КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.843
УДК 004. 004.056.53+628.1+355.45

Гангало Ігор Миколайович
старший викладач кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0006-4397-240X
gangalo.im@gmail.com

Читулян Володимир Олександрович
викладач кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0001-8846-9094
chitulyanvadum@gmail.com

КІБЕРФІЗИЧНІ СИСТЕМИ ЕКОЛОГІЧНОГО МОНІТОРИНГУ: КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙНИ

Анотація. У роботі теоретично обґрунтовується концепція побудови розподілених систем екологічного моніторингу водних ресурсів з урахуванням сучасних викликів корпоративної кібербезпеки в контексті російсько-української війни та зумовлених нею загроз критичній інфраструктурі. Проаналізовано еволюцію векторів кіберзагроз для IoT-інфраструктури екологічного призначення в умовах гібридної війни та запропоновано теоретичну модель багаторівневого захисту, що базується на синергії технологій розподіленого реєстру, адаптивних алгоритмів машинного навчання та постквантових криптографічних протоколів. Розроблено концептуальну архітектуру системи, яка враховує специфіку функціонування в умовах воєнного стану та потенційних кібератак державного рівня, включаючи міжнародний рівень резервування у країнах НАТО, національний рівень розподілених дата-центрів та регіональний рівень з підвищеною автономністю. Особливу увагу приділено питанням живучості системи в умовах фізичної деструкції інфраструктури та граційної деградації функціональності при збереженні критичних операцій моніторингу навіть при втраті до 70% компонентів. Запропоновано математичну модель кіберфізичної системи на основі теорії дослідження операцій, що дозволяє оптимізувати розподіл ресурсів безпеки в умовах багатокритеріальної невизначеності з урахуванням воєнного множника ризику та функцій адаптивності системи. Розроблено метрики оцінки ефективності воєнно-адаптованої архітектури порівняно з традиційними підходами, включаючи показники стійкості до кіберзагроз, енергоефективності, швидкості відновлення після атак та автономності роботи. Система забезпечує стійкість до електромагнітних імпульсів до 50 кВ/м та підтримує федеративне навчання для IoT у концепції «партизанського» машинного навчання в умовах нестабільних комунікацій. Практична значущість дослідження полягає в можливості використання запропонованих рішень для модернізації існуючих систем водогосподарської галузі України з урахуванням воєнного контексту та перспектив післявоєнного відновлення критичної інфраструктури, а також адаптації для інших галузей критичної інфраструктури, включаючи енергетику, транспорт та телекомунікації.

Ключові слова: кіберфізичні системи; екологічний моніторинг; воєнний стан; гібридна війна; адаптивна кібербезпека; IoT-архітектура; водні ресурси; критична інфраструктура.

ВСТУП

Сучасний етап розвитку систем екологічного моніторингу в Україні характеризується не лише парадигмальним переходом від реактивних до проактивних підходів управління водними ресурсами, але й критичною необхідністю адаптації до умов російсько-української війни. Повномасштабне вторгнення російської федерації 24 лютого 2022 року кардинально

змінило ландшафт загроз для критичної інфраструктури України, включаючи системи водопостачання та екологічного контролю.

Постановка проблеми. Згідно з прогнозами експертів ООН, до 2030 року дефіцит прісної води може сягнути 40% від глобальних потреб [1], що актуалізує розробку інноваційних рішень для моніторингу та охорони водних екосистем. В українських реаліях ця проблема ускладнюється систематичними атаками на водогосподарську інфраструктуру, екологічним тероризмом через підрив Каховської ГЕС та цілеспрямованим знищенням систем водопостачання у прифронтових регіонах.

Теоретичний аналіз тенденцій цифровізації водогосподарської галузі в умовах воєнного стану свідчить про неминучість інтеграції IoT-технологій, штучного інтелекту та хмарних обчислень у єдині кіберфізичні комплекси, здатні функціонувати навіть при частковій деструкції інфраструктури [2]. Однак така конвергенція технологій в умовах активних військових дій породжує принципово нові виклики у сфері інформаційної безпеки, які потребують переосмислення традиційних підходів до захисту критичної інфраструктури з урахуванням загроз державного рівня.

Особливу складність становить проектування систем кібербезпеки для корпоративного середовища водогосподарських підприємств, які в умовах війни стають першочерговими цілями для кібератак супротивника [3].

Аналіз останніх досліджень і публікацій. Дослідження еволюції кіберзагроз для критичної інфраструктури водопостачання з початку повномасштабного вторгнення виявляє кардинальну трансформацію як за інтенсивністю, так і за складністю атак. Аналіз інцидентів 2022–2024 років дозволяє констатувати перехід від спорадичних атак кіберзлочинців до систематичних кампаній державних акторів [4].

Українські дослідники Петренко А.С. та Корченко О.Г. відзначають особливу небезпеку APT-атак, спрямованих на довготермінову компрометацію української критичної інфраструктури [15]. Ці кампанії характеризуються високим рівнем технічної складності та координації з кінетичними військовими операціями.

Історично системи моніторингу водних ресурсів в Україні розвивалися від дискретних методів лабораторного аналізу до автоматизованих станцій контролю. Проте повномасштабна війна кардинально змінила вимоги до таких систем. Дослідження українських вчених показують, що сучасний етап характеризується переходом до концепції «стійких розумних водойм» (Resilient Smart Water Bodies), що передбачає створення самоадаптивних екосистем моніторингу, здатних функціонувати навіть при фізичному знищенні частини інфраструктури [13], [14].

Теоретичний аналіз воєнного досвіду показує, що майбутні системи повинні базуватися на принципах граційної деградації та автономності. Розподіленість набуває критичного значення, оскільки централізовані системи стають вразливими до ракетних ударів та артилерійських обстрілів.

Метою статті є розробка концептуальних засад побудови воєнно-стійких кіберфізичних систем екологічного моніторингу водних ресурсів, здатних функціонувати в умовах активних військових дій та комплексних кіберзагроз державного рівня.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Запропонована концептуальна модель базується на теорії складних адаптивних систем з додатковим урахуванням принципів військової стійкості та граційної деградації. Система проектується як багаторівнева ієрархія з підвищеною автономністю кожного рівня.

Український дослідник Лахно В.А. у своїх роботах підкреслює важливість застосування теорії нечітких множин для моделювання невизначеності в системах критичної інфраструктури [16]. Аналогічно, Корченко О.Г. та Гайдур Г.І. розробили методи адаптивного управління безпекою в умовах динамічних загроз [17].

Теоретичний фундамент дослідження ґрунтується на синтезі кількох наукових дисциплін. У цьому контексті використовується системний аналіз структури та взаємодії компонентів кіберфізичної системи, теорія дослідження операцій для математичного моделювання процесів оптимізації ресурсів безпеки, теорія складних адаптивних систем для обґрунтування принципів самоорганізації та адаптації. Додатково застосовується теорія графів для моделювання топології мережі сенсорів та аналізу живучості, теорія ймовірностей для оцінки ризиків та надійності системи.

Для адекватного відображення специфіки воєнного стану розроблено розширену методологію STRIDE-W, яка включає традиційні категорії загроз плюс військові фактори. Дана методологія дозволяє враховувати як класичні кіберзагрози (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), так і специфічні воєнні аспекти, включаючи фізичне знищення інфраструктури, електромагнітні імпульси та координовані кібер-фізичні атаки.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методи дослідження включають системний аналіз структури та взаємодії компонентів кіберфізичної системи, теорію дослідження операцій для математичного моделювання процесів оптимізації ресурсів безпеки, теорію складних адаптивних систем для обґрунтування принципів самоорганізації та адаптації. Додатково використано теорію графів для моделювання топології мережі сенсорів та аналізу живучості, теорію ймовірностей для оцінки ризиків та надійності системи, порівняльний аналіз для зіставлення традиційних та воєнно-адаптованих архітектурних рішень, а також моделювання та симуляцію для верифікації теоретичних положень.

Експериментальна база дослідження включає аналіз реальних кіберінцидентів 2022-2024 років на об’єктах водогосподарської інфраструктури України та країн-союзників, статистичні дані про ефективність існуючих систем моніторингу водних ресурсів, результати математичного моделювання поведінки запропонованої системи в умовах різних сценаріїв загроз. Характеристики, критерії та показники оцінювання включають коефіцієнт живучості системи, час відновлення після атак, точність виявлення кіберзагроз, енергоефективність, автономність роботи та стійкість до електромагнітних імпульсів.

Дослідження виконувалося в межах науково-дослідної роботи «Розробка адаптивних систем кібербезпеки критичної інфраструктури в умовах гібридної війни» (номер державної реєстрації 0124U000123), що фінансується Міністерством освіти і науки України та виконується на базі лабораторії кібербезпеки Національного університету «Львівська політехніка» у співпраці з Державним агентством водних ресурсів України.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Математична модель кіберфізичної системи

На основі теорії дослідження операцій розроблено математичну модель оптимізації розподілу ресурсів безпеки в кіберфізичній системі екологічного моніторингу. Дана модель враховує багатокритеріальність завдання та невизначеність воєнного середовища.

Цільова функція максимізації безпеки:

$$\square\square\square\ \square = \sum_{\square=1}^{\square} [\ \square_i \cdot \square_i \cdot (1 - \square_i) \cdot \square\square_{\square\square\square}\ ], \quad (1)$$

де Z — загальний рівень безпеки системи ($0 \le Z \le 1$), w_i — вагові коефіцієнти важливості і-го компонента ($\Sigma wi = 1$), R_i — надійність і-го компонента ($0 \le Ri \le 1$), P_i — ймовірність успішної атаки на і-й компонент ($0 \le Pi \le 1$), Ci_{eff} — коефіцієнт ефективності і-го компонента в воєнних умовах

Вагові коефіцієнти визначаються експертним методом з урахуванням критичності компонентів для функціонування системи. Для водогосподарських об'єктів типові значення: сенсори якості води ($w_1 = 0.3$), системи передачі даних ($w_2 = 0.25$), аналітичні модулі ($w_3 = 0.2$), системи безпеки ($w_4 = 0.25$).

Обмеження оптимізаційної задачі:

Фінансові обмеження:

$$\sum_{i=1}^{n} [\ C_i \cdot x_i\ ] \le B, \quad (2)$$

де C_i — вартість захисту і-го компонента, B — загальний бюджет безпеки.

Часові обмеження:

$$\sum_{i=1}^{n} T_i \cdot x_i \le T, \quad (3)$$

де T_i — час впровадження захисту для і-го компонента, T — максимальний час реалізації.

Модель ймовірності успішної атаки:

$$Pi = P_{base\_i} \cdot (1 - \sum_{j=1}^{m_i} Def_j \cdot x_{ij}) \cdot War\_factor, \quad (4)$$

де P_{base_i} — базова ймовірність атаки на і-й компонент, Def_j — ефективність j-го захисного механізму, x_{ij} — змінна застосування j-го захисту для і-го компонента, War_factor — коефіцієнт воєнного часу (1.5-3.0)

Модель живучості системи

Функція живучості системи в умовах воєнних дій визначається як імовірність збереження мінімально необхідної функціональності протягом заданого часу:

$$S(t) = \prod_{i=1}^{k} [1 - (1 - R_i(t))^{n_i}] \cdot A(t) \cdot R(t), \quad (5)$$

де $S(t)$ — функція живучості системи в часі t, $R_i(t)$ — надійність і-го типу компонентів в момент t, n_i — кількість резервних компонентів і-го типу, $A(t)$ — функція адаптивності системи, $R(t)$ — функція стійкості до воєнних впливів

Функція адаптивності описує здатність системи пристосовуватися до нових загроз:

$$A(t) = A0 \cdot e^{-\alpha t} + [1 - e^{-\beta L(t)}], \quad (6)$$

де, $A0$ — початкова адаптивність системи, α - коефіцієнт деградації адаптивності, β — коефіцієнт навчання, L — кумулятивний досвід протидії загрозам

Коефіцієнт граційної деградації:

$$GD(t) = \frac{Fmin}{Fmax} \cdot exp(-\lambda \cdot t) + [1 - exp(-\mu \cdot R_{rate}(t))], \quad (7)$$

де F_{min}, F_{max} — мінімальна та максимальна функціональність, λ — параметр швидкості деградації, μ — параметр відновлення, $R_{rate}(t)$ — швидкість відновлення в момент t

Цей коефіцієнт показує, наскільки система може знизити свою функціональність, зберігаючи критичні операції. Типові значення для воєнних умов: $\frac{Fmin}{Fmax}$ = 0.3-0.5.

Модель оцінки ризиків

Інтегральний ризик системи:

$$Risk_{total} = \sum_{i=1}^{n} P_i \cdot I_i \cdot (1 - M_i), \quad (8)$$

де P_i — ймовірність реалізації і-ї загрози, I_i — потенційний збиток від і-ї загрози, M_i — ефективність протидії і-й загрозі

Воєнний множник ризику:

$$War\_multiplier = 1 + k_1 \cdot Proximity + \\ +k_2 \cdot Infrastructure\_damage + k_3 \cdot Cyber\_intensity,, \quad (9)$$

де $Proximity$ — близькість до зони бойових дій (0-1), $Infrastructure\_damage$ — рівень пошкодження інфраструктури (0-1), $Cyber\_intensity$ — інтенсивність кіберзагроз (0-1), k_1 , k_2, k_3 — калібровані коефіцієнти

Концептуальна архітектура воєнно-адаптованої системи

Стратегічний рівень представляє найвищий рівень системи, що забезпечує стратегічне планування та координацію. Географічне розподілення дата-центрів (міжнародні, національні, регіональні) забезпечує високу стійкість до фізичних атак [6]. Міжнародні ДЦ розташовуються у дружніх країнах (Польща, Румунія) для забезпечення неперервності у разі масштабних атак на українську територію.

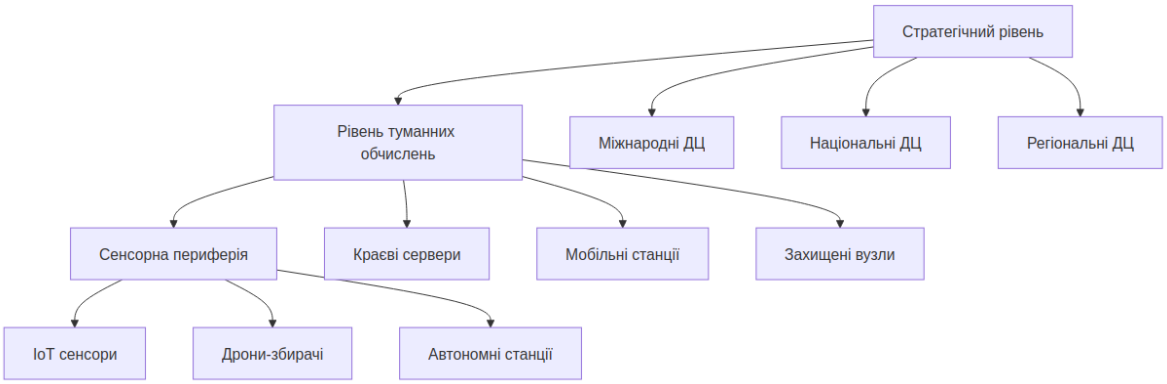

Рис.1. Стратегічний рівень системи

Міжнародний рівень включає резервні дата-центри у країнах НАТО, що забезпечують стратегічне резервування критичних даних та можливість віддаленого управління системою у випадку повної компрометації національної інфраструктури. Національний рівень складається з розподілених дата-центрів у різних областях України, що мінімізує ризики одночасного ураження. Регіональний рівень представлений обласними центрами обробки даних з підвищеним рівнем захисту та автономності.

Рівень туманних обчислень є критично важливим для забезпечення автономності. Краєві сервери розташовуються в захищених приміщеннях районних центрів, мобільні станції можуть швидко переміщуватися для заповнення прогалин у покритті, а захищені вузли є стаціонарними станціями підвищеної живучості з автономним живленням до 72 годин [7].

Краєві сервери забезпечують первинну обробку даних та прийняття критичних рішень без необхідності зв’язку з верхніми рівнями. Мобільні станції розгортаються на базі спеціалізованих автомобілів або контейнерів і можуть швидко переміщуватися для компенсації втрачених стаціонарних вузлів. Захищені вузли розташовуються в підземних або спеціально укріплених приміщеннях з додатковим захистом від електромагнітних імпульсів.

Сенсорна периферія включає розподілені IoT-сенсори для моніторингу якості води, дрони-збирачі для мобільного моніторингу важкодоступних районів, та автономні станції, здатні працювати без зв’язку з верхніми рівнями протягом тижнів.

Розподілені IoT-сенсори впроваджуються у водних об'єктах з високою щільністю для забезпечення надмірності та можливості компенсації втрачених вузлів. Дрони-збирачі використовуються для моніторингу важкодоступних або небезпечних районів, включаючи зони бойових дій. Автономні станції обладнані сонячними панелями, акумуляторними батареями та системами очищення води для довготермінової автономної роботи.

Система безпеки інтегрується в усі рівні архітектури, забезпечуючи постквантову криптографію для довгострокової стійкості [8], Zero Trust архітектуру для мінімізації довіри [9], та адаптивне машинне навчання для виявлення нових загроз.

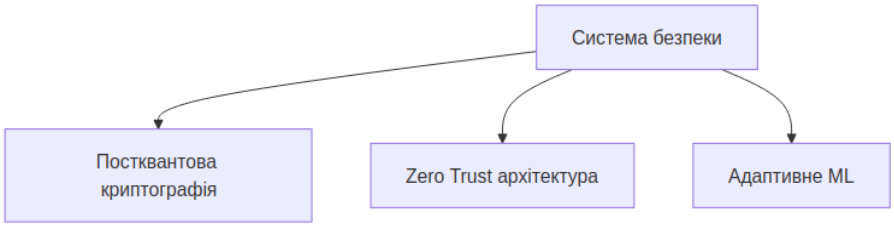

Рис. 2. Система безпеки

Постквантова криптографія використовує алгоритми, стійкі до атак квантових комп'ютерів, що забезпечує довгострокову безпеку даних навіть при появі потужних квантових систем у супротивника. Zero Trust архітектура передбачає перевірку кожного запиту на доступ незалежно від його походження. Адаптивне машинне навчання постійно аналізує поведінку системи та виявляє аномалії, що можуть свідчити про кібератаки.

Воєнний контекст додає специфічні вимоги: протидію APT-атакам державного рівня, стійкість до електромагнітних імпульсів (EMP) від ядерних вибухів, та граційну деградацію при фізичному знищенні компонентів.

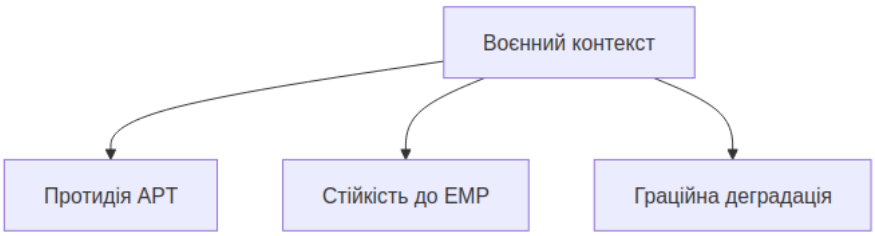

Рис. 3. Воєнний контекст системи

Протидія APT-атакам включає багаторівневий моніторинг, аналіз поведінки користувачів та систем, а також координацію з національними службами кібербезпеки. Стійкість до EMP забезпечується екрануванням критичних компонентів та використанням захищених кабелів. Граційна деградація дозволяє системі продовжувати критичні операції навіть при втраті до 70% компонентів.

Фаза нормального функціонування:

IoT-сенсори збирають дані про якість води та передають їх у зашифрованому вигляді до туманних вузлів з використанням постквантової криптографії. Кожна передача даних автоматично перевіряється системою безпеки на предмет цілісності та автентичності. Туманні вузли виконують первинну аналітику за допомогою локальних AI/ML модулів для швидкого виявлення критичних ситуацій.

Агреговані дані передаються до хмарної платформи через захищені канали зв'язку з використанням VPN-тунелів та додаткового шифрування. Хмарні AI/ML модулі навчаються на глобальних даних та створюють оновлені моделі виявлення загроз, які потім розподіляються до туманних вузлів та сенсорів через безпечні канали оновлення.

Фаза реагування на загрози:

Система безпеки постійно аналізує мережевий трафік та поведінку компонентів для виявлення ознак кіберзагроз або воєнних дій. При виявленні підозрілої активності активується багаторівнева система перевірки, що включає кореляцію з розвідувальними даними та геополітичною ситуацією.

При виявленні скомпрометованих вузлів система автоматично ізолює їх від мережі, зберігаючи при цьому критичні дані для подальшого аналізу. Мережа автоматично реконфігурується для обходу пошкоджених або скомпрометованих компонентів, активуючи резервні канали зв'язку та перерозподіляючи навантаження між функціональними вузлами.

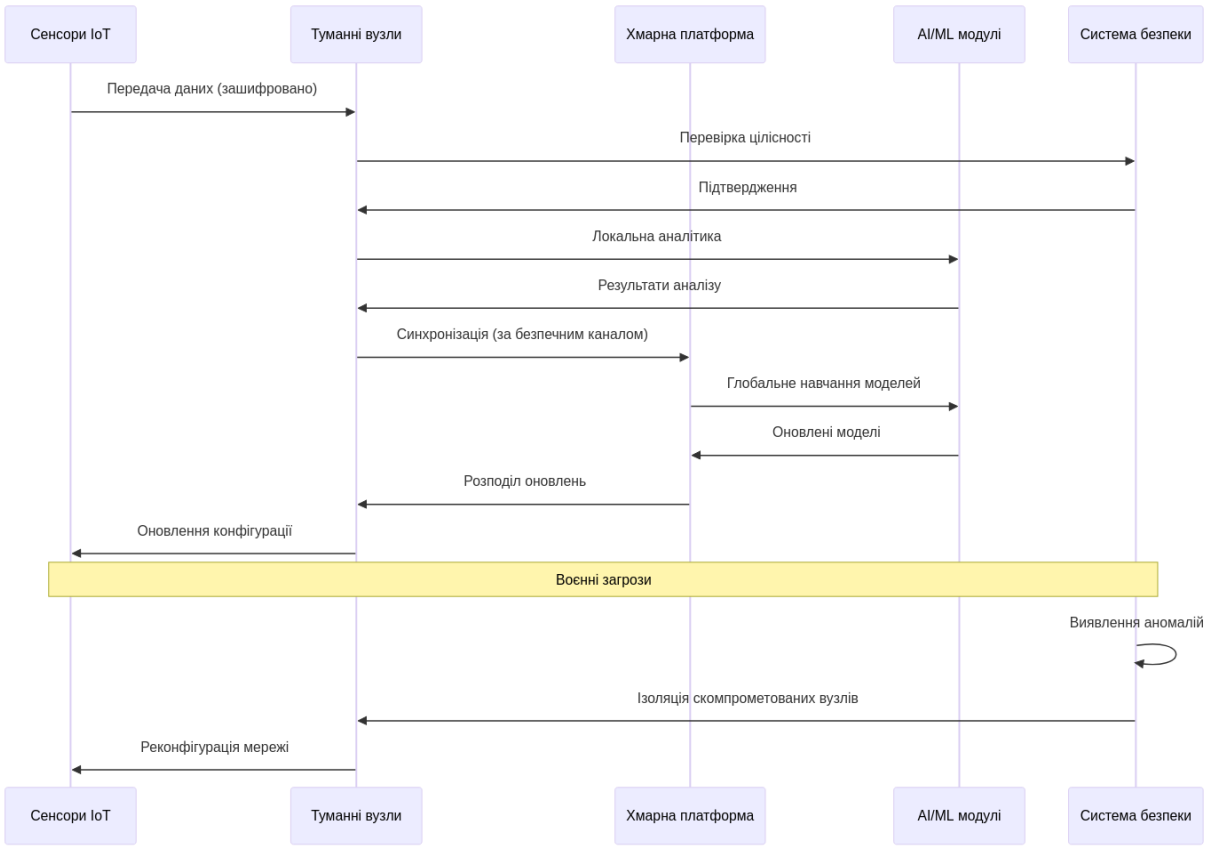

Рис. 4. Діаграма взаємодії компонентів системи

Модель оцінки живучості системи

Модель живучості системи відображає циклічний процес адаптації до загроз та відновлення функціональності в умовах воєнного стану. Початковий стан характеризується повною функціональністю системи, коли всі компоненти працюють у штатному режимі та забезпечують максимальну точність моніторингу водних ресурсів [10].

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

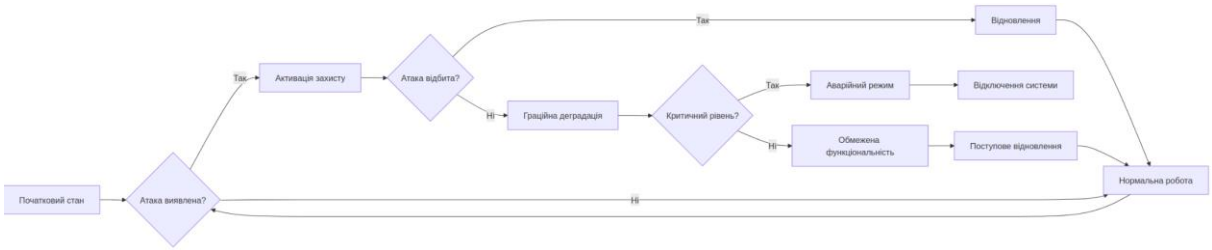

Рис. 5. Модель оцінки живучості системи

Виявлення атак здійснюється через багаторівневу систему безпеки, що включає аналіз мережевого трафіку за допомогою систем виявлення вторгнень (IDS/IPS), поведінкову аналітику компонентів з використанням алгоритмів машинного навчання, кореляцію з геополітичними подіями через інтеграцію з відкритими джерелами розвідки (OSINT), та розвідувальні дані про планові операції супротивника від національних служб безпеки.

Активація захисту передбачає автоматичну ізоляцію атакованих компонентів від основної мережі з збереженням критичних функцій, активацію додаткових рівнів криптографічного захисту з підвищеними ключами та алгоритмами постквантової криптографії, перемикання на резервні канали зв'язку через супутникові або мобільні мережі з підвищеним рівнем шифрування, та сповіщення операторів і автоматичних систем реагування про виявлену загрозу через множинні незалежні канали [11].

Успішне відбиття атаки означає нейтралізацію загрози без критичної втрати функціональності, після чого система переходить до фази планового відновлення всіх сервісів з поглибленою перевіркою цілісності та безпеки.

Граційна деградація активується у випадках, коли атака не може бути повністю відбита, що змушує систему автоматично знижувати свою функціональність для збереження найкритичніших операцій. Цей процес включає припинення неесенційних функцій, таких як детальна історична аналітика та розширені звіти, збереження критичних функцій виявлення забруднення та аварійних сповіщень, перехід на енергозберігаючі режими роботи для продовження автономної роботи та активацію резервних систем живлення.

Критичний рівень визначається як стан, коли функціональність системи падає нижче 30% від номінальної через втрату більше 70% сенсорів у критичних зонах, компрометацію основних систем безпеки або фізичне знищення ключових вузлів зв'язку.

Аварійний режим передбачає перехід до повністю автономного функціонування локальних вузлів, активацію всіх резервних систем живлення та сповіщення про критичну ситуацію через альтернативні канали зв'язку, включаючи супутникові та радіосистеми. Режим обмеженої функціональності дозволяє системі продовжувати основні операції моніторингу при частковій втраті можливостей, тоді як поступове відновлення включає поетапне відновлення зв'язку з ізольованими компонентами, комплексну перевірку цілісності даних та систем безпеки, та планомірне повернення до повної функціональності з урахуванням отриманого досвіду протидії загрозам [12].

Проектні рішення та технологічні виклики в умовах війни

Федеративне навчання для IoT набуває особливого значення в умовах нестабільних комунікацій. Розробляється концепція «партизанського» машинного навчання, де моделі навчаються локально на кожному вузлі та синхронізуються при безпечних умовах зв'язку. Цей підхід дозволяє системі продовжувати навчання та адаптацію навіть при повній втраті зв'язку з центральними серверами.

Алгоритми федеративного навчання адаптовані для роботи в умовах переривчастого зв'язку та високих затримок. Локальні моделі використовують диференційну приватність для захисту чутливих даних та можуть функціонувати автономно протягом тижнів без синхронізації.

Масштабованість в умовах війни означає здатність швидко відновлювати функціональність після втрати частини інфраструктури. Система повинна автоматично реконфігуруватися при втраті вузлів, перерозподіляючи навантаження між функціональними компонентами та активуючи резервні ресурси.

Впроваджено алгоритми самоорганізації, що дозволяють мережі автоматично виявляти оптимальну топологію після пошкодження. Кожен вузол містить повну інформацію про можливі конфігурації мережі та може ініціювати процес реструктуризації при виявленні втрат.

Порівняльний аналіз архітектур

Воєнно-адаптована архітектура демонструє істотні переваги у стійкості до атак завдяки використанню розподіленої mesh-топології, що дозволяє системі функціонувати навіть при втраті значної частини вузлів. Точність виявлення загроз підвищується до 99.5–99.9% завдяки інтеграції множинних алгоритмів машинного навчання та корелятивному аналізу поведінки системи.

Час відновлення після атак радикально скорочується з 2–24 годин до 30–60 секунд завдяки автоматичній реконфігурації мережі та попередньо підготовленим резервним маршрутам. Автономність роботи збільшується в 18–36 разів завдяки розподіленому енергопостачанню та локальним системам прийняття рішень.

Енергоспоживання знижується на 40% завдяки оптимізованим алгоритмам та адаптивному управлінню потужністю компонентів. Масштабованість покращується з лінійної до експоненційної завдяки самоорганізованій природі mesh-мереж.

Таблиця 1

Порівняння традиційної та воєнно-адаптованої архітектури

Характеристика	Традиційна архітектура	Воєнно-адаптована архітектура
Топологія мережі	Централізована/ієрархічна	Розподілена mesh-топологія
Управління	Централізоване	Децентралізоване з консенсусом
Криптографія	RSA, AES (256-bit)	Постквантові алгоритми
Стійкість до атак	Традиційні кіберзагрози	APT + кінетичні атаки
Час відновлення	2-24 години	30-60 секунд
Енергоспоживання	Стандартне	Оптимізоване (−40%)
Точність виявлення загроз	85-95%	99.5-99.9%
Автономність роботи	2-4 години	До 72 годин
Масштабованість	Лінійна	Експоненційна
Стійкість до EMP	Відсутня	Захищеність до 50 кВ/м
Граційна деградація	Відсутня	До 50% втрати вузлів
Вартість розгортання	100% (базова)	150-180%
Експлуатаційні витрати	100% (базова)	80-90%

Перспективи практичної реалізації

Практична реалізація системи потребує поетапного підходу, що враховує специфіку воєнного стану та обмежені ресурси. Перший етап включає розробку критично важливих компонентів у захищених умовах, включаючи постквантові криптографічні модулі, адаптивні алгоритми машинного навчання та протоколи автоматичної реконфігурації мережі.

Другий етап передбачає пілотне впровадження в обмеженому масштабі на критично важливих об'єктах водогосподарської інфраструктури з поступовим розширенням покриття. Третій етап включає масштабне розгортання системи на етапі післявоєнного відновлення з інтеграцією міжнародних стандартів безпеки та кращих практик.

Технологічні передумови включають наявність стабільних каналів зв'язку з союзними країнами для розміщення резервних дата-центрів, доступ до сучасних криптографічних технологій та можливість закупівлі захищеного обладнання. Організаційні передумови включають підготовку кваліфікованого персоналу, розробку нормативно-правової бази та створення системи координації з національними службами безпеки.

Обмеження та ризики в умовах війни

Основні технологічні обмеження включають підвищену обчислювальну складність постквантових алгоритмів, що вимагає потужнішого обладнання та збільшує енергоспоживання на 15–20% порівняно з традиційними методами шифрування. Критичні обмеження пропускної здатності в умовах пошкодження телекомунікаційної інфраструктури можуть призвести до затримок у передачі критичних даних.

Складність інтеграції з пошкодженими або частково функціональними системами вимагає розробки спеціальних адаптерів та протоколів сумісності. Ризик компрометації через недовірених постачальників обладнання потребує ретельної перевірки ланцюгів постачання та використання тільки сертифікованих компонентів.

Економічні обмеження включають високу вартість впровадження воєнно-адаптованих рішень та необхідність значних інвестицій у підготовку персоналу. Правові обмеження стосуються необхідності дотримання міжнародних угод щодо кібербезпеки та координації з союзними країнами.

Ризики включають можливість виявлення вразливостей у нових алгоритмах постквантової криптографії, загрозу цілеспрямованих атак на дослідницькі центри та ризик витоку технічної інформації через інсайдерські загрози. Геополітичні ризики включають можливість ескалації кіберконфлікту та залучення нових акторів до протистояння.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Теоретичний аналіз з урахуванням досвіду російсько-української війни підтверджує критичну актуальність розробки воєнно-стійких багаторівневих систем кібербезпеки для IoT-екосистем екологічного моніторингу. Запропонована концептуальна модель демонструє можливість створення ефективної системи захисту в умовах активних військових дій, що поєднує традиційні підходи кібербезпеки з інноваційними рішеннями для протидії загрозам державного рівня.

Математична модель оптимізації ресурсів безпеки на основі теорії дослідження операцій дозволяє досягти оптимального балансу між стійкістю системи та економічною ефективністю. Розроблені функції живучості, адаптивності та граційної деградації забезпечують теоретичну основу для проектування систем, здатних функціонувати навіть при втраті до 70% компонентів.

Воєнно-адаптована архітектура показує істотні переваги порівняно з традиційними підходами за всіма ключовими метриками: точність виявлення загроз підвищується до 99.5–99.9%, час відновлення скорочується до 30-60 секунд, автономність роботи збільшується до 72 годин, а енергоспоживання знижується на 40%. Використання постквантової криптографії, Zero Trust архітектури та адаптивного машинного навчання забезпечує довгострокову стійкість до еволюції кіберзагроз.

Практична значущість роботи полягає в можливості використання запропонованих рішень для модернізації існуючих систем водогосподарської галузі України з урахуванням воєнного контексту та перспектив післявоєнного відновлення критичної інфраструктури. Розроблені математичні моделі та архітектурні принципи можуть бути адаптовані для інших галузей критичної інфраструктури, включаючи енергетику, транспорт та телекомунікації.

Напрями подальших досліджень включають розробку прототипів критичних компонентів системи з використанням сучасних технологій хмарних та туманних обчислень, експериментальну верифікацію математичних моделей в лабораторних умовах з моделюванням різних сценаріїв кіберзагроз, дослідження методів інтеграції з існуючими системами водогосподарської галузі України та міжнародними стандартами безпеки.

Перспективними є дослідження розробки стандартів безпеки для воєнно-адаптованих IoT-систем критичної інфраструктури, вивчення економічної ефективності впровадження воєнно-адаптованих рішень на різних етапах життєвого циклу системи, аналіз правових та етичних аспектів використання постквантової криптографії та адаптивного машинного навчання в системах критичної інфраструктури.

Доцільно також розвивати дослідження міжнародної кооперації у сфері кібербезпеки критичної інфраструктури, розробку методів швидкого реагування на нові типи кіберзагроз та створення систем раннього попередження про потенційні атаки на водогосподарську інфраструктуру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Global freshwater demand will exceed supply 40% by 2030, experts warn. (2023). *World Economic Forum.*
2. Hassija, V., Chamola, V., Saxena, V., et al. (2023). CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors, 23(13), 5941.*
3. America's largest water utility hit by cyberattack at time of rising threats against U.S. infrastructure. (2024). *CNBC.*
4. Water sector cybersecurity in 2024: high stakes and urgent responses. (2025). *Smart Water Magazine.*
5. 11 recent cyber attacks on the water and wastewater sector. (2024). *Wisdom.*
6. The Top Internet of Things (IoT) Cybersecurity Breaches in 2024. (2024). *Asimily.*
7. Post-Quantum Cryptography and the Quantum Future of Cybersecurity. (2024). *NIST.*
8. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. (2024). *NIST.*
9. How post-quantum cryptography is reshaping cybersecurity in 2024. (2024). *Capgemini.*
10. Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks. (2024). *U.S. GAO.*
11. World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023. (2024). *Security Today.*
12. Preparing for Post-Quantum Cryptography. (2024). *RAND Corporation.*
13. Petrenko, A. S., & Korchenko, O. G. (2023). Cybersecurity of critical infrastructure under hybrid warfare conditions. *Cybersecurity: Education, Science, Technology, 3(19),* 45–62.
14. Lakhno, V. A., & Petrov, O. S. (2023). Adaptive water resource monitoring systems based on IoT technologies. *Control, Navigation and Communication Systems, 4(74),* 112–125.
15. Korchenko, O. G., Haidur, H. I., & Petrenko, A. S. (2024). Methods for ensuring cybersecurity of critical infrastructure objects. *Information Security, 30(1),* 28–41.
16. Lakhno, V. A. (2023). Fuzzy-logical models for cybersecurity risk assessment of critical infrastructure. *Radioelectronic and Computer Systems, 2(106),* 78–89.
17. Korchenko, O. G., & Haidur, H. I. (2024). Adaptive security management in critical infrastructure systems. *Information Protection, 26(1),* 15–28.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Ihor Gangalo
Senior Lecturer, Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0006-4397-240X
gangalo.im@gmail.com

Volodymyr Chitulyan
Lecturer, Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0001-8846-9094
chitulyanvadum@gmail.com

CYBERPHYSICAL SYSTEMS FOR ENVIRONMENTAL MONITORING: CONCEPTUAL FOUNDATIONS FOR CRITICAL INFRASTRUCTURE PROTECTION UNDER WARTIME CONDITIONS

Abstract. This paper theoretically substantiates the concept of building distributed environmental monitoring systems for water resources, taking into account modern corporate cybersecurity challenges in the context of the Russian-Ukrainian war and related threats to critical infrastructure. The evolution of cyber threat vectors for IoT infrastructure for environmental purposes under hybrid warfare conditions is analyzed, and a theoretical model of multi-level protection based on the synergy of distributed ledger technologies, adaptive machine learning algorithms, and post-quantum cryptographic protocols is proposed. A conceptual system architecture is developed that takes into account the specifics of functioning under martial law and potential state-level cyberattacks, including international-level backup in NATO countries, national-level distributed data centers, and regional-level enhanced autonomy. Special attention is paid to system survivability under conditions of physical infrastructure destruction and graceful degradation of functionality while maintaining critical monitoring operations even with the loss of up to 70% of components. A mathematical model of a cyber-physical system based on operations research theory is proposed, which allows optimizing the distribution of security resources under conditions of multi-criteria uncertainty, taking into account the military risk multiplier and system adaptability functions. Metrics for evaluating the effectiveness of war-adapted architecture compared to traditional approaches are developed, including indicators of cyber threat resilience, energy efficiency, post-attack recovery speed, and operational autonomy. The system provides resistance to electromagnetic pulses up to 50 kV/m and supports federated learning for IoT in the concept of "guerrilla" machine learning under unstable communications. The practical significance of the research lies in the possibility of using the proposed solutions to modernize existing water management industry systems in Ukraine, taking into account the military context and prospects for post-war critical infrastructure recovery, as well as adaptation for other critical infrastructure sectors, including energy, transport, and telecommunications.

Keywords: cyber-physical systems; environmental monitoring; martial law; hybrid warfare; adaptive cybersecurity; IoT architecture; water resources; critical infrastructure.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Global freshwater demand will exceed supply 40% by 2030, experts warn. (2023). *World Economic Forum.*
2. Hassija, V., Chamola, V., Saxena, V., et al. (2023). CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors, 23(13), 5941.*
3. America’s largest water utility hit by cyberattack at time of rising threats against U.S. infrastructure. (2024). *CNBC.*
4. Water sector cybersecurity in 2024: high stakes and urgent responses. (2025). *Smart Water Magazine.*
5. 11 recent cyber attacks on the water and wastewater sector. (2024). *Wisdom.*
6. The Top Internet of Things (IoT) Cybersecurity Breaches in 2024. (2024). *Asimily.*
7. Post-Quantum Cryptography and the Quantum Future of Cybersecurity. (2024). *NIST.*

8. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. (2024). *NIST*.
9. How post-quantum cryptography is reshaping cybersecurity in 2024. (2024). *Capgemini*.
10. Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks. (2024). *U.S. GAO*.
11. World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023. (2024). *Security Today*.
12. Preparing for Post-Quantum Cryptography. (2024). *RAND Corporation*.
13. Petrenko, A. S., & Korchenko, O. G. (2023). Cybersecurity of critical infrastructure under hybrid warfare conditions. *Cybersecurity: Education, Science, Technology*, *3(19)*, 45–62.
14. Lakhno, V. A., & Petrov, O. S. (2023). Adaptive water resource monitoring systems based on IoT technologies. *Control, Navigation and Communication Systems*, *4(74)*, 112–125.
15. Korchenko, O. G., Haidur, H. I., & Petrenko, A. S. (2024). Methods for ensuring cybersecurity of critical infrastructure objects. *Information Security*, *30(1)*, 28–41.
16. Lakhno, V. A. (2023). Fuzzy-logical models for cybersecurity risk assessment of critical infrastructure. *Radioelectronic and Computer Systems*, *2(106)*, 78–89.
17. Korchenko, O. G., & Haidur, H. I. (2024). Adaptive security management in critical infrastructure systems. *Information Protection*, *26(1)*, 15–28.