а негативний або нульовий приріст $\Delta S(k) = S(k-1) - S(k)$ є підставою для відхилення зміни. Це зменшує ризик формального рефакторингу, коли код виглядає простішим локально, але створює нові залежності або ускладнює безпековий аудит.

Висновки. Запропонована процедура дозволяє формалізувати зменшення технічного боргу як вимірюваний процес, у якому LLM виконує роль генератора кандидатних змін, а метрики − роль критерію прийняття. Пілотні результати засвідчили монотонне або майже монотонне зменшення $S(k)$, причому найбільший ефект спостерігається у проєктах з вищою початковою залежністю модулів. Отже, підхід може розглядатися як допоміжний засіб підвищення кіберстійкості, оскільки спрощення структури коду полегшує аудит, тестування і контроль безпечних змін.


1. Martinez S., Xu L., Elnaggar M., Alomar E.A. Software Refactoring Research with Large Language Models: A Systematic Literature Review. Journal of Systems and Software. 2025. URL: https://www.sciencedirect.com/science/article/abs/pii/S0164121225004315.
2. Tornhill A., Borg M., Hagatulah N., Söderberg E. ACE: Automated Technical Debt Remediation with Validated Large Language Model Refactorings. FSE Companion '25: Proceedings of the 33rd ACM International Conference on the Foundations of Software Engineering. 2025. P. 1318–1324. DOI: 10.1145/3696630.3730565.
3. Cordeiro J., Noei S., Zou Y. LLM-Driven Code Refactoring: Opportunities and Limitations. 2025 IEEE/ACM Second IDE Workshop (IDE). 2025. P. 32–36. DOI: 10.1109/IDE66625.2025.00011.
4. Rozière B., et al. Code Llama: Open Foundation Models for Code. arXiv:2308.12950. 2023. URL: https://arxiv.org/abs/2308.12950.
5. SonarSource. Understanding measures and metrics. SonarQube Server Documentation. 2026. URL: https://docs.sonarsource.com/sonarqube-server/user-guide/code-metrics/metrics-definition.


## Ризик-орієнтований підхід до захисту IoT-пристроїв у муніципальних системах

УДК 004.056:004.738.5:352.07

Олександр Голотенко[1], Сергій Кульчицький[2], Данило Стухляк[3]

*Тернопільський національний технічний університет імені Івана Пулюя,*
*[1]golotenko@gmail.com, [2]serhii_kulchytskyi0212@tntu.edu.ua,*
*[3]itaniumua@gmail.com*

Активне впровадження IoT-пристроїв у муніципальних системах є важливим напрямом цифрової трансформації громад. Такі пристрої застосовуються для екологічного моніторингу, керування освітленням, обліку ресурсів, контролю енергоспоживання, транспортних потоків і роботи комунальних об'єктів. Водночас їхня значна кількість, територіальна

розподіленість, бездротові канали зв'язку, обмежені обчислювальні ресурси та фізична доступність створюють підвищені кіберризики. За цих умов однаковий рівень захисту для всіх компонентів є неефективним, оскільки не враховує різної критичності пристроїв і можливих наслідків інциденту.

Метою роботи є обґрунтування ризик-орієнтованого підходу до захисту IoT-пристроїв у муніципальних системах, який дає змогу визначати пріоритетність заходів кібербезпеки з урахуванням критичності пристрою, рівня експозиції, потенційного впливу компрометації та наявних механізмів захисту. ISO/IEC 27005 розглядає управління ризиками як процес ідентифікації, аналізу, оцінювання та оброблення ризиків [1].

NIST Cybersecurity Framework 2.0 доповнює цю логіку безперервним циклом ідентифікації активів, захисту, виявлення подій, реагування, відновлення та управління ризиками [2].

Наукова новизна підходу полягає в адаптації ризик-орієнтованого управління до муніципального IoT-середовища, де пріоритет захисту визначається не лише технічними параметрами пристрою, а й його роллю у функціонуванні конкретного міського сервісу.

Сенсор температури в приміщенні, лічильник енергоспоживання на комунальному об'єкті та контролер вуличного освітлення можуть належати до одного класу IoT, але мати різний рівень критичності й різні вимоги до захисту.

Таблиця 1

Критерії ризик-орієнтованого захисту IoT-пристроїв

| Критерій | Зміст оцінювання | Приклад захисного рішення |
|---|---|---|
| Критичність пристрою | вплив на роботу муніципального сервісу | пріоритетне резервування та моніторинг |
| Рівень експозиції | доступність із мережі або фізичного середовища | сегментація, VPN, обмеження портів |
| Вразливість конфігурації | паролі, прошивка, відкриті сервіси | оновлення, унікальні облікові дані |
| Потенційний вплив | наслідки для даних, процесів і безперервності | журналювання, резервне відновлення |
| Наявний захист | поточні технічні й організаційні заходи | посилення контролю доступу |

Запропонований підхід передбачає п'ять етапів: інвентаризацію IoT-пристроїв, класифікацію за критичністю, ідентифікацію загроз і вразливостей, оцінювання ризику та визначення пріоритетних захисних заходів.

Для кожного пристрою доцільно фіксувати призначення, місце встановлення, тип підключення, протоколи обміну, відповідальний підрозділ і пов'язаний муніципальний сервіс.

Рівень ризику може визначатися через критичність, імовірність реалізації загрози, експозицію та потенційний вплив інциденту за експертною шкалою від 1 до 5 балів.

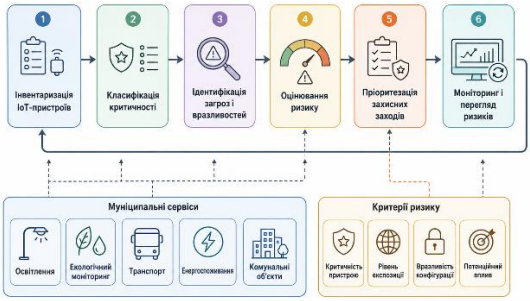


Рис.1. Ризик-орієнтований підхід до захисту IoT-пристроїв у муніципальних системах

З урахуванням сучасного ландшафту загроз особливої уваги потребують атаки на доступність, експлуатація відомих вразливостей, компрометація облікових даних і підміна даних. Можемо визначити загрози даним, атаки на доступність, соціальну інженерію та експлуатацію вразливостей серед провідних напрямів кіберзагроз Отже, ризик-орієнтований підхід дає змогу перейти від фрагментарного технічного захисту до системного управління безпекою муніципальних IoT-сервісів, раціонально розподіляти ресурси громади та підвищувати стійкість міської цифрової інфраструктури. Подальші дослідження доцільно спрямувати на кількісну модель оцінювання ризиків, автоматизацію інвентаризації активів та інтеграцію цього підходу з платформами моніторингу кібербезпеки [3,4].

1. Alavi A.H. et al. Internet of Things-enabled smart cities: State-of-the-art and future trends. Measurement. 2018. Vol. 129. P. 589-606.
2. Elmaghraby A.S., Losavio M.M. Cyber security challenges in smart cities: Safety, security and privacy. Journal of Advanced Research. 2014. Vol. 5(4). P. 491-497.
3. Tok Y.C., Chattopadhyay S. Identifying threats, cybercrime and digital forensic opportunities in smart city infrastructure via threat modeling. Forensic Science International: Digital Investigation. 2023. Vol. 45. Article 301540.
4. Kumar V. et al. Challenges in the design and implementation of IoT testbeds in smart-cities: A systematic review. arXiv:2302.11009. 2023.

## Development of an artificial intelligence-driven managed detection and response framework for proactive enterprise cyber defense

UDK 004.056.53(043.2)

Kyrylo Kurchak

*National University of Water and Environmental Engineering,*
*kurchak_ak21@nuwm.edu.ua*

The continuous evolution of enterprise computing paradigms, characterized by the widespread adoption of hybrid cloud architectures, distributed microservices, and extensive remote-work infrastructures, has radically expanded the corporate attack