

Алексіна Лариса Титівна*Державний університет інформаційно-комунікаційних технологій, Київ*

ORCID: 0009-0007-3842-8677

Зуб Людмила Миколаївна*Державний університет інформаційно-комунікаційних технологій, Київ*

ORCID: 0009-0005-6697-2683

Пронькін Олександр Васильович*Державний університет інформаційно-комунікаційних технологій, Київ*

ORCID: 0009-0004-8529-6919

Розмаїтий Дмитро Олегович*Державний університет інформаційно-комунікаційних технологій, Київ*

ORCID: 0009-0001-6385-8958

МОДЕЛЬ ВЗАЄМОДІЇ AI З ІОТ-ПРИСТРОЯМИ НА РІВНІ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Анотація. Сучасні IoT-системи складаються з мільйонів різномірних пристроїв, що потребують регулярних оновлень програмного забезпечення для підтримки функціональності та безпеки. Традиційні методи розгортання оновлень часто виявляються недостатньо гнучкими та ефективними, особливо в умовах динамічно змінюючихся мережних середовищ. У статті пропонується інноваційна модель взаємодії штучного інтелекту (AI) з IoT-пристроями на рівні оновлення ПЗ, яка поєднує переваги канаркових релізів з інтелектуальними алгоритмами оптимізації. Дослідження фокусується на розробці математичної моделі інтелектуального розгортання оновлень, що враховує такі ключові аспекти: поетапне впровадження змін (канаркові релізи), автоматизований моніторинг стабільності системи та адаптивне прийняття рішень на основі алгоритмів машинного навчання. Запропонована модель використовує методи навчання з підкріпленням (Reinforcement Learning) для динамічного вибору оптимальної стратегії розгортання, що дозволяє мінімізувати ризики збоїв і оптимізувати використання мережних ресурсів.

Особливу увагу приділено формалізації процесу розгортання за допомогою математичного апарату, що включає: визначення критеріїв успішності оновлення, функції витрат для оцінки якості розгортання та алгоритми прийняття рішень у реальному часі. Результати дослідження демонструють, що інтеграція AI у процес оновлення IoT-пристроїв дозволяє значно підвищити стабільність системи та зменшити кількість збоїв під час масштабних розгортань. У статті також розглядаються перспективні напрями подальших досліджень, зокрема: впровадження федеративного навчання для децентралізованого аналізу даних, інтеграція блокчейн-технологій для підвищення безпеки оновлень та розробка адаптивних алгоритмів для гетерогенних IoT-мереж. Запропонований підхід відкриває нові можливості для створення інтелектуальних, самокерованих IoT-систем, здатних ефективно функціонувати в умовах динамічно змінюючогося середовища.

Ключові слова: штучний інтелект, IoT, інформаційна система, оновлення програмного забезпечення, канаркові релізи, машинне навчання, розгортання оновлень, оптимізація мережі.

Aleksina Larysa

State university of information and communication technologies, Kyiv

ORCID: 0009-0007-3842-8677

Zub Liydmyla

State university of information and communication technologies, Kyiv

ORCID: 0009-0005-6697-2683

Pronkin Oleksandr

State university of information and communication technologies, Kyiv

ORCID: 0009-0004-8529-6919

Rozmaityi Dmytro

State university of information and communication technologies, Kyiv

ORCID: 0009-0001-6385-8958

MODEL OF AI INTERACTION WITH IOT DEVICES AT THE SOFTWARE UPDATE LEVEL

Abstract: *Modern IoT systems consist of millions of heterogeneous devices that require regular software updates to maintain functionality and security. Traditional methods of deploying updates are often insufficiently flexible and efficient, especially in dynamically changing network environments. This paper proposes an innovative model of interaction between artificial intelligence (AI) and IoT devices at the software update level that combines the advantages of canary releases with intelligent optimisation algorithms. The study focuses on the development of a mathematical model for intelligent update deployment that takes into account the following key aspects: phased implementation of changes (canary releases), automated monitoring of system stability, and adaptive decision-making based on machine learning algorithms. The proposed model uses Reinforcement Learning methods to dynamically select the optimal deployment strategy, which minimises the risk of failures and optimises the use of network resources.*

Particular attention is paid to the formalisation of the deployment process using a mathematical apparatus, including: the definition of criteria for successful updates, cost functions for assessing the quality of deployment, and real-time decision-making algorithms. The results of the study demonstrate that the integration of AI into the process of updating IoT devices can significantly improve system stability and reduce the number of failures during large-scale deployments. The article also discusses promising areas for further research, including the introduction of federated learning for decentralised data analysis, integration of blockchain technologies to improve update security, and development of adaptive algorithms for heterogeneous IoT networks. The proposed approach opens up new opportunities for the creation of intelligent, self-managed IoT systems capable of operating effectively in a dynamically changing environment.

Keywords: *artificial intelligence, IoT, information system, software updates, canary releases, machine learning, update deployment, network optimization.*

Постановка проблеми.

Сучасні IoT-мережі об'єднують мільйони різноманітних пристроїв, що працюють у динамічних умовах. Однією з ключових проблем є ефективне управління оновленнями програмного забезпечення, оскільки традиційні методи часто виявляються недостатньо гнучкими та безпечними. Особливі труднощі виникають при масштабних розгортаннях, де ризики збоїв із-за помилок у програмному забезпеченні значно зростають.

Інтеграція штучного інтелекту в процес оновлення IoT-пристроїв відкриває нові можливості для автоматизації та оптимізації. AI може аналізувати великі обсяги даних у реальному часі,

прогнозувати потенційні проблеми та адаптивно керувати процесом розгортання. Це дозволяє зменшити кількість збоїв і підвищити стабільність роботи всієї системи.

Актуальність дослідження полягає у необхідності розробки нових моделей взаємодії AI та IoT, які б забезпечували надійне та ефективне оновлення програмного забезпечення. Особливу увагу приділено поєднанню AI-алгоритмів із методом канаркових релізів, що дозволяє мінімізувати ризики за рахунок поступового впровадження змін.

Таким чином, основним завданням є розробка моделі, яка б інтегрувала AI для оптимізації процесу оновлення програмного забезпечення в IoT-мережах. Така модель має враховувати специфіку розподілених систем, забезпечувати безпеку та ефективність розгортання, а також адаптуватися до змін у мережному середовищі.

Мета і задачі дослідження.

Метою дослідження є розробка інтелектуальної AI-системи для оптимізації процесів оновлення програмного забезпечення в IoT-мережах. Основна увага спрямована на підвищення надійності розгортання оновлень, зменшення простоїв системи та раціональне використання ресурсів шляхом інтеграції машинного навчання з методологією канаркових релізів. Модель покликана автоматизувати прийняття рішень щодо стратегій розгортання, забезпечуючи стабільність роботи в гетерогенних IoT-мережах з різними характеристиками пристроїв.

До ключових завдань дослідження належать: аналіз існуючих механізмів оновлення IoT та їхніх обмежень; розробка AI-алгоритмів для прогнозування помилок і адаптивного планування розгортання; створення математичної моделі оцінки критеріїв успішності оновлень; впровадження прототипу системи для перевірки запропонованого підходу. Окремо досліджуються методи оптимізації використання мережної пропускну здатності під час масових оновлень та аспекти безпеки AI-керованих процесів у розподілених середовищах.

Результати дослідження.

Одним із перспективних підходів до оновлення IoT-пристроїв є поєднання канаркових релізів (canary releases) з AI-алгоритмами. Канарковий реліз - це техніка розгортання програмного забезпечення, при якій нова версія програми спочатку випускається для обмеженої групи користувачів перед повним розгортанням.

Основні особливості канаркових релізів:

- поступове розгортання: нова версія програми надається невеликій підгрупі користувачів;
- мінімізація ризиків: проблеми, якщо вони виникають, впливають тільки на невелику частину користувачів;
- раннє виявлення помилок: дозволяє виявити проблеми в реальному середовищі до повного розгортання;
- можливість швидкого відкату: у разі виявлення проблем, можна швидко відкотитися до попередньої версії.

Назва походить від практики шахтарів брати з собою в шахту канарку як систему раннього попередження про небезпечні гази. Аналогічно, канарі реліз служить "канаркою", виявляючи потенційні проблеми до масштабного розгортання.

Канаркові релізи (канаркове тестування) часто використовуються в DevOps, хмарних сервісах та веб-розробці, особливо компаніями, які практикують безперервну інтеграцію та доставку (CI/CD).

Для формалізації процесу розгортання оновлень запроваджується математична модель, яка дозволяє оптимізувати стратегію впровадження програмного забезпечення.

Канаркове розгортання передбачає поступове оновлення пристроїв за таким принципом:

Вибір пілотної групи:

Нехай N – загальна кількість IoT-пристроїв, а n – кількість пристроїв, які отримують оновлення першими.

Відношення $k = \frac{n}{N}$ визначає частку канаркового розгортання.

Оцінка стабільності:

Після оновлення n пристроїв система моніторингу вимірює показники:

Частка збоїв $f = \frac{\text{кількість пристроїв з помилками}}{n}$.

Продуктивність P (час відгуку, завантаження CPU тощо).

Критерій успішності:

Оновлення вважається стабільним, якщо:

$$f \leq f_{threshold} \text{ та } P \geq P_{min},$$

де $f_{threshold}$ – допустимий рівень збоїв, P_{min} – мінімально прийнятна продуктивність.

Якщо умови виконуються, оновлення поширюється на решту пристроїв.

Оптимізація розгортання за допомогою AI

AI-модель використовує методи навчання з підкріпленням (Reinforcement Learning, RL) для динамічного вибору оптимальної стратегії оновлення.

Модель RL:

Стан (State S_t): Поточний стан мережі (кількість оновлених пристроїв, рівень помилок, навантаження).

Дія (Action a_t): Рішення про те, чи продовжити розгортання ($a_t=1$), призупинити ($a_t = 0$) або відкотити оновлення ($a_t = -1$).

Витрати (Cost C): Функція витрат, що враховує:

$$C = \alpha \cdot f + \beta \cdot (1 - P) + \gamma \cdot \text{час розгортання},$$

де α, β, γ – вагові коефіцієнти.

Політика розгортання:

AI-агент навчається мінімізувати C , вибираючи оптимальну послідовність дій.

Формальна модель розгортання

Нехай:

- $U(t)$ – кількість оновлених пристроїв на кроці t .
- μ – інтенсивність виявлення помилок.

Тоді ймовірність успішного розгортання можна описати як:

$$P_{seccess} = 1 - e^{-\mu \cdot U(t)}.$$

Оптимальна стратегія полягає у виборі k (частки канаркового розгортання), що максимізує:

$$\min_k (P_{seccess} \cdot (1 - C)).$$

Запропонована математична модель дозволяє формалізувати процес інтелектуального розгортання оновлень у IoT-мережах. Використання AI для оптимізації канаркових релізів підвищує надійність системи та зменшує ризики масштабних збоїв.

Перспективи:

- Дослідження адаптивних алгоритмів для динамічного вибору k .
- Інтеграція федеративного навчання для децентралізованого аналізу даних.
- Впровадження моделей передбачуваного обслуговування (predictive maintenance) для IoT.

Висновки і перспективи подальших досліджень.

Дослідження показало, що інтеграція штучного інтелекту в процес оновлення ПЗ для IoT-пристроїв значно підвищує ефективність управління розгортанням. Запропонована модель, що

поєднує AI-алгоритми з методом канаркових релізів, дозволяє мінімізувати ризики збоїв та оптимізувати використання мережних ресурсів. Це відкриває нові можливості для створення стійких та самокерованих IoT-систем. Однак залишаються невирішеними питання, пов'язані з адаптацією моделі до гетерогенних IoT-мереж, де пристрої мають різні характеристики та обмеження. Перспективним напрямком є подальша розробка інтелектуальних алгоритмів, здатних враховувати специфіку різних типів пристроїв та умов їх роботи. Також потребує удосконалення механізм безпеки оновлень у розподілених системах.

У майбутньому розроблена модель може бути розширена шляхом додавання механізмів передбачуваного обслуговування (predictive maintenance) та адаптивного масштабування ресурсів. Це дозволить створювати ще більш інтелектуальні та автономні системи управління IoT-інфраструктурою, здатні ефективно функціонувати в умовах динамічно змінюючогося середовища.

Список використаної літератури

1. L. Bu, Y. Zhang, H. Liu, X. Yuan, J. Guo, and S. Han, "An IIoT-driven and AI-enabled framework for smart manufacturing system based on three-terminal collaborative platform," *Advanced Engineering Informatics*, 2021, doi: 10.1016/j.aei.2021.101370.
2. X. Lei, D. Huang, C. Zou, and Y. Zhuang, "Digital Technology - AI-IoT in Transformation of Industrial Manufacturing," in *Digital Transformation: Accelerating Organizational Intelligence: Volume 4: Digital Strategies and Organizational Transformation*, 2023. doi: 10.1142/9789811271984_0013.
3. P. Onu, A. Pradhan, and C. Mbohwa, "Potential to use metaverse for future teaching and learning," *Educ Inf Technol (Dordr)*, 2023, doi: 10.1007/s10639-023-12167-9.
4. Довженко, Т. П., Бондарчук А. П. "Аналіз сучасного етапу розвитку штучного інтелекту в телекомунікаціях." *Зв'язок 1* (2025): 43-48. Doi: 10.31673/2412-9070.2025.019552
5. Zhebka, V., Skladannyi, P., Bazak, Y., Bondarchuk, A., & Storchak, K. (2024). Methods for Predicting Failures in a Smart Home. In *Digital Economy Concepts and Technologies Workshop 2024* (Vol. 3665, pp. 70-78). Germany.
6. Чичкарьов, Євген, et al. "Виявлення мережесих вторгнень з використанням алгоритмів машинного навчання і нечіткої логіки." *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»* 3.19 (2023): 209-225. doi:10.28925/2663-4023.2023.19.209225
7. Hawkins, W. H., Hiser, J. D., & Davidson, J. W. (2016, April). Dynamic canary randomization for improved software security. In *Proceedings of the 11th Annual Cyber and Information Security Research Conference* (pp. 1-7).<https://doi.org/10.1145/2897795.2897803>
8. M. Andronie, G. Lăzăroiu, M. Iatagan, C. Uță, R. Ștefănescu, and M. Cocoșatu, "Artificial intelligence-based decision-making algorithms, internet of things sensing networks, and deep learning-assisted smart process management in cyber-physical production systems," 2021. doi: 10.3390/electronics10202497