підходу в умовах обмежених ресурсів та необхідності визначення найбільш критичних заходів захисту для CI/CD-середовищ.

1. Prates, L., & Pereira, R. (2025). DevSecOps practices and tools. International Journal of Information Security, 24 (1), 11. https://doi.org/10.1007/s10207-024-00914-z
2. Saaty, T. L., & Vargas, L. G. (2012). Models, Methods, Concepts & Applications of the Analytic Hierarchy Process (2nd ed.). Springer. DOI: doi.org/10.1007/978-1-4614-3597-6
3. National Institute of Standards and Technology. (2022). Secure Software Development Framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities (NIST Special Publication 800-218). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-218

Кібербезпека систем екологічного моніторингу як елемент критичної міської інфраструктури

УДК 004.056:502.3:004.738.5

Андрій Станько[1], Ірина Дідич[2], Артем Гончаренко[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]andrjj.stanko@gmail.com, [2]iryna.didych1101@gmail.com
Київський національний університет будівництва і архітектури,
[3]hosting.pat@gmail.com

Системи екологічного моніторингу є важливим елементом цифрової інфраструктури міста, адже забезпечують збирання, передавання, оброблення та візуалізацію даних про якість повітря, стан води, шумове навантаження, радіаційний фон, мікроклімат і екологічні ризики. У smart city вони поєднуються з IoT-пристроями, геоінформаційними платформами, диспетчерськими службами та публічними панелями, тому достовірність і доступність даних впливають на управлінські рішення та реагування служб.

Актуальність проблеми зумовлена тим, що кібератаки на такі системи можуть спричинити втрату даних або формування хибної картини екологічної ситуації. Підміна телеметрії, блокування панелей, компрометація хмарної платформи чи втручання в алгоритми оброблення підвищують ризик запізнілого реагування на аварійні викиди, пожежі та техногенні інциденти. Метою роботи є обґрунтування підходу до кіберзахисту систем екологічного моніторингу як елемента критичної міської інфраструктури.

Відповідно до NIST Cybersecurity Framework 2.0, управління кібербезпекою охоплює ідентифікацію активів і ризиків, захист, виявлення подій, реагування, відновлення та організаційне управління [1]. Для екологічного моніторингу об’єктом захисту є повний ланцюг формування інформації: сенсор, контролер, канал зв’язку, шлюз, edge-вузол, API, хмарна платформа, аналітичний модуль, інтерфейс оператора і публічний вебсервіс.

Наукова новизна підходу полягає в розгляді системи екологічного моніторингу як кіберфізичного ланцюга довіри, де безпека визначається не лише захищеністю пристроїв, а й цілісністю маршруту даних від вимірювання до управлінського рішення. Запропоновано виділяти три рівні кіберзахисту: польовий, мережево-платформний та управлінсько-аналітичний.

Польовий рівень охоплює сенсори, мікроконтролери, автономні станції, джерела живлення та модулі передавання даних. Типові загрози: фізичне втручання, підміна сенсора, стандартні паролі, зміна прошивки або порушення калібрування. Базові вимоги до безпеки IoT-пристроїв передбачають відмову від універсальних паролів, безпечне оновлення, захист конфіденційних параметрів, мінімізацію поверхні атаки та керування вразливостями [2].

Мережево-платформний рівень включає шлюзи, канали зв'язку, VPN-з'єднання, MQTT/HTTP API, edge-вузли, хмарні сервіси, бази даних і механізми автентифікації. Його порушення можуть спричинити перехоплення або втрату телеметрії, DDoS-атаки й компрометацію доступу. На управлінсько-аналітичному рівні ключовими є валідація даних, панелі моніторингу, модулі прогнозування, оповіщення та звітність, оскільки саме тут викривлені дані трансформуються в помилкові рішення

Таблиця 1

Рівні кіберзахисту системи екологічного моніторингу

Рівень системи	Основні компоненти	Типові кіберризики	Захисні заходи
Польовий	сенсори, контролери, станції моніторингу	підміна показників, фізичне втручання, вразливі паролі	автентифікація пристроїв, захист прошивки, контроль калібрування
Мережево-платформний	шлюзи, канали зв'язку, API, хмарні сервіси	перехоплення даних, DDoS, компрометація доступу	шифрування, сегментація, VPN, журналювання подій
Управлінсько-аналітичний	панелі моніторингу, бази даних, модулі прогнозування	викривлення аналітики, недоступність сервісу, помилкові рішення	резервування, валідація даних, контроль доступу, аудит

З урахуванням сучасного ландшафту загроз слід поєднувати технічні й організаційні заходи. За даними ENISA Threat Landscape 2024, актуальними залишаються атаки на доступність, програми-вимагачі, загрози даним, соціальна інженерія та експлуатація вразливостей [4]. Для міського моніторингу це означає резервування каналів, регулярне оновлення ПЗ, централізоване управління доступом, журналювання, перевірку цілісності даних і тестування планів реагування.

Практична реалізація підходу може ґрунтуватися на паспорті кібербезпеки, що містить перелік активів, потоки даних, критичні компоненти, модель доступу, вимоги до резервного копіювання та порядок реагування на інциденти. Отже, кібербезпека систем екологічного моніторингу є умовою надійності

розумного міста, екологічної безпеки та довіри населення. Подальші дослідження доцільно спрямувати на кількісне оцінювання ризиків, інтеграцію з SIEM/SOC-рішеннями та виявлення фальсифікованих або аномальних даних.

1. Bacco M., Delmastro F., Ferro E., Gotta A. Environmental monitoring for smart cities. IEEE Sensors Journal. 2017. Vol. 17(23). P. 7767-7774.
2. Zanella A. et al. Internet of Things for smart cities. IEEE Internet of Things Journal. 2014. Vol. 1(1). P. 22-32.
3. Sicari S. et al. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015. Vol. 76. P. 146-164.
4. Demertzi V., Demertzis S., Demertzis K. An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. Applied Sciences. 2023. Vol. 13(2). Article 790.

Застосування методу PERT для оцінки трудомісткості задач у мобільних застосунках управління проєктами

УДК 004.42

Стасюк Сергій[1], Мудрик Іван[2]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]serhii_stasiuk1107@tntu.edu.ua, [2]i1mudryk@tntu.edu.ua

Управління сучасними IT-проєктами стикається з двома критичними викликами: проблемою точної оцінки трудомісткості задач та необхідністю гарантування конфіденційності проєктної інформації. Мобільні застосунки для трекінгу задач обробляють надзвичайно чутливі корпоративні дані (строки, розподіл ресурсів, архітектурні інсайти, бізнес-процеси). Відповідно, інструмент планування має не лише вирішувати проблему зриву дедлайнів, але й відповідати суворим вимогам інформаційної безпеки.

Точна оцінка трудомісткості задач є одним із ключових викликів у сучасному IT-проєктному менеджменті. Сучасні менеджери проєктів все частіше використовують мобільні застосунки для трекінгу задач та управління ресурсами. Однак, однією з найскладніших задач залишається точна оцінка трудомісткості на етапі планування або безпосередньо "на ходу" (наприклад, під час дейлі-мітингів чи зустрічей з клієнтами). Традиційні однопунктові методи систематично ігнорують невизначеність і ризики, що призводить до зривів термінів та перевитрати бюджету. Метод PERT (Program Evaluation and Review Technique) вирішує цю проблему через три сценарії для кожної задачі: оптимістичний (О), реалістичний (Р) та песимістичний (П). Очікуваний час (Т) обчислюється за формулою бета-розподілу:

$$T = \frac{О + 4Р + П}{6}$$

Така зважена оцінка враховує статистичний розподіл можливих результатів і є суттєво точнішою за однопунктове прогнозування [1].

Аналіз популярних інструментів (Trello, Jira, Asana) показує, що вони орієнтовані на хмарну синхронізацію, що розширює поверхню атаки (attack