассмотрим методы улучшения информационной безопасности на базе ИИ. Безусловно, что для дальнейшего и плодотворного развития интеллектуальных систем необходимо в полной мере продолжать ведущие разработки по улучшению всех вышеперечисленных интеллектуальных систем. Поэтому важно продолжать активное инвестирование ведущими российскими компаниями в развитие ИИ. Так, например, разработчиками ИИ в России выступают такие компании как: «Яндекс», «Rubbles», «Voximplant».

Комплексное применение СППР и нейросетевых технологий в информационной безопасности обещает значительные преимущества и перспективы:

1. Обнаружение угроз и аномалий.

2. Автоматизация реакции на инциденты.

3. Улучшенная аналитика и прогнозирование.

Совместное применение СППР и нейросетевых технологий в информационной безопасности может значительно улучшить эффективность защиты информационных систем и сократить время реакции на угрозы, что важно в условиях постоянно меняющейся киберугрозовой среды.

В заключении отмечу, что сочетание ИИ в вопросах информационной безопасности имеет явные перспективы для укрепления защиты от постоянно растущего спектра киберугроз. Для подтверждения приведу слова Андрея Красовского, директора по маркетингу Swordfish Security: «В настоящее время ИИ всё еще не используется широко в области информационной безопасности, но у этих технологий большие перспективы в данном направлении» [3].

Список используемой литературы:

1. Аверкин А.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А. Толковый словарь по искусственному интеллекту. Москва: изд-во Радио и связь, 1992. с. 38.

2. ГОСТ Р 59895-2021. Технологии искуственного интеллекта в образовании. 2021. 2.1.7. с. 2.

3. Cisoclub. Искусственный интеллект в ИБ. 2023. URL: https://cisoclub.ru/aaiskusstvennyj-intellekt-v-ib/ (дата обращения: 17.04.2024).