ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ КИБЕРЗАЩИТЫ ВОЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Каравай М.А., Пинголь Е.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гусаков П.Б.

Аннотация. Современные вооружённые конфликты всё чаще включают киберкомпонент. Информационные системы армии и объектов критической инфраструктуры становятся приоритетными целями для кибератак. Использование искусственного интеллекта (ИИ) в военной сфере позволяет создать адаптивные и автоматизированные системы защиты, способные в реальном времени обнаруживать, анализировать и устранять угрозы. В работе рассматриваются особенности применения ИИ в кибербезопасности военных систем, примеры существующих решений и перспективы развития.

С расширением спектра киберугроз и переходом вооружённых конфликтов в цифровую плоскость защита военных информационных систем выходит на первый план. Традиционные методы кибербезопасности не всегда эффективны при атаках на сетевые структуры армейских подразделений, системы управления, радиосвязи, навигации и вооружения. Искусственный интеллект предлагает новые подходы, основанные на непрерывном анализе поведения систем, обнаружении аномалий и оперативном реагировании на потенциальные инциденты.

Одним из ключевых направлений является применение ИИ для защиты военных сетей в условиях ограниченного времени и ресурсов. Используются методы машинного обучения, включая глубокие нейросети, обучение без учителя и методы самообучения, позволяющие выявлять признаки атак даже без заранее заданных сигнатур. Это особенно актуально при противодействии APT-группировкам, использующим сложные и многоэтапные сценарии вторжения. ИИ способен анализировать сетевой трафик, лог-файлы, данные телеметрии с узлов связи и управления, создавая модель нормального поведения системы и оперативно определяя отклонения.

Важной особенностью военных ИИ-систем является требование к их автономности. В условиях радиоэлектронного противодействия, блокировки каналов связи и физической изоляции подразделений системы киберзащиты должны функционировать без внешней поддержки. Такие решения проектируются с учётом устойчивости к атакам на сами алгоритмы — в том числе попыткам внедрения вредоносных данных, способных изменить поведение модели. Кроме того, особое внимание уделяется интерпретируемости решений, чтобы командный состав мог оперативно принимать обоснованные действия на основе отчётов системы.

Дополнительным направлением развития ИИ-средств в военной информационной безопасности становится их интеграция с платформами класса SOAR (Security Orchestration, Automation and Response). Это позволяет не только выявлять инциденты, но и в автоматическом режиме запускать защитные сценарии: блокировать сетевые подключения, изолировать атакованные узлы, создавать маршруты обхода и передавать оперативные отчёты ответственным офицерам. В условиях ограниченного времени реагирования и высокой динамики боевой обстановки такая автоматизация становится критически важной.

Особое значение приобретает разработка систем объяснимого искусственного интеллекта (XAI), способных не только выносить решения, но и предоставлять их интерпретацию. Это необходимо при функционировании в связке с человеком-оператором в центрах боевого управления. Такие системы позволяют повысить доверие к автоматизированным решениям, минимизируя риски ошибочных действий и повышая оперативность принятия решений в условиях неопределённости.

В перспективе искусственный интеллект может быть глубоко интегрирован в единые автоматизированные системы управления войсками (АСУ), обеспечивая защиту от информационного воздействия на всех уровнях – от индивидуального бойца до командных пунктов оперативного звена. Возможно создание «умных» кибербарьеров, динамически адаптирующихся к боевой обстановке, обладающих способностью к самообучению и самостоятельному восстановлению после атак. Применение таких технологий укрепляет цифровую безопасность армии и становится одним из ключевых направлений обеспечения военного превосходства в XXI веке.

Таким образом, искусственный интеллект открывает новые горизонты для повышения устойчивости военных информационных систем. Он обеспечивает проактивную защиту, сокращает время реагирования, снижает нагрузку на операционный персонал и позволяет эффективно противостоять киберугрозам в условиях реального и гибридного конфликта. Комплексная интеграция ИИ в системы кибероборонs позволит вооружённым силам сохранить технологическое преимущество и обеспечить цифровой суверенитет в информационном противостоянии.

Список использованных источников:

1. Злотин А.И., Мацкевич В.М. Кибероборона: современные подходы и технологии. Военная мысль, 2020.

2. Чеботарёв А.А. Интеллектуальные системы в кибероборонe. Вестник ВА РБ, 2022.

3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.

4. Мельников И.С. Искусственный интеллект в военном деле: перспективы и вызовы. Информационная безопасность, 2021.