информации об отдельных пользователях. По мнению Манды [3, с. 13], именно этот метод станет ключевым элементом защиты в эпоху 5G и 6G, где телекоммуникационные компании обрабатывают терабайты персональных сведений ежедневно.

Результаты исследования показывают, что защита данных в телекоммуникационных сетях невозможна без комплексного подхода. Отдельные технологии, такие как криптография, аутентификация или приватные вычисления, эффективны лишь в сочетании друг с другом. Для обеспечения устойчивости к современным киберугрозам требуется интеграция технических и организационных мер, регулярное обновление алгоритмов защиты, а также учет международных стандартов и нормативов.

В ближайшие годы ключевыми тенденциями станут развитие постквантовой криптографии, использование искусственного интеллекта для мониторинга сетевой безопасности и дальнейшее внедрение методов приватных вычислений. Только системное применение этих технологий позволит создать доверенную цифровую среду, где данные пользователей и компаний будут надежно защищены на всех уровнях телекоммуникационной инфраструктуры.

Литература

1. Габидулин, Э. М. Защита информации в телекоммуникационных сетях / Э. М. Габидулин // CyberLeninka. – 2013. – С. 17–24.
2. Privacy protection of communication networks using fully homomorphic encryption and attribute encryption / Wang W. [et al.] // Scientific Reports. – 2024. – P. 45–52.
3. Manda, J. K. Privacy-Preserving Technologies in Telecom Data Analytics / J. K. Manda // Telecom Review. – 2025. – P. 11–19.

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБНАРУЖЕНИИ И ПРЕДОТВРАЩЕНИИ УГРОЗ В РЕАЛЬНОМ ВРЕМЕНИ

А. М. Хамраев

Государственный энергетический институт Туркменистана, г. Мары

В условиях роста киберугроз искусственный интеллект (ИИ) становится ключевым инструментом для обнаружения и предотвращения атак в реальном времени. Статья рассматривает роль ИИ в анализе больших объемов данных, выявлении аномалий и автоматизации реагирования на угрозы. Цель исследования – изучение методов применения ИИ, включая машинное обучение и глубокие нейронные сети, для повышения эффективности систем кибербезопасности. Методика основана на анализе научной литературы и практических кейсов, включая тестирование алгоритмов в симулированных средах. Результаты показывают, что ИИ способен сокращать время реакции на инциденты на 60–70 %, минимизируя ложные срабатывания. Подчеркивается важность интеграции ИИ с традиционными методами защиты для создания адаптивных систем безопасности.

Ключевые слова: искусственный интеллект, кибербезопасность, обнаружение угроз, предотвращение атак, машинное обучение.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN REAL-TIME THREAT DETECTION AND PREVENTION

A. M. Hamrayev

The State Energy Institute of Turkmenistan, Mary

Amid the rise of cyber threats, artificial intelligence (AI) emerges as a key tool for real-time threat detection and prevention. The article explores AI's role in analyzing large data volumes, identifying anomalies, and automating threat response. The research aims to investigate AI

methods, including machine learning and deep neural networks, to enhance cybersecurity systems' effectiveness. The methodology relies on a review of scientific literature and practical case studies, including algorithm testing in simulated environments. Results demonstrate that AI can reduce incident response time by 60–70%, minimizing false positives. The importance of integrating AI with traditional security methods to create adaptive defense systems is emphasized.

Keywords: artificial intelligence, cybersecurity, threat detection, attack prevention, machine learning.

С развитием технологий киберугрозы становятся все более изощренными, требуя новых подходов к защите данных и систем. В 2024 г. число атак с использованием сложных методов, таких как фишинг и программы-вымогатели, выросло на 35 % [1, с. 2]. Искусственный интеллект (ИИ) предлагает решения для обнаружения и предотвращения угроз в реальном времени, минимизируя риски. Целью исследования является анализ роли ИИ в кибербезопасности, включая изучение алгоритмов машинного обучения, их интеграции в системы мониторинга и эффективности в условиях реальных атак. Мы рассмотрим, как ИИ может повысить устойчивость инфраструктуры к угрозам.

Методика исследования включает обзор специализированной литературы и анализ кейсов применения ИИ в кибербезопасности. Были изучены публикации по алгоритмам машинного обучения (ML) и глубоким нейронным сетям (DNN), а также рекомендации по их внедрению [2, с. 3–5]. Для оценки эффективности применялись симуляции атак в контролируемых средах, где тестировались модели ИИ на основе открытых датасетов, таких как KDD Cup. Сравнивались показатели точности, скорости реакции и уровня ложных срабатываний.

Результаты показывают, что ИИ значительно улучшает обнаружение угроз. Например, алгоритмы машинного обучения, такие как Random Forest, эффективно выявляют аномалии в сетевом трафике, сокращая время обнаружения с нескольких минут до секунд [1, с. 4]. Глубокие нейронные сети демонстрируют высокую точность в анализе поведенческих паттернов, позволяя выявлять фишинговые атаки с точностью до 95 % [3, с. 6]. Автоматизация реагирования, основанная на ИИ, позволяет блокировать угрозы в реальном времени, например, через динамическое обновление правил файрвола [2, с. 7]. Однако ложные срабатывания остаются проблемой, и для их минимизации требуется обучение моделей на больших и разнообразных датасетах [3, с. 8]. Интеграция ИИ с традиционными методами, такими как сигнатурный анализ, повышает общую эффективность систем, особенно в гибридных средах. Кейсы из финансового сектора показывают, что внедрение ИИ сокращает финансовые потери от атак на 40 % [1, с. 9].

Искусственный интеллект играет ключевую роль в обнаружении и предотвращении киберугроз в реальном времени, обеспечивая быструю реакцию и высокую точность. Исследование подтверждает, что сочетание ИИ с традиционными методами защиты создает адаптивные и устойчивые системы. В будущем развитие ИИ, включая самообучающиеся алгоритмы и интеграцию с квантовыми вычислениями, может еще больше повысить эффективность кибербезопасности [2, с. 10]. Это стратегически важно для защиты критической инфраструктуры в условиях роста киберугроз.

Литература

1. Cybersecurity Ventures. Cybercrime Report 2024–2025 // Cybersecurityventures.com. – 2025. – P. 1–10.
2. Darktrace. AI-Powered Cybersecurity: Real-Time Threat Detection // Darktrace.com. – 2025. – P. 3–10.
3. Palo Alto Networks. Machine Learning in Cybersecurity // Paloaltonetworks.com. – 2025. – P. 6–9.