

Д. Н. Титов^{1✉}, Е. В. Рыжкова¹

Применение ИИ в интернете вещей

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: alena.tarasova.2014@mail.ru

Аннотация: В статье рассматриваются современные подходы к применению периферийных вычислений и искусственного интеллекта (ИИ) в рамках концепции Интернета энергии (IoE), как одного из направлений развития Интернета вещей (IoT). Рассматриваются возможности применения периферийного искусственного интеллекта в системах IoE. Анализируются преимущества локальной обработки данных для повышения энергоэффективности, снижения задержек, обеспечения безопасности и автономного управления. Особое внимание уделено угрозам информационной безопасности и ограничениям периферийных устройств в IoT-среде [1–5].

Ключевые слова: Интернет вещей (IoT), Интернет энергии (IoE), периферийные вычисления, искусственный интеллект, информационная безопасность

E. V. Ryzhkova^{1✉}, D. N. Titov¹

Application of AI in the Internet of things

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: alena.tarasova.2014@mail.ru

Abstract. The article discusses modern approaches to the use of edge computing and artificial intelligence (AI) within the concept of the Internet of Energy (IoE), as one of the areas of development of the Internet of Things (IoT). The possibilities of using edge artificial intelligence in IoE systems are considered. The advantages of local data processing for increasing energy efficiency, reducing latency, ensuring security and autonomous control are analyzed. Particular attention is paid to information security threats and limitations of edge devices in the IoT environment [1–5].

Keywords: Internet of Things (IoT), Internet of Energy (IoE), edge computing, artificial intelligence, information security

Введение

Сегодня повышается актуальность разработки инновационных решений для снижения уровней выбросов углекислого газа. Информационно-коммуникационные технологии (ИКТ), особенно в сфере повышения энергоэффективности, становятся важным инструментом в достижении этих целей [6–8].

Одним из актуальных направлений является использование периферийных вычислений – альтернативы традиционным облачным системам. Данные технологии позволяют более эффективно контролировать энергопотребление в зданиях. Сложные интеллектуальные системы, основанные на концепциях Интернета вещей (IoT) и алгоритмах искусственного интеллекта (ИИ), позволяют формировать так называемый Интернет энергии (IoE) – распределенную цифровую

среду, в которой все элементы энергосистемы (потребители, производители, аккумуляторы, устройства учета и контроля) объединены в единую сеть. Данная сеть, позволяет анализировать и регулировать потребление энергии в реальном времени [9–13]. Применение Интернета энергии способствует интеграции возобновляемых источников энергии в энергосеть, что, в свою очередь, влияет на осознанность потребителей, которая повышается через их информированность.

ИИ помогает контролировать потребление энергии, обнаруживать аномалии и прогнозировать неисправности, используя большие данные для принятия решений. Хотя облачные технологии широко применяются в целях энергоэффективности, они не лишены недостатков – в частности, требуют значительных ресурсов и могут способствовать дополнительной нагрузке на сеть. В этом плане применение периферийного ИИ позволит снизить задержки, осуществит оптимизацию обработки данных и тем самым уменьшит энергозатраты [14–16].

Методы и материалы

Современные методы контроля энергопотребления и оптимизации эксплуатационных затрат используют облачные технологии, которые требуют высокой вычислительной мощности [17].

Однако, с развитием технологий 5G и распространением IoT-устройств возникает возможность перераспределения нагрузки, благодаря чему локальная обработка данных снижает зависимость от энергоемких центров обработки информации и повышает устойчивость систем к внешним воздействиям. Все вышеперечисленное способствует не только ускорению обработки данных и принятию решений, но и позволяет повысить уровень безопасности.

Периферийные вычисления ускоряют анализ информации за счет минимизации расстояния между источником данных и процессором, это не только повышает производительность, но и увеличивает надежность, особенно в критических ситуациях, когда решение нужно принять в течение секунд. Таким образом, обработка на месте повышает уровень защиты, поскольку данные не покидают локальную сеть, что снижает вероятность их утечки [18].

Периферийные вычисления обеспечивают обработку данных непосредственно в месте их формирования, что существенно снижает задержки и позволяет оперативно реагировать на критические события без обращения к удаленным серверам. Данный способ особенно важен в производственной или технологической среде, где промедление может привести к сбоям. Локальная обработка данных позволяет уменьшить нагрузку на сеть и энергопотребление устройств за счет сокращения объема передаваемых данных. По мере роста числа IoT-устройств периферийный подход обеспечивает масштабируемость, позволяя исключить узкие места в системах. Кроме того, децентрализация повышает уровень информационной безопасности и конфиденциальности, а также способствует созданию автономных систем управления, принимающих решения на основе локальных данных [19–20].

Результаты

Вычисления на границе сети позволяют минимизировать задержки и повысить безопасность обработки данных, это важно для систем, работающих в режиме реального времени. В энергетике применение локальных ИИ-решений позволяет обеспечить эффективное управление потреблением: например, устройства автоматически переводят в спящий режим при отсутствии нагрузки.

Технологии мониторинга без вмешательства (NILM) позволяют точно отслеживать энергопотребление и оперативно выявлять аномалии, включая несанкционированное использование энергии. Такие подходы способствуют предотвращению потерь.

Периферийные вычисления также оптимизируют распределение энергии, перераспределяя нагрузку между сетевыми линиями и облегчая интеграцию возобновляемых источников в энергосистему, все это делает систему более гибкой и устойчивой к перегрузкам.

Локальная обработка данных также снижает риски утечек и усиливает защиту конфиденциальной информации. Однако перенос традиционных облачных механизмов безопасности на периферию затруднен из-за географического размещения устройств и их ограниченных ресурсов.

Однако необходимо рассмотреть и основные проблемы безопасности периферийных систем:

- уязвимость устройств из-за слабой аппаратной защиты;
- сложности в аутентификации и контроле доступа;
- проблемы управления доверием между разными участниками системы;
- необходимость регулярных обновлений ПО при ограниченных ресурсах.

Для эффективной защиты таких систем требуется учитывать специфику их архитектуры, ограниченные возможности вычислений и их сетевые особенности.

Заключение

Внедрение периферийных вычислений в энергетику демонстрирует высокий потенциал для повышения энергоэффективности, устойчивости и безопасности интеллектуальных систем. Обработка данных на месте их возникновения позволяет существенно сократить задержки, снизить нагрузку на сеть и минимизировать энергозатраты. При этом важно учитывать особенности архитектуры и ограниченные ресурсы периферийных устройств, что требует комплексного подхода к вопросам кибербезопасности. Развитие Интернета энергии и локальных ИИ-решений становится ключевым направлением цифровой трансформации энергетической отрасли.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Суомалайнен А., Интернет вещей: видео, аудио, коммутация: ДМК Пресс, 2019. – 122 с.
2. Santucci, G. The internet of things: Between the revolution of the internet and the metamorphosis of objects. Vision and Challenges for Realising the Internet of Things, 2010. – P. 11–24.
- 3) Мачей К., Интернет вещей новая технологическая революция: Эксмо, 2017. – 330.

- 4) Sardeshmukh, H., & Ambawade, D. Internet of Things: Existing protocols and technological challenges in security. In *Intelligent Computing and Control, 2017 International Conference on IEEE*. – Pp. 1–7.
- 5) Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. 2017. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84, 25–37.
- 6) Al-Gburi, A., Al-Hasnawi, A., & Lilien, L. Differentiating Security from Privacy in Internet of Things: A Survey of Selected Threats and Controls. In *Computer and Network Security Essentials*. Springer, Cham. 2018. – Pp. 153–172.
- 7) В. П. Мешалкин, А. Ю. Пучков, Е. И. Лобанева, М. И. Дли. Предварительная оценка прагматической ценности информации в задаче классификации на основе глубоких нейронных сетей // *Прикладная информатика*. – 2021. – Т. 16. № 3. – С. 9–20.
- 8) Krishna, B. S., & Gnanasekaran, T. A systematic study of security issues in Internet-of-Things (IoT). In *I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 International Conference on*. 2017, February. – Pp. 107–111.
- 9) Ramadhan, A. A survey of security aspects for Internet of Things in healthcare. In *Information Science and Applications (ICISA) 2016* (pp. 1237–1247). Springer, Singapore.
- 10) Varadarajan, P., & Crosby, G. Implementing IPsec in wireless sensor networks. In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on* (pp. 1–5). IEEE.
- 11) Sain, M., Kang, Y. J., & Lee, H. J. (2017, February). Survey on security in Internet of Things: State of the art and challenges. In *Advanced Communication Technology (ICACT), 2017 19th International Conference on* (pp. 699–704). IEEE.
- 12) Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, 4(5), 1250–1258.
- 13) Свон, Мелани. Блокчейн: схема новой экономики. – М.: «Олимп-бизнес», 2017. – 240 с. – ISBN 978-5-9693-0360-7.
- 14) P. Ocheja, B. Flanagan, H. Ueda, and H. Ogata, “Managing lifelong learning records through blockchain,” *Research and Practice in Technology Enhanced Learning*, vol. 14, no. 1, pp. 1–19, 2019.
- 15) J. Y. Chun and G. Noh, “Blockchain-based access control audit system for next generation learning management,” *KIPS Transactions on Software and Data Engineering*, vol. 9, no. 11, pp. 351–356, 2020.
- 16) M. Jirgensons and J. Kapenieks, “Blockchain and the future of digital learning credential assessment and management,” *Journal of Teacher Education for Sustainability*, vol. 20, no. 1, pp. 145 – 156, 01 Jun. 2018. <https://content.sciendo.com/view/journals/jtes/20/1/article-p145.xml>.
- 17) Колосок Ирина Николаевна, Коркина Елена Сергеевна Применение облачных и граничных технологий при развитии интеллектуальной энергосистемы // *Информационные и математические технологии в науке и управлении*. 2024. №4 (36). URL: <https://cyberleninka.ru/article/n/primenenie-oblachnyh-i-granichnyh-tehnologiy-pri-razvitii-intellektualnoy-energositemy> (дата обращения: 19.05.2025).
- 18) Adams and A. Blandford, “Security and online learning: to protect or prohibit,” in *Usability Evaluation of Online Learning Programs*, C. Ghaoui, Ed. UK: IDEA Publishing, March 2003, pp. 331–359.
- 19) Pedro Franco. *The Blockchain // Understanding Bitcoin: Cryptography, Engineering and Economics*. – John Wiley & Sons, 2014. – 288 p. – ISBN 978-1-119-01916-9.
- 20) Raval S. *Decentralized Applications. Harnessing Bitcoin's Blockchain Technology*. – 2016. – 118 с. – ISBN 978-1-491-92454-9.

© Д. Н. Тутов, Е. В. Рыжкова, 2025