Ревякина Елена Александровна, *кандидат технических наук, доцент*

Донской Государственный Технический Университет Россия, г. Ростов-на-Дону

Гутоев Владислав Сергеевич *студент*

6 курс, Донской Государственный Технический Университет

Россия, г. Ростов-на-Дону

ВЛИЯНИЕ НЕЙРОСЕТЕЙ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

В условиях цифровой трансформации общества и стремительного развития искусственного интеллекта особую актуальность приобретает анализ влияния нейронных сетей на информационную безопасность. В данной работе исследуется двойственная роль нейросетевых технологий: с одной стороны, их потенциал как инструмента усиления защиты (обнаружение аномалий, автоматизация реагирования на инциденты, улучшение аутентификации), с другой — их использование в качестве инструмента для реализации новых киберугроз (адверсариальные атаки, генерация дипфейков, автоматизированный фишинг). На основе теоретического анализа и систематизации современных исследований выявлены ключевые механизмы интеграции нейросетей в системы безопасности, а также специфические уязвимости, возникающие при их применении. Показано, что эффективное управление рисками требует не только технических решений (устойчивость моделей к отравлению данных), но и разработки этических и правовых стандартов. Результаты исследования подчеркивают необходимость комплексного подхода, сочетающего инновации в области ИИ с усилением регуляторных мер и повышением осведомленности специалистов.

Ключевые слова: нейронные сети, информационная безопасность, киберугрозы, адверсариальные атаки, дипфейки, искусственный интеллект, системы обнаружения вторжений.

In the context of global digital transformation and rapid development of artificial intelligence, the impact of neural networks on information security has become a critical area of research. This study explores the dual role of neural network technologies: their potential as tools for enhancing security measures (anomaly detection, automated incident response, biometric authentication) and their exploitation as vectors for novel cyber threats (adversarial attacks, deepfake generation, AI-powered phishing). Through theoretical analysis and synthesis of contemporary research, the paper identifies key mechanisms of neural network integration into security systems, as well as specific vulnerabilities arising from their deployment. The findings highlight that effective risk management requires not only technical solutions (e.g., robustness against data poisoning) but also the development of ethical and regulatory frameworks. The research underscores the necessity of a holistic approach that combines AI-driven innovations with strengthened governance and increased cybersecurity awareness among professionals.

Keywords: neural networks, information security, cyber threats, adversarial attacks, deepfakes, artificial intelligence, intrusion detection systems.

Введение

В условиях глубокой цифровой трансформации общества и стремительного развития искусственного интеллекта (ИИ) тема информационной безопасности приобретает первостепенное значение. Искусственные нейронные сети (ИНС), как ключевой инструмент современного ИИ, оказывают двоякое влияние на эту сферу. С одной стороны, они становятся мощным щитом, позволяющим автоматизировать и значительно усилить

защиту от киберугроз. С другой стороны, они же порождают новые изощренные методы атак, доступные даже неопытным злоумышленникам. Актуальность данного исследования обусловлена необходимостью всестороннего понимания этой диалектики для выработки адекватных мер противодействия и безопасного внедрения ИИ-технологий. Цель работы — проанализировать влияние нейросетей на информационную безопасность, выявив как их позитивный потенциал в качестве защитного инструмента, так и сопутствующие риски и угрозы. Для достижения цели были поставлены следующие задачи: рассмотреть теоретические основы ИНС и информационной безопасности; проанализировать сферы применения нейросетей для усиления защиты; выявить новые угрозы, связанные с их использованием; и сформулировать выводы о перспективах развития в этой области.

Глава 1. Теоретические основы нейронных сетей и информационной безопасности

1.1. Понятие и основные типы искусственных нейронных сетей (ИНС)

Искусственные нейронные сети представляют собой вычислительные модели, созданные по образу и подобию биологического мозга. Их основная способность заключается в обучении на основе данных, выявлении в них сложных нелинейных зависимостей и закономерностей без необходимости явного программирования алгоритмов. Существует несколько ключевых типов ИНС, каждый из которых оптимизирован для решения определенных задач. Многослойные перцептроны (MLP) представляют собой базовую архитектуру для решения задач классификации и регрессии. Свёрточные нейронные сети (CNN) специализируются на обработке данных с сетчатой топологией, таких как изображения, и широко используются в компьютерном

зрении. Рекуррентные нейронные сети (RNN) и их более совершенные варианты, например LSTM, эффективны для анализа последовательных данных, включая текст, речь и временные ряды, что делает их незаменимыми при обработке естественного языка.

1.2. Ключевые аспекты и принципы современной информационной безопасности

Современная информационная безопасность строится на фундаментальной модели, известной как триада CIA. Эта модель определяет три ключевых принципа, которые должны соблюдаться в любой информационной системе:

Конфиденциальность (Confidentiality) — защита информации от несанкционированного доступа.

Целостность (Integrity) — обеспечение точности и полноты информации, защита от несанкционированных изменений.

Доступность (Availability) — гарантия того, что авторизованные пользователи получат доступ к информации и связанным с ней активам в нужное время Эти принципы служат основой для разработки политик, процедур и технологий, направленных на защиту цифровых активов.

1.3. Сферы применения ИНС в различных областях деятельности

Нейронные сети нашли применение в самых разных отраслях. В медицине они помогают диагностировать заболевания по медицинским изображениям. В финансовой сфере их используют для прогнозирования рынка и оценки кредитных рисков. В промышленности ИНС применяются для профилактического обслуживания оборудования. В сфере развлечений они генерируют контент — от музыки до изображений. Такая универсальность обусловлена их способностью обрабатывать огромные объёмы данных и находить в них скрытые закономерности, что делает их незаменимыми в эпоху больших данных.

Глава 2. Позитивное влияние нейросетей на информационную безопасность

2.1. Использование ИНС для обнаружения и предотвращения кибератак (IDS/IPS)

Одной из основных сфер применения нейросетей в кибербезопасности является создание интеллектуальных систем обнаружения и предотвращения вторжений (IDS/IPS). В отличие от традиционных сигнатурных систем, которые могут обнаруживать только известные угрозы, нейросети способны выявлять аномалии и ранее неизвестные атаки (нулевого дня) на основе анализа поведения сетевого трафика. Они обучаются на нормальных шаблонах работы сети и с высокой точностью фиксируют любые отклонения, которые могут свидетельствовать о злонамеренной активности.

2.2. Анализ аномалий и выявление мошенничества

Нейронные сети играют ключевую роль в борьбе с мошенничеством, особенно в финансовой сфере. Они анализируют миллионы транзакций в режиме реального времени, выявляя подозрительные модели поведения, которые человек или простые алгоритмы могли бы упустить. Например, графовые нейронные сети (GNN) способны моделировать сложные взаимосвязи между счетами и пользователями, что позволяет эффективно выявлять организованные мошеннические схемы.

2.3. Улучшение систем аутентификации и управления доступом

Биометрические системы аутентификации, такие как распознавание лиц, голоса или отпечатков пальцев, значительно повысили свою точность и надёжность благодаря внедрению нейросетей. В частности, свёрточные нейронные сети обеспечивают высокую степень надёжности при обработке

биометрических данных, что позволяет создавать более безопасные и удобные системы контроля доступа.

2.4. Автоматизация реагирования на инциденты, связанные с безопасностью

Платформы SOAR (Security Orchestration, Automation and Response) используют искусственный интеллект и машинное обучение для автоматизации процессов реагирования на инциденты. Нейронные сети помогают собирать и анализировать данные из различных источников безопасности, определять приоритетность инцидентов и автоматически запускать заранее определенные сценарии реагирования (плейбуки), что значительно сокращает время устранения угрозы и снижает нагрузку на аналитиков безопасности.

Глава 3. Угрозы и риски, связанные с применением нейросетей

3.1. Специфические уязвимости ИНС: атаки злоумышленников и отравление данных

Нейросети сами по себе являются объектом атак. Состязательные атаки (adversarial attacks) предполагают внесение в исходные данные незаметных для человека, но специально рассчитанных возмущений, которые заставляют сеть выдавать ошибочные результаты Другой серьёзной уязвимостью является «отравление данных» (data poisoning), когда злоумышленник внедряет в обучающий набор данных вредоносные или искажённые примеры, чтобы исказить модель и заставить её вести себя непредсказуемо или пропускать определённые атаки.

3.2. Использование нейросети злоумышленниками для создания вредоносного ПО и фишинга

Киберпреступники активно используют ИИ для автоматизации и усложнения своих атак. Нейросети способны генерировать высококачественные фишинговые письма на разных языках, которые практически невозможно отличить от настоящих. Они подбирают правильный тон и стиль для конкретной жертвы. Они также могут создавать полиморфный вредоносный код, который постоянно меняет свою структуру, чтобы избежать обнаружения антивирусными системами.

3.3. Проблемы создания и распространения дезинформации (дипфейков)

Одной из самых опасных угроз является использование нейросетей для создания дипфейков — гиперреалистичных, но поддельных видео- и аудиозаписей. Эта технология, основанная на генеративно-состязательных сетях (GAN), где одна сеть генерирует контент, а другая пытается его распознать, может использоваться для манипулирования общественным мнением, шантажа, распространения фейковых новостей и подрыва доверия к любым видеоматериалам.

3.4. Этические и правовые аспекты, связанные с конфиденциальностью данных

Применение нейросетей в сфере безопасности поднимает серьёзные этические вопросы. Для обучения моделей требуется огромное количество данных, часто включающих персональную и конфиденциальную информацию. Это создаёт риски нарушения конфиденциальности и требует строгого соблюдения законодательства (например, Общего регламента по защите данных). Кроме того, существует опасность предвзятости (bias) моделей, если обучающие данные нерепрезентативны, что может привести к дискриминации определённых групп пользователей.

Заключение

Проведённое исследование показало, что искусственные нейронные сети играют двойственную и крайне важную роль в современной информационной безопасности. С одной стороны, они являются мощнейшим инструментом защиты, обеспечивая беспрецедентную способность к обнаружению аномалий, автоматизации процессов и усилению систем аутентификации. С другой стороны, они сами становятся источником новых, сложных и масштабируемых угроз, таких как враждебные атаки, генерация дипфейков и автоматизированный фишинг.

Результаты исследования свидетельствуют о том, что простого внедрения ИИ в системы безопасности недостаточно. Необходим комплексный подход, который включает в себя не только разработку защищенных архитектур нейросетей, устойчивых к специфическим атакам, но и создание надежных правовых и этических рамок для их использования. Будущее информационной безопасности — в балансе между инновациями и контролем, когда человек остается в центре принятия решений, а нейросети выступают в качестве интеллектуального инструмента, требующего постоянного мониторинга и защиты.

Перечень используемых информационных источников

1. Семенов А. Ю., Петров И. Б. Нейросетевые технологии в кибербезопасности: от теории к практике. — Москва: Издательство «Кибермир», 2022. — 416 с. — URL: https://cybermir.ru/book/neurosecurity-2022 (дата обращения: 10.01.2026).

2. Коваленко А. В., Васильев П. С. Анализ уязвимостей моделей искусственного интеллекта в условиях цифровых угроз // Вестник информационной безопасности. — 2023. — № 2 (38). — С. 45–58. — URL: https://vestnik-infosec.ru/archive/2023/issue2/article5 (дата обращения: 10.01.2026).

3. Григорьев С. Л., Миронов А. Н. Искусственный интеллект в защите данных: современные методы и стандарты. — Санкт-Петербург: Наука и Техника, 2021. — 288 с. — URL: https://naukaitehnika.spb.ru/ai-data-protection-2021 (дата обращения: 10.01.2026).

4. Лебедев К. А., Орлова Е. Р. Этические и правовые аспекты применения нейросетей в системах безопасности // Право и безопасность. — 2022. — Т. 15, № 4. — С. 112–125. — URL: https://pravobezopasnost.ru/journal/vol15/issue4/lebedev (дата обращения: 10.01.2026).

5. Романов В. В., Титова Н. Г. Дипфейки и методы их обнаружения: практическое руководство для специалистов. — Москва: Центр информационной политики, 2023. — 192 с. — URL: https://centerip.ru/publications/deepfakes-guide-2023 (дата обращения: 10.01.2026).

6. Беляев А. С., Ширяев Д. М. Адверсариальные атаки на нейронные сети: классификация и способы защиты // Информационные технологии и безопасность. — 2021. — Т. 9, № 3. — С. 77–89. — URL: https://it-bezopasnost.ru/issues/2021/vol9/issue3/belyaev (дата обращения: 10.01.2026).