УДК 004.8:004.056

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРБЕЗОПАСНОСТИ

М.Д. ЮРОВ

Международный университет «МИТСО»
(г. Минск, Беларусь)

E-mail: maksimyurauscience@gmail.com

Аннотация. Рассмотрена двойственная роль искусственного интеллекта (ИИ) в кибербезопасности, включая его технологический фундамент, ключевые области применения, а также преимущества и вызовы внедрения. Показано, что интеграция ИИ ведет к перераспределению функций между автоматизированными системами и человеком, формированию спроса на гибридных специалистов и развитию интеллектуальных инструментов проактивной защиты.

Abstract. The dual role of artificial intelligence (AI) in cybersecurity is examined, including its technological foundation, key areas of application, and the benefits and challenges of implementation. It is shown that the integration of AI leads to a redistribution of functions between automated systems and humans, creating a demand for hybrid specialists, and developing intelligent proactive defense tools.

Введение

Стремительное развитие технологий ведет к росту разнообразия и числа киберугроз. В таких условиях традиционные системы информационной безопасности, применяемые в организациях по всему миру, утрачивают актуальность, не успевая адаптироваться к увеличению и усложнению кибератак. Масштаб проблемы подтверждают и финансовые прогнозы, согласно которым глобальные потери от киберпреступлений составят 11,9 трлн долларов США в 2026 году и увеличатся до 19,7 трлн долларов США в 2030 году [1]. При этом ИИ становится одним из ключевых факторов, одновременно способствующих как росту числа атак, так и совершенствованию защиты [2].

Двойственная природа и технологический фундамент ИИ в кибербезопасности

Двойственная природа ИИ в сфере кибербезопасности проявляется в том, что одни и те же технологические достижения одновременно усиливают как наступательный, так и оборонительный потенциал. С одной стороны, злоумышленники применяют ИИ для повышения эффективности, адаптивности, а также масштабируемости кибератак, с другой — организации используют ИИ для усиления проактивности, устойчивости и оперативности систем информационной безопасности.

Технологический фундамент современных средств защиты информации на базе ИИ опирается на несколько взаимодополняющих ветвей ИИ. Машинное обучение, использующее алгоритмы для обучения на основе данных и прогнозирования, применяется для обнаружения возможных угроз и автоматического реагирования на них, охватывая различные устройства, разных пользователей и разные сети. Глубокое обучение и нейронные сети применяются для обнаружения сложных угроз и автоматического реагирования на них. Благодаря технологии обработки естественного языка генеративный ИИ позволяет специалистам по безопасности взаимодействовать с системами на естественном языке, генерировать отчеты, резюмировать результаты анализа, а также предоставлять развернутые ответы, ускоряя тем самым исследование инцидентов и реагирование на них. ИИ-агенты применяются для автономного выполнения рутинных задач безопасности, таких как анализ фишинга, предотвращение утечек данных, оптимизация политик условного доступа и ранжирование уязвимостей, освобождая время специалистов для проактивной защиты [3].

Ключевые области применения ИИ в кибербезопасности

Варианты использования ИИ охватывают практически все ключевые области кибербезопасности. В сфере управления идентификацией и доступом алгоритмы анализируют закономерности в поведении пользователей при входе в систему и выявляют аномалии. При наступлении определенных условий ИИ-решения способны автоматически инициировать двухфакторную проверку подлинности, принудительный сброс пароля или, если есть основания подозревать компрометацию учетной записи, полностью

заблокировать вход пользователя. В области безопасности конечных точек ИИ помогает идентифицировать все устройства организации, поддерживать их в актуальном состоянии с новейшими операционными системами и решениями безопасности, а также обнаруживать вредоносные программы и следы кибератак на устройствах. Для обеспечения безопасности данных алгоритмы ускоряют выявление и маркировку конфиденциальной информации. Кроме того, ИИ способен оперативно обнаруживать попытки несанкционированной передачи данных вовне и блокировать такие действия. В безопасности облака ИИ объединяет информацию от различных поставщиков облачных служб, формируя комплексное представление о рисках и уязвимостях, что позволяет быстрее устранять угрозы [3].

Центральную роль ИИ играет в обнаружении угроз и реагировании на инциденты. Решения класса XDR (Extended Detection and Response) используют ИИ для отслеживания аномального поведения на конечных точках, в сообщениях электронной почты, учетных данных и облачных приложениях, коррелируя разрозненные инциденты в единую картину атаки. Продвинутые модели ИИ способны предотвращать сложные атаки, в том числе программы-вымогатели, и предоставлять рекомендации по улучшению охвата системы безопасности. Решения класса SIEM (Security Information and Event Management), в свою очередь, применяют ИИ для агрегирования сигналов со всей организации и формирования действенных рекомендаций на основе аналитики угроз, что позволяет реализовывать упреждающий подход к киберугрозам. При реагировании на инциденты генеративный ИИ дополнительно упрощает исследование, автоматически отвечая на вопросы и переводя технический анализ на естественный язык [3].

Преимущества и вызовы внедрения ИИ

К преимуществам ИИ в кибербезопасности относятся более раннее выявление угроз за счет выделения действительно важных инцидентов из тысяч безопасных событий и связывания разрозненных действий в единую картину атаки. Инструменты на базе генеративного ИИ упрощают создание отчетов, помогают обнаруживать скрытые уязвимости и ускоряют выполнение сложных задач. Непрерывное обучение и понимание контекста позволяют радикально снизить количество ложных срабатываний, а способность ИИ к адаптации обеспечивает устойчивость защиты при любом масштабе угроз [3].

Вместе с тем использование ИИ в кибербезопасности сопряжено с рядом вызовов. Прежде всего, внедрение и поддержка ИИ-решений требуют значительных дополнительных затрат на вычислительные ресурсы, хранение данных, а также привлечение профильных специалистов. Серьезной проблемой также остается безопасность самих систем ИИ, поскольку они уязвимы, а их компрометация способна не только снизить эффективность защиты, но и создать дополнительные векторы для кибератак. Кроме того, несовершенство систем ИИ, выражающееся в ложных срабатываниях, непредсказуемых ошибках и сильной зависимости от качества исходных данных, по-прежнему ограничивает их надежность в критически значимых сценариях.

Заключение

Интеграция ИИ в кибербезопасность ведет к перераспределению ролей, при котором рутинные операционные задачи все чаще передаются ИИ-агентам, а специалисты концентрируются на стратегических решениях и проактивной охоте на сложные угрозы. Параллельно формируется запрос на гибридных профессионалов, владеющих компетенциями одновременно в области безопасности и анализа данных. Развиваются специализированные ИИ-инструменты, такие как интеллектуальные обманные ловушки, системы прогнозирования мошенничества и автономные агенты, обрабатывающие оповещения, благодаря чему центры кибербезопасности превращаются в среды с глубоко интегрированным ИИ, где контроль человека сосредоточен на интерпретации аналитики и принятии окончательных решений [3].

Список использованных источников

1. Global Cybercrime Report 2025 // Proxyrack. — URL: https://www.proxyrack.com/blog/global-cybercrime-report-2025/ (date of access: 24.05.2026).

2. Тренды атак в 2026 году // Positive Technologies. — URL: https://ptsecurity.com/research/analytics/trendy-atak-v-2026-godu/ (дата обращения: 24.05.2026).

3. Что такое ИИ для кибербезопасности? // Microsoft. — URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-ai-for-cybersecurity (дата обращения: 24.05.2026).