УДК 004.891:620.9

Вассунова Юлия Юрьевна, доцент кафедры теоретические основы электротехники, Казанский Государственный Энергетический Университет, г. Казань

Зинатуллин Альберт Раифович, бакалавр, Казанский Государственный Энергетический Университет, г. Казань

ЭТИКА И БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ AI В ЭНЕРГЕТИКЕ: Р ИСКИ И МЕРЫ ПРЕДОСТОРОЖНОСТИ

Аннотация

В статье рассматриваются этические и безопасностные проблемы внедрения ис кусственного интеллекта (AI) в энергетическую отрасль. Анализируются ключе вые сферы его применения: прогнозирование спроса, оптимизация энергосетей, управление возобновляемыми источниками энергии, предиктивное обслужива ние и кибербезопасность.

Выявляются основные риски: непрозрачность AI-алгоритмов, неопределённост ь ответственности за ошибки, угроза усиления социального неравенства, риски утечки данных и сокращения рабочих мест из-за автоматизации. Среди опаснос тей безопасности выделены уязвимость к кибератакам (включая data poisoning и adversarial attacks), чрезмерная зависимость от автоматизированных решений и последствия ошибок в исходных данных.

Предлагаются меры предосторожности: повышение прозрачности алгоритмов, разработка отраслевых стандартов и законодательной базы, усиление киберзащ иты, резервирование систем, обучение персонала и этический аудит. Подчёркив ается необходимость сбалансированного подхода, сочетающего инновации с эт ическими нормами и мерами безопасности.

Annotation

The article discusses the ethical and safety issues of introducing artificial intelligence (AI) in the energy industry. It analyzes the key areas of its application: demand forecasting, energy grid optimization, renewable energy management, predictive maintenance, and cybersecurity.

The main risks are identified: the opacity of AI algorithms, the uncertainty of liability for errors, the threat of increasing social inequality, the risks of data leakage, and the reduction of jobs due to automation. Among the security hazards, vulnerability to cyberattacks (including data poisoning and adversarial attacks) is highlighted, as well as excessive dependence on automated solutions and the consequences of errors in the source data.

Precautions are proposed, such as increasing the transparency of algorithms, developing industry standards and legal frameworks, strengthening cyber protection, system redundancy, staff training, and ethical auditing. The need for a balanced approach is emphasized.

Ключевые слова: искусственный интеллект (AI), энергетика, этика технологий, безопасность AI-систем, кибербезопасность, непрозрачность алгоритмов, ответственность за ошибки AI.

Keywords: artificial intelligence (AI), energy, technology ethics, AI system security, cybersecurity, algorithm opacity, and responsibility for AI errors.

Искусственный интеллект (AI) всё активнее внедряется в энергетическую отрасль — от прогнозирования спроса и оптимизации работы электросетей до управления возобновляемыми источниками энергии и предотвращения аварий. Вместе с преимуществами появляются серьёзные вызовы: этические дилеммы, риски безопасности, угрозы конфиденциальности данных. Цель этой статьи — проанализировать ключевые риски использования AI в энергетике и предложить меры предосторожности, которые помогут минимизировать негативные последствия.

Прежде чем говорить о рисках, важно понять, где именно используется AI. В сфере прогнозирования спроса и нагрузки искусственный интеллект

анализирует исторические данные и погодные условия, чтобы предсказать потребление энергии. В оптимизации работы энергосетей интеллектуальные системы балансируют нагрузку, предотвращают перегрузки и снижают потери. При управлении возобновляемыми источниками энергии (ВИЭ) AI помогает интегрировать солнечные и ветряные электростанции в общую сеть, учитывая их нестабильность. В диагностике и предиктивном обслуживании датчики и алгоритмы выявляют неисправности оборудования до того, как они приведут к аварии. Автоматизация распределительных сетей с помощью умных сетей (Smart Grids) позволяет самостоятельно реагировать на изменения, минимизируя участие человека. Кроме того, AI активно задействуется в сфере кибербезопасности: он обнаруживает аномалии в сетевом трафике и предотвращает кибератаки.

Рассмотрим этические риски использования AI в энергетике. Один из ключевых вопросов — прозрачность и объяснимость решений. Многие алгоритмы AI, особенно глубокие нейронные сети, работают как «чёрные ящики»: даже разработчики не всегда могут объяснить, почему система приняла то или иное решение. В энергетике это особенно критично: если AI отключит часть сети, необходимо понимать причину, чтобы избежать повторения ошибок в будущем.

Не менее важен вопрос ответственности за ошибки. Кто несёт ответственность, если AI-система допустила ошибку, приведшую к аварии или отключению электроэнергии? Производитель программного обеспечения, оператор сети или владелец инфраструктуры? На данный момент чёткого регулирования в этой сфере пока нет.

Ещё одна проблема связана с возможным усилением дискриминации и социального неравенства. AI может неосознанно способствовать неравенству: например, если система оптимизирует энергоснабжение только для «выгодных» районов, оставляя без должного внимания отдалённые или бедные регионы.

Конфиденциальность данных также вызывает серьёзные опасения. Для эффективной работы AI требуются огромные массивы данных, в том числе информация о потреблении энергии отдельными домохозяйствами. Утечка таких данных может привести к серьёзному нарушению приватности граждан.

Кроме того, внедрение AI оказывает влияние на рынок труда. Автоматизация способна сократить рабочие места в энергетике, особенно среди операторов и техников. Это ставит перед обществом задачу разработки программ переквалификации и социальной поддержки для затронутых групп работников.

Перейдём к рискам безопасности. Одной из наиболее серьёзных угроз являются кибератаки на AI-системы. Злоумышленники могут внедрить вредоносные данные для «отравления» модели (data poisoning), обмануть алгоритм, подавая искажённые входные данные (adversarial attacks), или перехватить управление через уязвимости в программном обеспечении.

Чрезмерная зависимость от AI также представляет опасность. Высокая степень автоматизации снижает способность операторов принимать решения в критических ситуациях. Если система даст сбой, персонал может оказаться не готов к ручному управлению, что усугубит последствия аварии.

Ошибки в исходных данных, например неверные показания датчиков, могут привести к каскадным отказам в энергосети. Это подчёркивает важность качества информации, на которой обучаются и работают AI-алгоритмы.

Физические угрозы тоже нельзя игнорировать. Повреждение датчиков или инфраструктуры, от которой зависит работа AI, может парализовать всю систему и вызвать масштабные сбои в энергоснабжении.

Какие же меры предосторожности могут снизить эти риски? Прежде всего, необходимо повысить прозрачность и объяснимость AI. Для этого целесообразно использовать алгоритмы с интерпретируемыми результатами — например, деревья решений вместо сложных нейросетей там, где это возможно. Также стоит внедрять стандарты объяснимого AI (XAI —

eXplainable AI), которые требуют от разработчиков документировать логику работы систем.

Законодательное регулирование играет не менее важную роль. Необходимо разработать чёткие правила ответственности за ошибки AI, создать отраслевые стандарты безопасности и сертификации для AI-решений в энергетике, а также ввести обязательные требования к тестированию систем перед их внедрением.

Защита данных и кибербезопасность должны обеспечиваться комплексом мер: шифрованием данных на всех этапах передачи и хранения, многофакторной аутентификацией для доступа к критическим системам, регулярным тестированием на проникновение (penetration testing), а также использованием AI для обнаружения аномалий в сетевом трафике.

Для повышения устойчивости систем важно предусмотреть резервирование и отказоустойчивость. Дублирование критически важных систем с возможностью ручного управления и создание «аварийных» алгоритмов, которые активируются при сбое основного AI, помогут минимизировать последствия возможных сбоев.

Обучение персонала — ещё один ключевой элемент безопасности. Тренинги для операторов по работе с AI-системами и действиям в чрезвычайных ситуациях, а также программы переквалификации для сотрудников, чьи должности могут быть автоматизированы, позволят адаптировать человеческий ресурс к новым условиям.

Этические комитеты и аудит помогут контролировать влияние AI на общество. Создание независимых комиссий для оценки последствий внедрения технологий и регулярный аудит алгоритмов на предмет дискриминации и предвзятости станут важными шагами к справедливому использованию AI.

Международное сотрудничество также имеет большое значение, поскольку энергетика — глобальная отрасль. Обмен опытом в области безопасности AI и разработка единых международных стандартов, например

под эгидой МАГАТЭ или МЭА, позволят повысить общую надёжность и устойчивость энергетических систем.

Перед внедрением AI в реальную энергосеть необходимо проводить тщательное тестирование в контролируемых условиях. Симуляции на цифровых двойниках (digital twins) и моделирование экстремальных сценариев, таких как стихийные бедствия или кибератаки, помогут выявить слабые места и улучшить надёжность системы.

В заключение отметим, что AI обладает огромным потенциалом для энергетики: он повышает эффективность, снижает затраты и помогает перейти к устойчивому развитию. Однако его внедрение требует взвешенного подхода. Ключевые принципы безопасного и этичного использования AI в энергетике включают прозрачность (алгоритмы должны быть объяснимы), ответственность (чёткое распределение зон ответственности), безопасность (защита от киберугроз и физических сбоев), социальную справедливость (учёт интересов всех групп населения) и адаптивность (готовность к изменениям на рынке труда). Только комплексный подход, сочетающий технологические инновации, законодательные меры и этические нормы, позволит реализовать преимущества AI без ущерба для общества и инфраструктуры. Будущее энергетики зависит не только от мощности алгоритмов, но и от того, насколько разумно и ответственно мы их применяем.

Литература

1. Алиев Р. А. Искусственный интеллект как новый фактор энергетической безопасности // Проблемы постсоветского пространства. 2025. Т. 12, № 1. С. 30–48. DOI: 10.24975/2313-8920-2025-12-1-30-48. e-cis.info +1
2. Ведомство Минэнерго РФ. Энергетическая стратегия Российской Федерации на период до 2035 года. Утв. Распоряжением Правительства РФ от 09.06.2020 г. № 1523-р. URL: (дата обращения: 2026-04-02).

3. Кочеров Д. С., Сидоров Д. Н. Применение методов машинного обучения для прогнозирования выработки солнечных электростанций // Известия РАН. Энергетика. 2021. № 4. С. 68–80.
4. Кравченко В. В., Хамицкая В. И. Инновационное применение искусственного интеллекта в энергетике // Белорусский национальный технический университет. 2024. С. 32–35.
5. Лизикова М. С. Искусственный интеллект в ядерной энергетике: применение и регулирование // В кн.: Могелевский С. Д. и др. (ред.) Закон и бизнес: Правовое пространство для развития бизнеса в России. М.: Проспект, 2020. С. 131–139.
6. Рубцова Л. Э. Этика искусственного интеллекта: вызовы и решения // Актуальные исследования. 2025. № 3 (238). Ч. I. С. 95–97. URL: (дата обращения: 2026-04-02).

Literature

1. Aliev, R. A. (2025). Artificial intelligence as a new factor in energy security. Problems of the Post-Soviet Space, 12(1), pp. 30–48. DOI: 10.24975/2313-8920-2025-12-1-30-48.
2. Energy Strategy of the Russian Federation for the Period up to 2035 (2020). Approved by Decree No. 1523-r of the Government of the Russian Federation dated 09.06.2020. Available at: (Accessed: 02.04.2026).
3. Kocherov, D. S., Sidorov, D. N. (2021). Application of machine learning methods for forecasting solar power plant output. Proceedings of the RAS. Energy, (4), pp. 68–80.
4. Kravchenko, V. V., Khamitskaya, V. I. (2024). Innovative application of artificial intelligence in energy. Belarusian National Technical University, pp. 32–35.
5. Lizikova, M. S. (2020). Artificial intelligence in nuclear energy: application and regulation. In: Mogelevsky, S. D. et al. (eds.) Law and Business: Legal Space for Business Development in Russia. Moscow: Prospekt, pp. 131–139.

6. Rubtsova, L. E. (2025). Ethics of artificial intelligence: challenges and solutions. Actual Research, 3(238), Part I, pp. 95–
97. Available at: (Accessed: 02.04.2026).