ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Орлов К. И., Шклянко А. А., Полоско Е. И.

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

Ефремов А.А. – заведующий кафедрой ЭИ, к.э.н., доцент

Аннотация. Данная работа посвящена исследованию на тему использования технологий искусственного интеллекта в информационной безопасности и их влиянию на повышение уровня защиты данных. Также будет рассмотрены такие аспекты, как преимущества использования искусственного интеллекта в информационной безопасности, как он помогает при защите от новых видов кибератак и предотвращении использования вредоносных программ.

Искусственный интеллект (ИИ) – это мощная технология, которая помогает специалистам сферы информационной безопасности автоматизировать рутинные задачи, идентифицировать и реагировать на угрозы в наименьшие сроки, а также повышать точность своих действий для укрепления уровня безопасности от различных проблем и кибератак.

Искусственный интеллект доказал свою важность в борьбе с проблемами информационной безопасности, предлагая разработку «Интеллектуальных Агентов» для эффективного решения

конкретных задач безопасности. «Интеллектуальный Агент», в виде аппаратного или программного обеспечения, разработан для повышения вероятности достижения определенной цели из-за его способности наблюдать, учиться и принимать проанализированные решения. Эти «Интеллектуальные Агенты» могут обнаруживать недостатки в сложных структурах кода, выявлять необычные образцы входа пользователей и даже распознавать новые типы вредоносных программ, отличающихся от традиционных методов обнаружения.

Внутри «Интеллектуальные Агенты» обрабатывают огромные объемы данных для изучения и понимания паттернов (шаблонов). Когда они открываются в системах защиты, агенты применяют свои знания, анализируя входящие данные, включая ранее неизвестную информацию.

Применение ИИ в кибербезопасности может быть ценным и эффективным подходом, но, как и любая технология, она имеет свои достоинства и недостатки. Хотя автоматизация и приносит значительные преимущества, важно найти баланс и сочетать её с человеческой экспертизой. Синергия между автоматизированными инструментами и опытными специалистами по кибербезопасности необходима для создания надежной защиты от разнообразных и постоянно меняющихся киберугроз. Использование искусственного интеллекта в кибербезопасности позволяет эффективно преодолевать сложности, с которыми сталкиваются организации, и значительно улучшать их уровень безопасности. Вот ряд преимуществ, которые автоматизация может предложить:

– Эффективность и скорость. Автоматизация может значительно увеличить скорость и эффективность кибербезопасности. Автоматизированные системы могут быстро анализировать огромные объемы данных, обнаруживать угрозы и реагировать на проблемы гораздо быстрее, чем при ручных методах. Эта скорость крайне важна в столь быстро меняющейся обстановке;

– Снижение человеческого фактора. Автоматизация помогает уменьшить риск человеческой ошибки, часто являющейся причиной киберинцидентов. Автоматизированные системы могут следовать заранее определенным протоколам безопасности, минимизируя вероятность ошибок, которые могут привести к уязвимостям систем безопасности;

– Круглосуточный мониторинг и реагирование. Автоматизированные меры кибербезопасности обеспечивают постоянный мониторинг сетей и систем, обеспечивая активную защиту от потенциальных угроз. Это бдительное наблюдение сложно поддерживать вручную, особенно в больших и сложных информационных технологиях;

– Масштабируемость. Автоматизированные системы могут легко масштабироваться для обработки большого объема данных и различных задач безопасности. Эта масштабируемость крайне важна для организаций с сложной инфраструктурой и большим объемом сетевого трафика;

– Рутинные и повторяющиеся задачи. Автоматизация хорошо подходит для выполнения рутинных и повторяющихся задач, позволяя человеческим специалистам по кибербезопасности сосредоточиться на более сложных и стратегических аспектах безопасности. Это повышает удовлетворенность работой и использует человеческую экспертизу там, где она наиболее необходима.

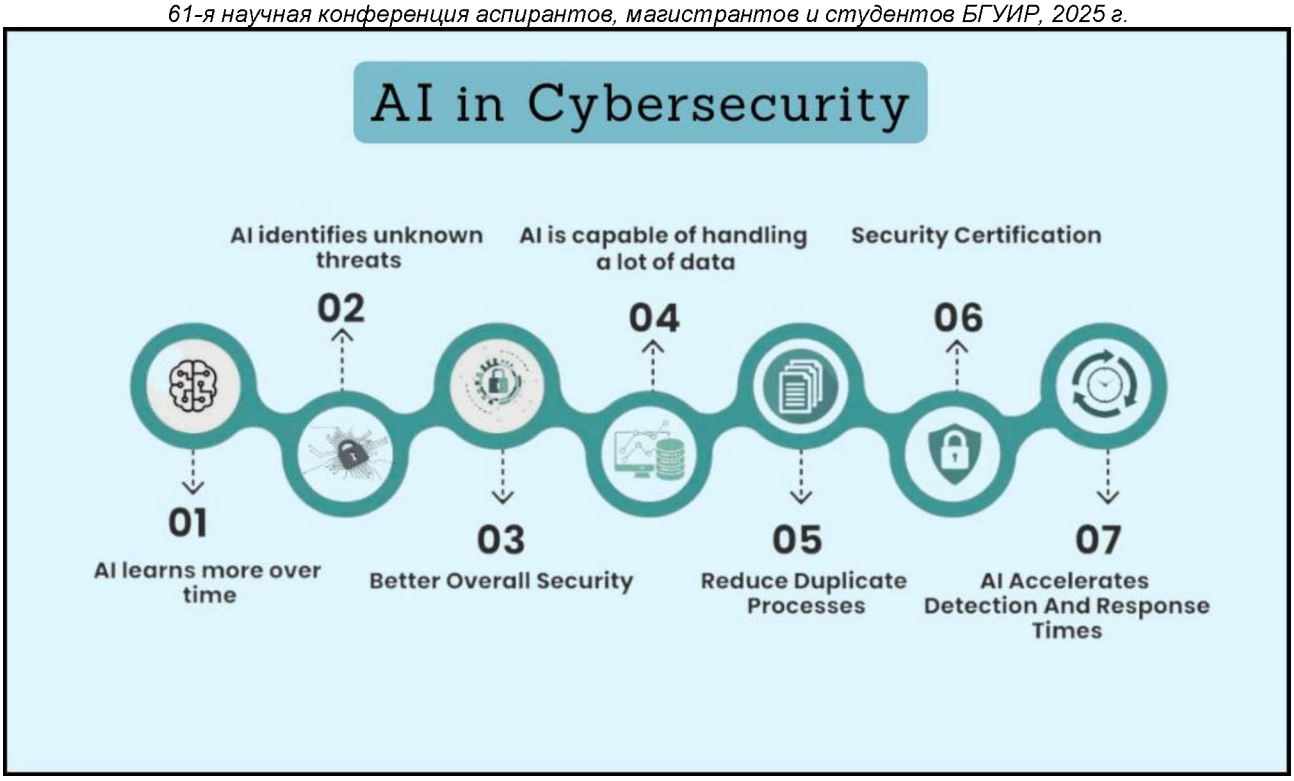

Рисунок 1.Преимущества использования ИИ в кибербезопасности

Как и было упомянуто выше, в использовании искусственного интеллекта, как и в любой другой технологии присутствуют свои недостатки:

– Снижение порога входа для злоумышленников. Искусственный интеллект представляет опасность для информационной безопасности тем, что снижает порог знаний, необходимых для создания злоумышленниками вредоносного программного обеспечения. Таким образом он не только помогает справляться с угрозами, но и сам стимулирует увеличение их количества.

– Зависимость от данных и алгоритмов. Использование искусственного интеллекта в информационной безопасности требует постоянного обновления баз данных и алгоритмов, что может быть затруднительно и в случае атаки злоумышленников на эти ресурсы, может привести к большим угрозам для безопасности.

– Повышенная опасность для неподготовленных пользователей.

– Усиление сложности киберугроз. С использованием ии увеличилась важность наличия квалифицированных специалистов по кибербезопасности. Однако глобальный спрос на этих экспертов значительно превышает предложение. Согласно исследованию 2022 года о кибербезопасности от (ISC)², в мире наблюдается дефицит в 3,4 миллиона специалистов по кибербезопасности.

– Более серьезные угрозы. По мере увеличения сложности искусственного интеллекта возрастает и сложность киберугроз. Может возникнуть ситуация, когда опытный киберпреступник использует инструмент искусственного интеллекта для создания высоко персонализированного сообщения спирфишинга. Это сообщение, идеально вписываясь во внутренний стиль коммуникации организации, может обмануть даже самых бдительных сотрудников, не говоря уже о рядовых пользователях.

Список использованных источников:

1. The Role of AI in Cybersecurity – A Comprehensive Guide on AI in Cybersecurity [Электронный ресурс] – Режим доступа: https://www.eccu.edu/blog/technology/the-role-of-ai-in-cyber-security/ – Дата доступа: 06.04.2025

2. The Role of Artificial Intelligence (AI) in Modern Cybersecurity [Электронный ресурс] – Режим доступа: https://www.encryptionconsulting.com/the-role-of-artificial-intelligence-ai-in-modern-cybersecurity/ – Дата доступа: 06.04.2025

3. Artificial intelligence for cybersecurity: Literature review and future research directions [Электронный ресурс] – Режим доступа: https://www.sciencedirect.com/science/article/pii/S1566253523001136 – Дата доступа: 06.04.2025

4. Cybersecurity and AI: The challenges and opportunities [Электронный ресурс] – Режим доступа: https://www.weforum.org/agenda/2023/06/cybersecurity-and-ai-challenges-opportunities/ – Дата доступа: 06.04.2025

5. The Power and Limitations of AI in Cybersecurity [Электронный ресурс] – Режим доступа: https://www.fortinet.com/blog/ciso-collective/power-and-limitations-of-ai-in-cybersecurity – Дата доступа: 06.04.2025