1. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report: 4th Quarter 2024. 2024. URL: https://www.apwg.org/trendsreports/ (дата звернення: 25.04.2025)

Altulaihan E., Alismail A., Rahman M. M., Ibrahim A. Email security issues, tools, and techniques used in investigation. *Sustainability*. – 2023. – Vol. 15. – №10612.

## Формалізація методики побудови безпечних інформаційних систем екологічного моніторингу

УДК 004.75

Кирило Вадурін[1], Андрій Перекрест[2]
*Кременчуцький національний університет імені Михайла Остроградського, [1]kir3337@gmail.com, [2]pksg13@gmail.com*

Наразі спостерігаються тенденції до розширення використання датчиків якості повітря в інфраструктурі Smart City для моніторингу екологічної ситуації. Існують платформи для збору та аналізу даних, проте питання безпеки інформаційних систем та формалізації відповідних методик залишаються поза увагою. Актуальність запланованої роботи пов'язана з необхідністю забезпечення безпеки та надійності інформаційних систем екологічного моніторингу в умовах розширення інфраструктури Smart City.

У ході аналізу подібних рішень виявлено, що питання безпеки інформаційних систем екологічного моніторингу, особливо в контексті Smart City, потребують додаткової уваги. Airly [1] пропонує комплексні рішення для моніторингу якості повітря, але питання безпеки даних не є пріоритетними. У той же час, існують дослідження, спрямовані на забезпечення безпеки та енергоефективності аутентифікації в розумних містах за допомогою біометрії та криптографічних методів [2], проте вони не враховують специфіку датчиків якості повітря. Платформи, такі як Kyiv Smart City [3], демонструють можливості моніторингу якості повітря, але потребують удосконалення в частині довгострокової підтримки та інтеграції з іншими міськими системами. Державна система моніторингу довкілля в Україні [4] потребує модернізації та впровадження сучасних технологій для забезпечення ефективного збору та аналізу даних. Таким чином, невирішеними залишаються питання формалізації безпеки, масштабування рішень та інтеграції даних моніторингу з іншими системами Smart City.

Метою роботи є формалізація методики побудови безпечних інформаційних систем екологічного моніторингу на основі розподіленої апаратної інфраструктури датчиків якості повітря та виконавчих пристроїв Smart City, що забезпечить захист даних та надійність функціонування системи.

Основними завданнями, що наразі не вирішені, є розробка конкретних методів формалізації безпеки інформаційних систем екологічного моніторингу, забезпечення захисту даних та надійності розподіленої апаратної інфраструктури датчиків якості повітря, а також вирішення питань масштабування, довгострокової підтримки та інтеграції даних моніторингу з іншими міськими системами.

Тому, ході роботи, передбачається розробка формалізованої методики побудови інформаційних систем, яка враховує специфіку розподіленої апаратної інфраструктури датчиків якості повітря та виконавчих пристроїв. Це дозволить підвищити захищеність даних, запобігти несанкціонованому доступу та забезпечити стабільне функціонування системи в цілому.

У рішенні заплановано використати такі методи: формалізація вимог до безпеки інформаційних систем, моделювання загроз та ризиків, криптографічні методи захисту даних, методи забезпечення відмовостійкості та відновлення даних, а також методи аналізу та візуалізації даних моніторингу. Планується застосування методів машинного навчання для виявлення аномалій та прогнозування змін якості повітря.


Рис.1. Графічне представлення сформованої концепції

Пропоноване рішення має функціонувати наступним чином: датчики якості повітря, розміщені в різних точках міста, безперервно збирають дані про концентрацію забруднюючих речовин. Ці дані передаються захищеними каналами зв’язку до центрального серверу, де вони обробляються та аналізуються на основі ретроспективних даних задля визначення загальних характеристик забруднення, а також ідентифікації цифрових патернів станцій, щоб запобігти ін’єкціям. У разі виявлення перевищень допустимих норм, втрати чи підміни даних, система автоматично формує оповіщення та надсилає їх відповідним службам, або населенню (у режимі оповіщення). Також, система забезпечує можливість автоматизованого керування виконавчими пристроями, такими, як системами вентиляції, очищення повітря у громадських будівлях.

1. The role of air quality sensors in smart city infrastructure. URL: https://airly.org/en/the-role-of-air-quality-sensors-in-smart-city-infrastructure/

2. Nyangaresi, V.O., Abduljabbar, Z.A., Mutlaq, K.AA. et al. Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme. Sci Rep 14, 16223 (2024). https://doi.org/10.1038/s41598-024-67064-z

3. Платформа, де можна перевірити якість повітря у Києві. URL: https://www.village.com.ua/village/city/city-news/285841-platforma-de-mozhna-pereviriti-yakist-povitrya-u-kieva

4. Екологічний моніторинг довкілля. URL: https://mepr.gov.ua/diyalnist/napryamky/ekologichnyj-monitoryng/ekologichnyj-monitoryng-dovkillya (дата звернення: 10.04.2025).

## Сучасні виклики та використання командного підходу в управлінні інформаційними системами

УДК 342.95

Петро Венгерський[1], Михайло В`ячало[2]
*Львівський національний університет ім.І.Франка,*
*[1]Petro.Venherskyy@lnu.edu.ua, [2]Mykhaylo.Vyachalo@lnu.edu.ua*

Процес управління інформаційними системами (ІС) в умовах сучасної цифрової трансформації є надзвичайно складним та багаторівневим. Ефективність управління ІС впливає не лише на стабільність бізнес-процесів, але й безпосередньо на рівень кіберзахисту в організації. Зростання складності ІТ інфраструктури, поширення хмарних сервісів, розвиток кіберзагроз породжують нові виклики, які потребують системного та командного підходу.[1]

Нижче розглянемо ключові виклики сучасності в управлінні ІС та рішення які допоможуть організаціям впоратись з ними:

1. Гібридна інфрастуктура (on-premises + cloud). Дедалі більше організацій працюють в змішаних середовищах: локальні сервери, публічні/приватні хмари, SaaS – рішення. Це в свою чергу створює труднощі з контролем, моніторингом та забезпеченням безпеки.[3] Ефективними рішеннями, які можуть допомогти в покращенні управління ІС у даному випадку, можуть бути наступні:
   - впровадження ефективного контролю доступу (IAM, SSO)
   - використання хмарно-орієнтованих платформ управління безпекою (CSPM)
   - ефективна та тісна взаємодія адміністраторів хмарної та локальної інфрастурктури.
2. Зростання складності систем. API-інтеграції та автоматизація, мікросервіси, велике різноманіття ІТ-рішень створюють високий ризик конфігураційних помилок, несумісності та вразливостей.[1] Рішеннями можуть бути:
   - стандартизація розгортання (Infrastructure as Code)
   - автоматичні тести безпеки (DevSecOps)
   - регулярні код-рев`ю та конфігураційні аудити
3. Кадрові проблеми та перевантаження фахівців. Постійний розвиток технологій, збільшення навантаження на SOC-команди, брак кваліфікованих кадрів – все це безпосередньо впливає на якість управління ІС.[4] Рішеннями тут можуть бути:
   - побудова міжфункціональних команд підтримки (SRE, SecOps)