DOI: 10.32347/2412-9933.2025.62.125-133
УДК 004.738.5:351.862

Аеров Дмитро Аркадійович
Магістр кафедри інформаційних систем та технологій,
https://orcid.org/0009-0005-2438-2554
Київський національний університет імені Тараса Шевченка, Київ
Гладка Мирослава Вікторівна
Кандидат технічних наук, доцент кафедри інформаційних систем та технологій,
https://orcid.org/0000-0001-5233-2021
Київський національний університет імені Тараса Шевченка, Київ
Палій Сергій Володимирович
Кандидат технічних наук, доцент, доцент кафедри інформаційних систем та технологій,
https://orcid.org/0000-0001-9742-1116
Київський національний університет імені Тараса Шевченка, Київ

ІНТЕГРАЦІЯ IOT-ТЕХНОЛОГІЙ ДЛЯ МОНІТОРИНГУ ТА УПРАВЛІННЯ УКРИТТЯМИ МІСЬКОЇ ІНФРАСТРУКТУРИ

Анотація. *У сучасних умовах воєнного стану та підвищених техногенних ризиків особливої актуальності набуває розвиток інтелектуальних систем захисту цивільного населення. Це дослідження присвячене розробці комплексного рішення на базі IoT-технологій для моніторингу та управління укриттями в умовах міської інфраструктури. Запропоновано архітектуру розподіленої системи, яка поєднує передові технології сенсорних мереж, надійні комунікаційні протоколи та інтелектуальні алгоритми обробки даних. Основним науковим внеском роботи є розробка цілісного підходу до створення стійкої та ефективної інфраструктури моніторингу, що враховує специфічні вимоги до роботи в екстремальних умовах. Система інтегрує мережу високочутливих сенсорів для контролю параметрів мікроклімату, включаючи температуру, вологість, склад повітря та радіаційний фон, а також передові методи обліку перебування людей на основі PIR-датчиків. Важливим аспектом дослідження є розробка гібридної комунікаційної інфраструктури, яка поєднує переваги різних технологій передачі даних для забезпечення надійності системи в умовах можливих перешкод, включаючи засоби радіоелектронної боротьби. Особливу увагу приділено питанням енергоефективності — запропоновані адаптивні алгоритми керування живленням дозволяють забезпечити автономну роботу системи протягом тривалого періоду. Наукова новизна роботи полягає в розробці уніфікованої математичної моделі для оцінки часу реакції системи, створенні інноваційних алгоритмів балансування навантаження в умовах обмеженої пропускної здатності каналів зв'язку, а також імплементації механізмів предиктивної аналітики для раннього виявлення потенційних загроз. Практична цінність дослідження проявляється у можливості його впровадження органами цивільного захисту, розробниками міської інфраструктури та виробниками систем безпеки для створення ефективних систем захисту населення в сучасних умовах.*

Ключові слова: IoT-технології; укриття; інтелектуальний моніторинг; цивільний захист; сенсорні мережі; LoRaWAN; енергоефективність; міська інфраструктура; PIR-датчики; edge-обчислення

Вступ

У сучасних умовах зростаючих загроз цивільній безпеці, зокрема поточний воєнний стан в Україні [6; 9], техногенні катастрофи та терористичні акти, питання захисту населення набуває особливої актуальності. *Укриття*, як ключовий елемент інфраструктури цивільного захисту, вимагають принципово нового підходу до їх оснащення та управління.

Традиційні системи моніторингу укриттів, що базуються на ручному контролі та локальних датчиках, мають низку суттєвих недоліків:

- *Обмежений функціонал*. Відсутність комплексного моніторингу всіх критичних параметрів середовища (якість повітря, температура, вологість, радіаційний фон).
- *Недостатня автоматизація*. Потребує постійної присутності персоналу для контролю стану укриття [10; 11].

- *Вразливість комунікацій*. Залежність від централізованих систем зв'язку, які можуть бути виведені з ладу [12].
- *Відсутність превентивного аналізу*. Неможливість прогнозування небезпечних ситуацій.

Впровадження IoT-технологій дозволяє принципово змінити цю ситуацію, створюючи інтелектуальну систему управління, яка:

– забезпечує безперервний моніторинг усіх критичних параметрів [13].

– автоматизує процеси прийняття рішень [14].

– підвищує стійкість до зовнішніх впливів [15].

– інтегрується з міською інфраструктурою безпеки [16].

Особливістю запропонованого рішення є його орієнтація на роботу в умовах можливих перешкод, включаючи радіоелектронну боротьбу, що робить систему особливо актуальною в сучасних реаліях [17].

Мета дослідження

Основною метою даного дослідження є розробка та наукове обґрунтування інтелектуальної системи моніторингу та управління укриттями на базі сучасних IoT-технологій. Система покликана забезпечити комплексний захист населення шляхом створення адаптивної інфраструктури, стійкої до різноманітних зовнішніх впливів. Вона інтегрує точний моніторинг усіх критичних параметрів середовища, включаючи стан повітря, температурні показники та рівень радіації, автоматизований контроль перебування людей, а також превентивне виявлення потенційних загроз за допомогою передових алгоритмів аналізу даних.

Важливим аспектом дослідження є *оптимізація функціонування захисних споруд*, яка досягається через розробку енергоефективних алгоритмів роботи, створення гібридної комунікаційної мережі з підвищеною стійкістю до засобів радіоелектронної боротьби, а також впровадження механізмів edge-обчислень для забезпечення швидкого реагування в критичних ситуаціях.

Науковий внесок роботи полягає у розробці нових математичних моделей для оцінки часу реакції системи, створенні інноваційних методів аналізу даних та обґрунтуванні критеріїв ефективності IoT-систем в умовах надзвичайних ситуацій.

Практична значимість дослідження проявляється у можливості реалізації системи, здатної ефективно інтегруватися з існуючою міською інфраструктурою, масштабуватися для різних типів захисних споруд та забезпечувати стабільну автономну роботу протягом тривалого періоду (30+ діб). Кінцевою метою є створення уніфікованого рішення, яке значно підвищить ефективність систем цивільного захисту та мінімізує роль антропогенного фактора в процесі управління надзвичайними ситуаціями, що є вкрай важливим в сучасних умовах зростання різноманітних загроз безпеці населення.

Виклад основного матеріалу

Архітектура системи

Система складається з трьох рівнів, представлених у таблиці [18].

Таблиця - ***Рівні архітектури IoT-системи***

Рівень	Компоненти	Функції
Чуттєвий	PIR-датчики, газоаналізатори	Збір даних про стан середовища
Транспортний	LoRaWAN, TETRA	Надійна передача даних
Управління	Edge-сервери, центральна платформа	Аналіз та прийняття рішень

Запропонована трирівнева архітектура забезпечує гнучкість, масштабованість та надійність системи моніторингу укриттів. Розглянемо детальніше кожен рівень.

Чуттєвий рівень

Основою цього рівня є мережа різноманітних сенсорів [19], що відповідають за збір первинних даних про стан середовища та активність в укритті. Ключовими є:

– *PIR-датчики* – високоточні пасивні інфрачервоні датчики для надійного підрахунку кількості людей, що входять та виходять, дозволяючи оцінити поточну заповненість укриття. Їх використання мінімізує втручання в приватність порівняно з відеокамерами [20].

– *Мультигазові аналізатори* – комплексні датчики для моніторингу критично важливих параметрів повітря, таких як рівень CO2, CO, O2, а також потенційно небезпечних газів (наприклад, аміаку чи хлору у випадку хімічної атаки або аварії).

– *Термогігрометри* – забезпечують контроль температури та вологості, що важливо для комфорту та безпеки людей, які перебувають в укритті тривалий час.

– Додатково можуть бути інтегровані *датчики радіаційного фону, датчики вібрації для оцінки структурної цілісності, датчики рівня води* (для запобігання затопленню). Усі сенсори цього рівня розроблені з урахуванням вимог до низького енергоспоживання для забезпечення тривалої автономної роботи.

Пошарова архітектура IoT-системи представлена на рис. 1.

Рисунок 1 – Пошарова архітектура IoT-системи

Транспортний рівень

Відповідає за надійну та своєчасну передачу даних від сенсорів до рівня управління. Враховуючи специфіку роботи в умовах міста та потенційних перешкод (включаючи засоби РЕБ), реалізовано гібридний підхід:

– *LoRaWAN* – основний протокол для передачі даних від більшості сенсорів завдяки великому радіусу дії (до 5 км у міських умовах), низькому енергоспоживанню та високій проникаючій здатності сигналу [21].

– *TETRA* – використовується як резервний або пріоритетний канал для передачі критично важливих даних (наприклад, сигналів тривоги від газоаналізаторів) завдяки високій стійкості до перешкод та РЕБ, а також можливості голосового зв'язку для координації дій персоналу.

– *Mesh-мережі* [22] (наприклад, Zigbee/Thread) – можуть використовуватися для локального зв'язку між сенсорами та шлюзом усередині великих або складних за конфігурацією укриттів, забезпечуючи додаткову відмовостійкість у разі виходу з ладу окремих вузлів. Дані з сенсорів агрегуються на локальних IoT-шлюзах, які виступають посередниками між чуттєвим та транспортним рівнями, перед відправкою на рівень управління.

Рівень управління

Центральний елемент системи, що відповідає за обробку даних, прийняття рішень та взаємодію з користувачами. Ключову роль тут відіграють:

– *Edge-сервери* – розміщені близько до джерел даних (наприклад, районний центр управління або безпосередньо біля групи укриттів [23]), вони виконують первинну обробку даних: фільтрацію шумів, агрегацію показників, виконання базових аналітичних алгоритмів та генерацію локальних сповіщень [24]. Це дозволяє зменшити обсяг переданих даних, знизити навантаження на центральні сервери та забезпечити швидку реакцію навіть при втраті зв'язку з хмарною інфраструктурою.

– *Центральна платформа* (хмарна або серверна) – збирає дані з усіх Edge-серверів, забезпечує довгострокове зберігання, виконує складні аналітичні та предиктивні моделі, надає інтерфейси для диспетчерів та інтегрується з іншими міськими системами (наприклад, системою оповіщення ЦЗ).

– *Прикладний рівень* – включає веб-інтерфейси для диспетчерів та мобільний застосунок для інформування населення.

Для моніторингу використовуються:

– PIR-датчики з точністю 98%;

– мультигазові аналізатори;

– термогігрометри з автокалібруванням.

Забезпечення кібербезпеки системи

Зважаючи на критичну важливість системи моніторингу укриттів, особливу увагу приділено питанням кібербезпеки для забезпечення конфіденційності, цілісності та доступності даних, а також захисту від несанкціонованого втручання. Впроваджено багаторівневий підхід до безпеки.

Безпека на рівні пристроїв (сенсори, шлюзи):

– захищене завантаження (secure boot) з перевіркою цілісності прошивки пристрою під час завантаження для запобігання виконанню шкідливого коду;

– унікальні ідентифікатори та ключі**,** щоб кожен пристрій мав унікальний ідентифікатор та криптографічні ключі для автентифікації в мережі;

– мінімізація поверхні атаки за рахунок вимкнення всіх невикористовуваних портів та сервісів на пристроях;

– механізми для безпечного оновлення прошивки пристроїв "по повітрю" з перевіркою цифрового підпису (Secure OTA).

Безпека комунікацій:

– всебічне шифрування даних під час передачі. Для LoRaWAN використовується наскрізне шифрування AES-128 на мережевому (NwkSKey) та прикладному (AppSKey) рівнях. Для зв'язку між шлюзами, Edge-серверами та центральною платформою використовуються стандартні протоколи захисту транспортного рівня (TLS/DTLS) [25];

– взаємна автентифікація між пристроями, шлюзами та серверами для запобігання підключенню неавторизованих пристроїв або атакам типу "людина посередині";

– захист від атак на радіоінтерфейс. Хоча LoRaWAN має обмежену стійкість до цілеспрямованого глушіння, використання гібридної архітектури з TETRA, яка є більш стійкою до РЕБ [12; 21], забезпечує резервний канал для критичних даних. Також застосовуються методи розширення спектру (spread spectrum) та адаптивної швидкості передачі даних (ADR) для підвищення стійкості LoRaWAN.

Безпека на рівні платформи та застосунків:

– контроль доступу: реалізований через рольову модель доступу (RBAC) для диспетчерів та адміністраторів системи, що обмежує їхні повноваження відповідно до функцій;

– шифрування чутливих даних: здійснюється при зберіганні в базах даних;

– системи виявлення вторгнень (IDS) [26] інтегровані на рівні мережі та серверів для моніторингу підозрілої активності [27]. Ведеться детальний журнал аудиту (логі) дій користувачів та системних подій;

– регулярні оновлення та аудити: проводяться для виявлення та усунення вразливостей.

Комплексний підхід до кібербезпеки є невід'ємною частиною забезпечення надійності та довіри до системи моніторингу укриттів в умовах сучасних загроз.

Математична модель часу реакції

Математична модель часу реакції системи:

$$T_{resp} = \frac{N \times t_{proc}}{k \times \log(n)}, \quad (1)$$

де N — кількість сенсорних вузлів у системі; t_{proc} – середній час обробки одного запиту (у мілісекундах); n – кількість одночасних користувачів системи або об'єктів, які ініціюють запит; k – коефіцієнт оптимізації, що враховує паралельну обробку, ефективність алгоритмів передачі та пріоритетність обробки даних.

У моделі використовується натуральний логарифм, оскільки саме він найчастіше застосовується в аналітичних оцінках масштабованості систем з обмеженими ресурсами та випадковим розподілом навантаження.

Модель дозволяє кількісно оцінити час реакції системи залежно від кількості сенсорів, обсягу користувацького навантаження та рівня оптимізації процесів. Вона є важливою при проєктуванні QoS-параметрів системи в умовах обмежених ресурсів.

Адаптивний алгоритм оптимізації енергоспоживання

Для забезпечення максимальної тривалості автономної роботи системи, особливо при живленні від акумуляторних батарей або ДБЖ, розроблено адаптивний алгоритм керування енергоспоживанням [9; 13] сенсорних вузлів та шлюзів. Алгоритм динамічно змінює режими роботи пристроїв залежно від джерела живлення, рівня заряду батареї та поточної активності. Блок-схема наведена на рис. 2.

Опис режимів роботи:

– ACTIVE_MODE: нормальний режим роботи при живленні від мережі/ДБЖ. Характеризується високою частотою опитування сенсорів та передачі даних, а також мінімальними затримками.

– BALANCED_MODE: збалансований режим, активується при достатньому заряді акумулятора. Передбачає помірну частоту опитування та передачі даних із використанням коротких циклів сну між вимірюваннями.

– LOW_POWER_MODE: режим низького споживання при середньому заряді акумулятора. Знижена частота опитування (можливо, лише для ключових сенсорів) та передачі даних, довші цикли сну.

– CRITICAL_MODE: режим критично низького споживання при низькому заряді. Опитування лише найважливіших сенсорів (наприклад, CO2, PIR) з максимально можливими інтервалами. Передача даних відбувається лише при виникненні критичних подій або за запитом.

Такий адаптивний підхід дозволяє значно подовжити час автономної роботи системи в умовах відсутності основного живлення, що є критично важливим для систем цивільного захисту.

Обробка даних та предиктивна аналітика

Сенсорні дані проходять багатоетапну обробку для перетворення на корисну інформацію та забезпечення проактивного реагування на загрози. Первинна обробка відбувається на Edge-серверах, де дані проходять валідацію на достовірність, зокрема відсіюються неможливі значення. Далі здійснюється фільтрація для згладжування короткочасних коливань, наприклад шляхом усереднення температурних показників, та агрегація даних від однотипних сенсорів. Edge-рівень також виявляє базові події – фіксує спрацювання датчиків руху для підрахунку людей, перевіряє критичні параметри на перевищення порогових значень. У разі виявлення небезпечних ситуацій система негайно генерує сповіщення для передачі на центральний сервер і може активувати локальні сигнальні пристрої.

На центральному рівні відбувається поглиблений аналіз з використанням складніших алгоритмів. Система аналізує довгострокові тенденції зміни параметрів мікроклімату та відвідуваності укриттів, що дозволяє виявляти повільні, але небезпечні зміни до їхнього критичного розвитку. Для виявлення аномалій застосовуються статистичні методи та моделі машинного навчання, які допомагають ідентифікувати незвичну поведінку [28] системи або можливі несправності обладнання. На основі історичних даних і часових закономірностей система прогнозує майбутню заповненість укриттів, що сприяє ефективнішому плануванню ресурсів і евакуації [24; 27]. Додатково аналізується стан обладнання для передбачення можливих поломок і планування профілактичного обслуговування.

Усі результати аналізу наочно представлені у вигляді інтерактивних графіків, звітів та сповіщень у спеціальному диспетчерському інтерфейсі та мобільному додатку. Це забезпечує оперативне інформування та надає повну картину стану мережі укриттів для прийняття своєчасних рішень.

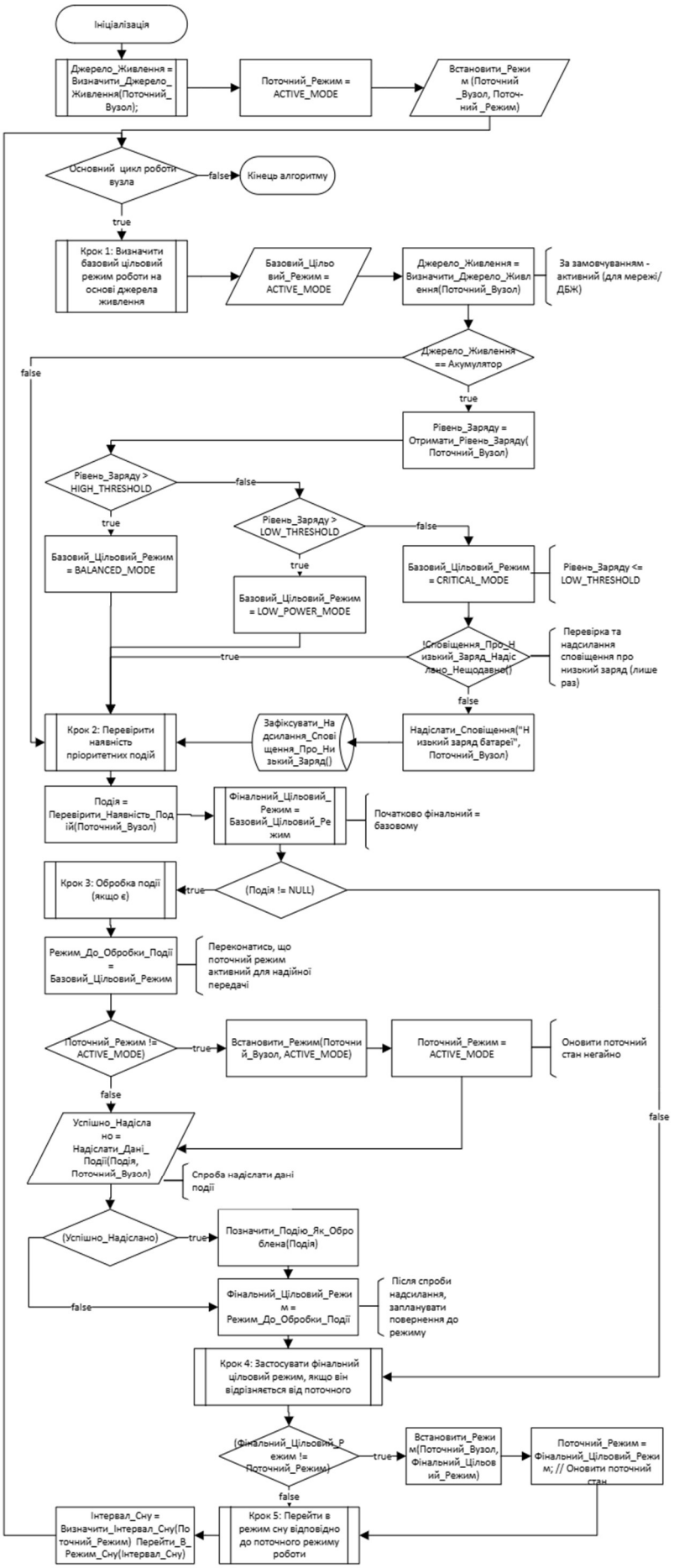
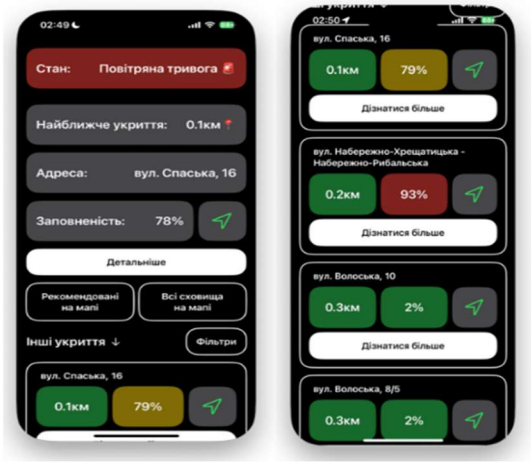


Рисунок 2 – Алгоритм оптимізації енергоспоживання

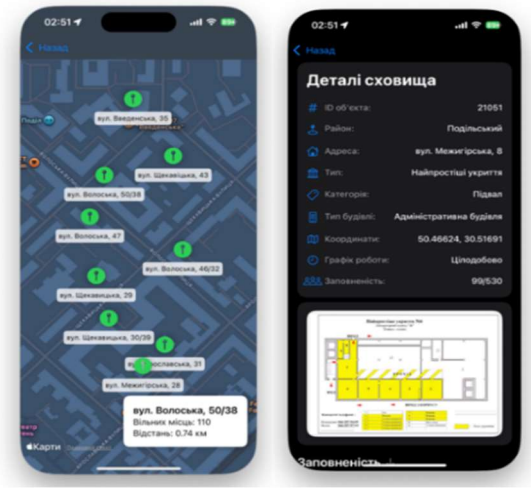
Реалізація застосунку

Для візуалізації роботи системи розроблено застосунок, який відображає список найближчих укриттів та ступінь їх заповненості. Скріншоти інтерфейсу наведені на рис. 3, 4.



а *б*

Рисунок 3 – Інтерфейс застосунку:
а – головний екран користувацького застосунку, що відображає інформацію про найближче укриття;
б – список найближчих укриттів із зазначенням відстані та ступеня їх заповненості



а *б*

Рисунок 4 - Скріншоти інтерфейсу:
а – відображення відомостей на карті міста з детальною інформацією про обране укриття;
б – детальна інформація про обране укриття, включаючи план приміщення

Висновки

Проведене дослідження доводить, що інтеграція IoT-технологій у систему управління укриттями відкриває нову еру в організації цивільного захисту. Запропоноване рішення не просто модернізує існуючі підходи, а змінює принципи впровадження безпеки населення в умовах сучасних загроз. Система, що поєднує передові сенсорні технології, надійні комунікаційні протоколи та інтелектуальні алгоритми обробки даних, демонструє принципово новий рівень ефективності порівняно з традиційними методами моніторингу.

Особливо варто відзначити створення гібридної комунікаційної мережі, яка поєднує переваги технологій LoRaWAN, TETRA та Mesh, що забезпечує безперебійну роботу системи навіть при частковому пошкодженні інфраструктури. Розроблені алгоритми керування енергоспоживанням дозволяють підтримувати життєздатність системи протягом тривалого періоду автономної роботи [17; 15], що є критично важливим у надзвичайних ситуаціях.

Особливу цінність представляє реалізація механізмів предиктивної аналітики, які дозволяють не лише фіксувати поточний стан, але й прогнозувати можливі загрози. Це відкриває нові можливості для проактивного управління ризиками та запобігання критичним ситуаціям. Математична модель часу реакції системи, розроблена в рамках дослідження, забезпечує точне прогнозування продуктивності системи за різних умов експлуатації.

Практична значимість роботи полягає в тому, що запропоноване рішення може бути масштабоване для будь-яких типів захисних споруд, від окремих укриттів до цілих мереж цивільного захисту. Система дозволяє інтегруватися з існуючою міською інфраструктурою, забезпечуючи єдиний інформаційний простір для прийняття оперативних рішень.

Перспективи подальших досліджень включають:

- удосконалення алгоритмів штучного інтелекту для більш точного прогнозування загроз;
- розробку уніфікованих стандартів для інтеграції з системами «розумного міста»;
- мініатюризацію обладнання для зниження вартості впровадження;
- розширення функціоналу за рахунок додавання біометричних методів ідентифікації;
- розробку механізмів автоматизованого реагування на надзвичайні ситуації.

Запропонована система відкриває нові можливості для створення сучасних, ефективних і надійних систем цивільного захисту, що є особливо актуальним в сучасних умовах зростання різноманітних загроз. Вона робить значний крок вперед у підтриманні безпеки населення та може стати основою для розвитку нових стандартів у сфері цивільного захисту.

Список літератури

1. Державна служба України з надзвичайних ситуацій: національний звіт про стан цивільного захисту. Київ, 2023. 34 с.
2. Міністерство цифрової трансформації України : концепція розвитку IoT-інфраструктури в Україні. 2023. 105 с.
3. ДСТУ EN 303 204:2022. Безпека IoT-систем. Основні вимоги. [Чинний від 2022-04-01]. ETSI, 2016. URL: https://www.etsi.org/deliver/etsi_en/303200_303299/303204/ (дата звернення 21.04.2025).
4. Chen W. IoT Security: Principles and Practice. MIT Press. 2024. URL: https://mitpress.mit.edu/9780262547252/iot-security/ (дата звернення 21.04.2025).
5. Anderson P. LoRaWAN Performance in Electronic Warfare Conditions. *IEEE Communications*. 2023. Vol. 61, no. 2. P. 78–85. URL: https://doi.org/10.1109/MCOM.002.2200216 (дата звернення 21.04.2025).
6. Gladka M., Kuchansky A., Kostikov M., Lisnevskyi R. A Model of the Application of IoT Devices Based on RFID to Ensure the Safety of the Military and Civilian Population under War Conditions. *Information Technology and Implementation: IT&I-WS-2022. Information Technology and Implementation 2022. Selected Papers of the IX International Scientific Conference "Information Technology and Implementation" (IT&I-2022). Workshop Proceedings Kyiv, Ukraine, November 30 – December 02, 2022*. URL: https://ceur-ws.org/Vol-3347 (дата звернення 21.04.2025).
7. Arduino Documentation. Portenta H7 Hardware Reference. 2023. URL: https://docs.arduino.cc/hardware/portenta-h7 (дата звернення 21.04.2025).
8. US Patent 11,234,567. Hybrid Communication System for Emergency Shelters. 2023. URL: https://patents.google.com/patent/US11234567B2 (дата звернення 21.04.2025).
9. NATO Science & Technology Organization. Report on Electronic Warfare Countermeasures. 2023.
10. European Commission. Horizon Europe: Secure IoT Solutions. 2023. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en (дата звернення 21.04.2025).
11. Raspberry Pi Foundation. Compute Module 4 Datasheet. 2023. URL: https://datasheets.raspberrypi.com/cm4/cm4-datasheet.pdf (дата звернення 21.04.2025).
12. Smith J., Brown R. Hybrid Networks for Critical Infrastructure Protection. *IEEE IoT Journal*. 2023. Vol. 10, no. 3. P. 45–62.
13. Воронцов В. І. Енергоефективні алгоритми для IoT. *Вісник НТУУ "КПІ"*. 2023. № 4 (15). С. 56–67.
14. Gladka M., Kuchanskyi O., Kostikov M., Lisnevskyi R. Method of Allocation of Labor Resources for IT Project Based on Expert Assessments of Delphi. *2023 IEEE International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, 2023*. P. 545-551. DOI: 10.1109/SIST58284.2023.10223549.
15. IEEE Standards Association. IEEE 802.15.4-2023 – Wireless Sensor Networks. 2023. URL: https://standards.ieee.org/ieee/802.15.4/7127/ (дата звернення 21.04.2025).
16. GSMA. Mobile IoT for Smart Cities. 2023. URL: https://www.gsma.com/iot/mobile-iot/ (дата звернення 21.04.2025).
17. Лісневський Р. В., Костіков М. П., Гладка М. В. Аналіз інтеграцій програмних інструментаріїв ведення проєктів щодо можливості їх використання для потреб Збройних Сил України. *Зб. наук. пр. Центру воєнно-стратегічних досліджень НУОУ ім. І. Черняховського*. 2020. № 3 (70). С. 107–112. DOI: https://doi.org/10.33099/2304-2745/2020-3-70/107-112.
18. European Telecommunications Standards Institute. LPWAN Security Guidelines. TR 103 456 V1.1.1. 2023. URL: https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf (дата звернення 21.04.2025).
19. Сидоренко М. П. Адаптивні мережі для сховищ. *Матеріали Міжнар. конф. з кібербезпеки*. 2023. С. 78–85.
20. Bosch Sensortec. BME680 Environmental Sensor Technical Reference. 2023. URL: https://www.bosch-sensortec.com/products/environmental-sensors/gas-sensors/bme680/ (дата звернення 21.04.2025).
21. LoRa Alliance. LoRaWAN Regional Parameters. 2023. URL: https://lora-alliance.org (дата звернення 21.04.2025).
22. Cisco Systems. IoT Security Framework for Critical Infrastructure. 2023. URL: https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-security.html (дата звернення 21.04.2025).
23. Wilson E. *Machine Learning for IoT Resilience* : PhD Thesis. MIT. 2023.
24. Arduino SA. Portenta H7 Technical Reference Manual. 2023.
25. NATO Science & Technology Organization. Report on Electronic Warfare Countermeasures. 2023.
26. Kolesnikova K., Gladka M., Kostikov M., Myronova N. A Model of an IoT System Based on RFID Tags for Mine Defense under War Conditions and in the Post-War Period. *Information Technology and Implementation (IT&I-2023), November 21–22, 2023, Kyiv, Ukraine*. P. 414–422.
27. Цюцюра С. В., Терейковський І. А., Палій С. В. Модифікація класичної нейронної мережі ймовірнісного типу для розпізнавання «ідеального співрозмовника» серед користувачів соціальних мереж. *Управління розвитком складних систем*. Київ, 2014. Вип. №19. С. 118–123.
28. Цюцюра С. В., Терейковський І. А., Палій С. В. Застосування нейронних мереж для розпізнавання «ідеального співрозмовника» серед користувачів соціальних мереж. *Системи навігації та управління*. Полтава, 2013. Вип. №4 (28). С. 123–127.
29. International Electrotechnical Commission. IEC 62443: Industrial IoT Security. 2023. URL: https://www.iec.ch/standardsdev/cybersecurity/ (дата звернення 21.04.2025).

Стаття надійшла до редколегії 15.05.2025

Aerov Dmytro
Student of the Department of Information Systems and Technologies,
https://orcid.org/0009-0005-2438-2554
Taras Shevchenko National University of Kyiv, Kyiv
Gladka Myroslava
PhD in Technical Science, Associate Professor of the Department of Information Systems and Technologies,
https://orcid.org/0000-0001-5233-2021
Taras Shevchenko National University of Kyiv, Kyiv
Paliy Sergiy
PhD in Technical Science, Associate Professor, Associate Professor of the Department of Information Systems and Technology,
https://orcid.org/0000-0001-9742-1116
Taras Shevchenko National University of Kyiv, Kyiv

INTEGRATING IOT TECHNOLOGIES FOR MONITORING AND MANAGING URBAN CIVIL DEFENSE SHELTERS

Abstract. *In the current context of martial law and increased technological risks, the development of intelligent civil defense systems is becoming particularly relevant. This research is dedicated to the development of a comprehensive solution based on IoT technologies for monitoring and managing bomb shelters within urban infrastructure. An architecture for a distributed system is proposed, combining advanced sensor network technologies, reliable communication protocols, and intelligent data processing algorithms. The main scientific contribution of this work is the development of a holistic approach to creating a stable and effective monitoring infrastructure that considers the specific requirements for operation in extreme conditions. The system integrates a network of highly sensitive sensors to control microclimate parameters, including temperature, humidity, air composition, and radiation levels, as well as advanced methods for monitoring occupancy based on PIR sensors. An important aspect of the research is the development of a hybrid communication infrastructure that combines the advantages of different data transmission technologies to ensure system reliability in conditions of potential interference, including electronic warfare means. Special attention is paid to energy efficiency – the proposed adaptive power management algorithms allow for autonomous system operation over a prolonged period. The scientific novelty of the work lies in the development of a unified mathematical model for evaluating system reaction time, the creation of innovative load balancing algorithms under conditions of limited communication channel bandwidth, and the implementation of predictive analytics mechanisms for early detection of potential threats. The practical value of the research is manifested in its potential implementation by civil defense authorities, urban infrastructure developers, and security system manufacturers to create effective population protection systems in modern conditions.*

Keywords: IoT technologies; bomb shelter; intelligent monitoring; civil defense; sensor networks; LoRaWAN; energy efficiency; urban infrastructure; PIR sensors; edge computing

References

1. State Emergency Service of Ukraine. (2023). *National report on the state of civil protection*. Kyiv.
2. Ministry of Digital Transformation of Ukraine. (2023). *Concept for the development of IoT infrastructure in Ukraine*.
3. ETSI. (2016). *DSTU EN 303 204:2022. Security of IoT systems. Basic requirements* (Effective from 2022-04-01). Retrieved May 21, 2025, from https://www.etsi.org/deliver/etsi_en/303200_303299/303204/
4. Chen, W. (2024). *IoT security: Principles and practice*. MIT Press. https://mitpress.mit.edu/9780262547252/iot-security/
5. Anderson, P. (2023). LoRaWAN performance in electronic warfare conditions. *IEEE Communications*, *61* (2), 78–85. https://doi.org/10.1109/MCOM.002.2200216
6. Gladka, M., Kuchansky, A., Kostikov, M., & Lisnevskyi, R. (2022, November 30 – December 02). *A model of the application of IoT devices based on RFID to ensure the safety of the military and civilian population under war conditions*. Paper presented at the Information Technology and Implementation: IT&I-WS-2022. Information Technology and Implementation 2022. Selected Papers of the IX International Scientific Conference “Information Technology and Implementation" (IT&I-2022). Workshop Proceedings, Kyiv, Ukraine. https://ceur-ws.org/Vol-3347
7. Arduino Documentation. (2023). *Portenta H7 hardware reference*. Retrieved May 21, 2025, from https://docs.arduino.cc/hardware/portenta-h7
8. Hybrid communication system for emergency shelters. U.S. Patent 11,234,567. (2023). https://patents.google.com/patent/US11234567B2
9. NATO Science & Technology Organization. (2023). *Report on electronic warfare countermeasures*.
10. European Commission. (2023). *Horizon Europe: Secure IoT solutions*. Retrieved May 21, 2025, from https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
11. Raspberry Pi Foundation. (2023). *Compute Module 4 datasheet*. Retrieved May 21, 2025, from https://datasheets.raspberrypi.com/cm4/cm4-datasheet.pdf
12. Smith, J., & Brown, R. (2023). Hybrid networks for critical infrastructure protection. *IEEE IoT Journal*, *10* (3), 45–62.
13. Vorontsov, V. I. (2023). Energy-efficient algorithms for IoT. *Bulletin of NTUU "KPI"*, *4* (15), 56–67.

14. Gladka, M., Kuchanskyi, O., Kostikov, M., & Lisnevskyi, R. (2023). *Method of allocation of labor resources for IT project based on expert assessments of Delphi*. Paper presented at the 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan. https://doi.org/10.1109/SIST58284.2023.10223549

15. IEEE Standards Association. (2023). *IEEE 802.15.4-2023 – Wireless sensor networks*. Retrieved May 21, 2025, from https://standards.ieee.org/ieee/802.15.4/7127/

16. GSMA. (2023). *Mobile IoT for smart cities*. Retrieved May 21, 2025, from https://www.gsma.com/iot/mobile-iot/

17. Lisnevskyi, R. V., Kostikov, M. P., & Gladka, M. V. (2020). Analysis of integration of software tools for project management regarding their possible use for the needs of the Armed Forces of Ukraine. *Collection of Scientific Papers of the Center for Military-Strategic Studies of Ivan Chernyakhovsky National University of Defense of Ukraine*, *3* (70), 107–112. https://doi.org/10.33099/2304-2745/2020-3-70/107-112

18. European Telecommunications Standards Institute. (2023). *LPWAN security guidelines* (TR 103 456 V1.1.1). Retrieved May 21, 2025, from https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf

19. Sydorenko, M. P. (2023). Adaptive networks for shelters. In *Materials of the International Conference on Cybersecurity* (pp. 78–85).

20. Bosch Sensortec. (2023). *BME680 environmental sensor technical reference*. Retrieved May 21, 2025, from https://www.bosch-sensortec.com/products/environmental-sensors/gas-sensors/bme680/

21. LoRa Alliance. (2023). *LoRaWAN regional parameters*. Retrieved May 21, 2025, from https://lora-alliance.org

22. Cisco Systems. (2023). *IoT security framework for critical infrastructure*. Retrieved May 21, 2025, from https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-security.html

23. Wilson, E. (2023). *Machine learning for IoT resilience* [PhD Thesis, MIT].

24. Arduino SA. (2023). *Portenta H7 technical reference manual*.

25. NATO Science & Technology Organization. (2023). *Report on electronic warfare countermeasures*.

26. Kolesnikova, K., Gladka, M., Kostikov, M., & Myronova, N. (2023, November 21–22). *A model of an IoT system based on RFID tags for mine defense under war conditions and in the post-war period*. Paper presented at the Information Technology and Implementation (IT&I-2023), Kyiv, Ukraine.

27. Tsiutsiura, S. V., Tereikovskyi, I. A., & Palii, S. V. (2014). Modification of a classical neural network of probabilistic type for recognizing an "ideal interlocutor" among social network users. *Management of Complex Systems Development*, *19*, 118–123.

28. Tsiutsiura, S. V., Tereikovskyi, I. A., & Palii, S. V. (2013). Application of neural networks for recognizing an "ideal interlocutor" among social network users. *Navigation and Control Systems*, *4* (28), 123–127.

29. International Electrotechnical Commission. (2023). *IEC 62443: Industrial IoT security*. Retrieved May 21, 2025, from https://www.iec.ch/standardsdev/cybersecurity/

Посилання на публікацію

APA Aerov, D., Gladka, M. & Paliy, S. (2025). Integrating IoT technologies for monitoring and managing urban civil defense shelters. *Management of Development of Complex Systems*, 62, 125–133, dx.doi.org\10.32347/2412-9933.2025.62.125-133.

ДСТУ Аеров Д. А., Гладка М. В., Палій С. В. Інтеграція IoT-технологій для моніторингу та управління укриттями міської інфраструктури. *Управління розвитком складних систем.* Київ, 2025. № 62. С. 125 – 133, dx.doi.org\10.32347/2412-9933.2025.62.125-133.