DOI: https://doi.org/10.36910/6775-2524-0560-2025-59-12
УДК 004.9
Готович Володимир Анатолійович, к.т.н., доцент
https://orcid.org/0000-0003-2143-6818
Карташов Віталій Вікторович, к.т.н., доцент
https://orcid.org/0000-0003-0530-3919
Максим'як Юрій Богданович, аспірант
https://orcid.org/0009-0008-2489-8659
Матійчук Любомир Павлович, д.е.н., доцент
https://orcid.org/0000-0001-6701-4683
Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна

ЗАДАЧА РОЗРОБКИ ПРОГРАМНОЇ ПЛАТФОРМИ ДЛЯ МІСЦЕВОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО ОПОВІЩЕННЯ

Готович В. А., Карташов В. В., Максим'як Ю. Б., Матійчук Л. П. Задача розробки програмної платформи для місцевої автоматизованої системи централізованого оповіщення. У статті розглядається задача створення сучасної програмної платформи для місцевої автоматизованої системи централізованого оповіщення (МАСЦО), яка є ключовим елементом інфраструктури цивільного захисту в умовах зростаючої загрози надзвичайних ситуацій та воєнного стану. Проаналізовано чинну нормативно-правову базу України, зокрема Концепцію модернізації системи централізованого оповіщення, а також зарубіжні приклади реалізації подібних систем (Emergency Alert в Австралії, WEA у США, Reverse 112 в ЄС). У результаті проведеного аналізу запропоновано багаторівневу хмарно-орієнтовану архітектуру платформи за моделлю «cloud-edge», у якій критичні сервіси (керування сценаріями, база даних, обробка подій) розміщені у хмарі, а безпосереднє доведення сигналів забезпечують локальні шлюзи та кінцеві пристрої (електросирени, гучномовці, інформаційні табло). Описано функціональні можливості платформи: автоматизоване або ручне запускання сигналів тривоги, мультиканальне інформування населення (через сирени, SMS, Cell Broadcast, телебачення, інтернет), підтримка сценаріїв, віддалене адміністрування, візуалізація стану системи на електронній мапі, а також моніторинг і тестування обладнання. Значну увагу приділено питанням кібербезпеки: реалізовано багаторівневу авторизацію, журналювання дій, шифрування команд, резервування каналів і інфраструктури. Платформа підтримує інтеграцію з існуючим обладнанням та службами через стандартизовані протоколи (NAPAPI, CAP) і передбачає подальший розвиток за такими напрямами: впровадження AI-модулів прогнозування загроз, інтеграція з ГІС, мобільними додатками (зокрема "Дія"), підтримка IoT-пристроїв, блокчейн-аудит, інклюзивність інтерфейсів. Запропоноване рішення дозволяє суттєво підвищити надійність, масштабованість і швидкість реагування системи, відповідає міжнародним практикам і може стати основою для модернізації оповіщення на рівні територіальних громад.
Ключові слова: система централізованого оповіщення, МАСЦО, хмарна архітектура, cloud-edge, телекомунікаційна мережа, інформування населення, надзвичайні ситуації, цивільний захист.

Hotovych H., Kartashov V., Maksymyak Y., Matiichuk L. The task of developing a software platform for a local automated centralized alert system. The article explores the development of a modern software platform for a local automated centralized public warning system (LAPWS), which serves as a key component of civil protection infrastructure amid increasing risks of emergencies and wartime conditions. The study analyzes the current legal and regulatory framework in Ukraine, including the Concept for the modernization of the centralized public warning system, as well as foreign implementations such as Australia's Emergency Alert, the U.S. Wireless Emergency Alerts (WEA), and the EU's Reverse 112 systems. Based on this analysis, the article proposes a multi-level cloud-oriented platform architecture following the "cloud-edge" model, where critical services (scenario management, database operations, and event processing) are hosted in the cloud, while the direct delivery of alerts is handled by local edge gateways and end-user devices (electronic sirens, loudspeakers, and digital signage). The functional capabilities of the platform are described in detail: automated or manual initiation of alarm signals, multi-channel public alerting (via sirens, SMS, Cell Broadcast, TV, and the Internet), scenario-based operation, remote administration, real-time visualization of system status on a digital map, and hardware monitoring and testing. Particular attention is given to cybersecurity measures, including multi-level user authorization, activity logging, command encryption, and infrastructure redundancy. The platform supports integration with existing equipment and national systems through standardized protocols (NAPAPI, CAP) and envisions further development in areas such as AI-based threat prediction, integration with geographic information systems (GIS), mobile applications (including "Diia"), IoT support, blockchain-based audit trails, and inclusive interface design. The proposed solution significantly improves system reliability, scalability, and response time, aligns with international best practices, and offers a practical foundation for modernizing emergency alert systems at the community level.
Keywords: centralized public warning system, LAPWS, cloud architecture, cloud-edge, telecommunications network, public alerting, emergencies, civil protection.

Постановка задачі. Забезпечення своєчасного та ефективного оповіщення населення про загрозу або виникнення надзвичайних ситуацій є одним із ключових завдань національної системи цивільного захисту. У контексті сучасних викликів, зокрема повномасштабної війни, кліматичних

катастроф і технологічних ризиків, значно зростає потреба у надійних, масштабованих та захищених інструментах для інформування громадян.

Оповіщення населення про загрозу або виникнення надзвичайних ситуацій є одним із ключових завдань цивільного захисту на державному і місцевому рівнях. Від оперативності та надійності системи централізованого оповіщення залежить своєчасне реагування населення на небезпеку, мінімізація можливих втрат і збитків. Зокрема, під час повітряних тривог, які стали частими в умовах повномасштабної агресії проти України, ефективність систем оповіщення безпосередньо впливала на життя та безпеку населення в містах і селищах. Існуюча система оповіщення України була створена ще у 1970–1980-х роках за командно-сигнальним принципом і наразі не відповідає сучасним вимогам [1]. Структура успадкованої системи не враховує сучасної організації органів влади, нової структури цивільного захисту та сучасних технологічних можливостей [1]. У зв'язку з цим Урядом було схвалено Концепцію розвитку та технічної модернізації системи централізованого оповіщення (2018 р.) [1] і затверджено План заходів її реалізації [2]. Цими документами передбачено поступове оновлення загальнодержавної автоматизованої системи оповіщення та створення ефективних територіальних і місцевих підсистем. Задача розробки сучасної програмної платформи для місцевої автоматизованої системи централізованого оповіщення (МАСЦО) є актуальним і пов'язаним із загальнодержавними заходами у сфері цивільного захисту, зокрема технічної модернізації систем оповіщення.

Дана задача ускладнюється фрагментарністю підходів до впровадження локальних систем оповіщення, відсутністю уніфікованої платформи, недостатньою інтеграцією з національними системами ДСНС та обмеженими можливостями адаптації до різних каналів доведення інформації до населення (мобільні мережі, Інтернет, радіо, телебачення). Крім того, постає необхідність забезпечення високого рівня кібербезпеки та надійності, підтримки сучасних принципів цифрової трансформації й міжсистемної взаємодії.

Таким чином, розробка єдиної МАСЦО є актуальною науково-технічною задачею, яка знаходиться на перетині інтересів державної безпеки, інформаційних технологій, телекомунікацій, системного проєктування та кіберзахисту. Її вирішення дозволить підвищити ефективність реагування на надзвичайні ситуації, зменшити рівень збитків та забезпечити стійкість функціонування критичної інфраструктури. Запропоновані рішення можуть бути використані органами місцевого самоврядування та ДСНС при створенні або модернізації локальних систем оповіщення. Впровадження описаної платформи дозволить підвищити ефективність і оперативність оповіщення населення про надзвичайні ситуації, забезпечити сумісність обладнання різних виробників, централізований контроль та високий рівень надійності системи в цілому. Наведені рекомендації щодо подальших робіт вказують напрям для розробників і відповідальних служб у реалізації сучасної МАСЦО.

Огляд сучасних досліджень і рішень, проблемні аспекти. Питанню оповіщення населення та модернізації відповідних систем присвячено ряд нормативних актів і науково-практичних досліджень. Зокрема, постановою Кабінету Міністрів України №733 (2017 р.) затверджено Положення про організацію оповіщення і зв'язку у сфері цивільного захисту, яке визначає структуру та функції єдиної державної системи оповіщення [3]. В цьому Положенні встановлено поділ на загальнодержавну систему, територіальні та локальні підсистеми, включаючи місцеві автоматизовані системи централізованого оповіщення на рівні областей, районів, громад і міст. Згідно з наведеним в Положенні визначенням, місцева автоматизована система оповіщення населення – це програмно-технічний комплекс, призначений для доведення сигналів і повідомлень керівному складу місцевих органів влади та населенню на відповідній території адміністративно-територіальної одиниці [4]. Наказом МВС України №93 (2019 р.) затверджено Інструкцію щодо проектування, впровадження в експлуатацію, експлуатації та технічного обслуговування автоматизованих систем централізованого оповіщення [5], що встановлює вимоги до створення таких систем. Це нормативне підґрунтя підкреслює увагу держави до стандартизації та надійності систем оповіщення.

Попри наявність законодавчої бази, реалізація сучасних рішень на місцях стикається з низкою труднощів. Аналіз стану місцевих систем оповіщення показує, що багато з них перебувають у застарілому чи навіть занедбаному стані та функціонують з низькою ефективністю [6]. Причинами

цьому є обмежене фінансування, зношеність обладнання (електросирени радянського зразка, аналогові засоби зв'язку тощо), а також фрагментарність модернізації систем в різних регіонах. Деякі міста і громади вже впроваджують нові локальні системи оповіщення, але відсутність єдиної платформи призводить до розрізненості рішень та проблем сумісності. Зокрема, відзначається недостатня інтеграція з сучасними каналами оповіщення (мобільні мережі, інтернет-платформи), обмежені можливості дистанційного контролю стану обладнання та кіберзахисту систем.

Варто звернути увагу на досвід зарубіжних країн, які успішно реалізували сучасні системи оповіщення населення. Наприклад, в Австралії діє національна система Emergency Alert, яка дозволяє екстреним службам надсилати голосові повідомлення на стаціонарні телефони і текстові SMS-повідомлення на мобільні телефони у визначеній зоні небезпеки [7]. У США функціонує інтегрована система оповіщення IPAWS, що включає технологію Wireless Emergency Alerts (WEA) – надсилання коротких екстрених оповіщень на мобільні телефони за технологією стільникового мовлення (cell broadcast) з географічним таргетуванням [8]. В Європейському Союзі з 2018 року законодавчо зобов'язано всі країни-члени впровадити системи оповіщення, що здатні розсилати попередження на телефони громадян у визначеному районі (так звані служби "Reverse 112"). Згідно з Європейським кодексом електронних комунікацій, з червня 2022 року кожна держава ЄС повинна забезпечити можливість надсилання таких оповіщень на мобільні пристрої населення [9]. При цьому наголошується на багатоканальному підході: окрім мобільних телефонів, задіюються також сирени, радіо і телебачення, інтернет-сайти, соцмережі, електронна пошта тощо – щоб максимально охопити всі верстви населення [9]. Впроваджені за кордоном технології демонструють ефективність поєднання централізованого керування з різноманітними каналами доведення інформації, а також важливість забезпечення стійкості та кібербезпеки таких систем. Цей досвід є цінним орієнтиром для України при розробці власної програмної платформи МАСЦО.

Необхідність вирішення зазначених проблем та врахування кращих світових практик обумовлює актуальність дослідження і розробки єдиної програмної платформи для місцевих систем оповіщення. Основними викликами є: відсутність стандартизації програмно-апаратних рішень, несумісність компонентів (сирени, засоби зв'язку, програмне забезпечення), обмежена інтеграція з загальнонаціональною системою, потреба у впровадженні нових каналів оповіщення (мобільні сповіщення, інтернет-додатки) при збереженні надійності традиційних засобів (стаціонарні сирени, радіомовлення), а також необхідність забезпечення високого рівня кібербезпеки системи. Таким чином, постає завдання чіткого визначення вимог та архітектури програмної платформи МАСЦО, яка б відповідала сучасним критеріям ефективності, оперативності та безпеки.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на наявність нормативного регулювання та окремі спроби модернізації систем централізованого оповіщення в Україні, залишаються нерозв'язаними на науково-методичному та інженерному рівнях такі задачі:

1. Досі відсутня уніфікована, масштабована та стандартизована програмна платформа для побудови МАСЦО, здатна інтегруватися з національними інфраструктурами ДСНС, а також підтримувати різнорідні кінцеві пристрої (цифрові сирени, табло, мобільні канали тощо);
2. Реалізація сучасної хмарноорієнтованої архітектури системи з підтримкою принципу «cloud-edge», що дозволяє забезпечити одночасно централізоване управління і локальну автономність у разі втрати зв'язку. Задача потребує розробки спеціалізованих сценаріїв передачі команд, механізмів резервування, автоматичного відновлення функціонування та подолання затримок у телеметрії;
3. Вирішення комплексу питань інформаційної безпеки, включаючи застосування сучасних криптографічних протоколів, механізмів автентифікації, журналювання подій та захисту від кіберзагроз у розподіленому середовищі.

Також малодослідженими залишаються аспекти інтеграції з джерелами даних про загрози (давачі, моніторингові системи, геоінформаційні платформи), автоматичного запуску сценаріїв оповіщення, та підтримки інклюзивних каналів інформування (Text-to-Speech, мультимовність, адаптація для осіб з інвалідністю).

Мета дослідження. Метою дослідження є наукове обґрунтування та розробка архітектурного і функціонального підходу до створення програмної платформи для МАСЦО, яка забезпечує високу надійність, масштабованість, інформаційну безпеку та здатність до інтеграції з

національними та регіональними системами цивільного захисту. У межах цієї мети дослідження передбачає аналіз нормативно-правових та технічних передумов побудови таких систем, визначення вимог до ключових компонентів платформи, моделювання її загальної структури з використанням сучасних хмарних технологій, опис механізмів багатоканального інформування та розробку принципів забезпечення кіберстійкості та міжсистемної взаємодії. Очікуваним результатом є формування цілісної концепції уніфікованої платформи МАСЦО, що може бути практично реалізована в умовах цифрової трансформації сфери цивільного захисту.

Основні результати дослідження. На основі проведеного огляду науково-технічних публікацій та діючих нормативних документів виявлено значні недоліки відомих інформаційних систем. В даній роботі пропонується програмна платформа МАСЦО, яка реалізує гібридну модель «cloud-edge». Усі критичні сервіси (управління, обробка подій, зберігання конфігурацій і журналів) розгортаються в публічній або державній хмарі (наприклад, на базі Microsoft Azure), що забезпечує автоматичне масштабування, георезервування та керовану безпеку (рис. 1). На території громад залишаються лише "тонкі" шлюзи (edge-gateway) – компактні промислові контролери або одноплатні комп'ютери, підключені до локальної мережі пристроїв оповіщення (сирен, табло, гучномовців). Кожен такий шлюз відповідає за обмін телеметрією з хмарою, кешування критичних сценаріїв, підтримку черг локального кешу для подій, що не були передані через втрату зв'язку, і їх автоматичну ретрансляцію після відновлення з'єднання. Завдяки цьому шлюз забезпечує автономну роботу при короткочасній або нестабільній втраті зв'язку, не втрачаючи критичних подій або команд.

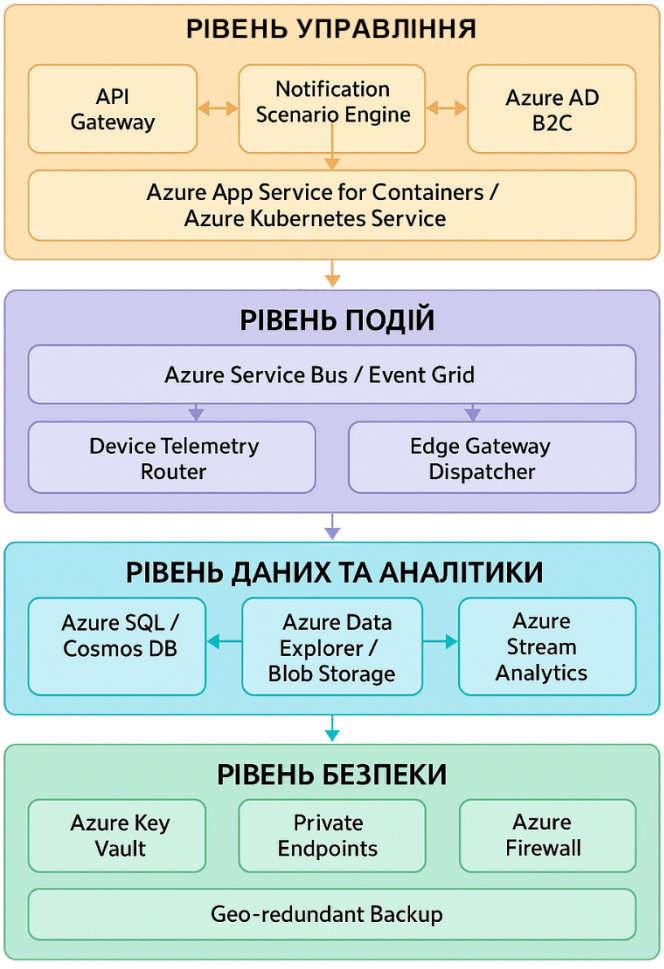

Рис. 1. Архітектура хмарного шару програмної платформи МАСЦО

У хмарі функціонують декілька рівнів, які взаємодіють на основі подієвої (event-driven) моделі через асинхронні черги Service Bus / Event Grid. Це забезпечує стійкість до відмов окремих компонентів і еластичне масштабування трафіку. До таких рівнів належать:

- рівень управління включає мікросервіси, розгорнуті в контейнерах (Azure App Service for Containers або Azure Kubernetes Service), які приймають команди операторів, формують сценарії оповіщення, проводять аутентифікацію та авторизацію (Azure AD B2C) і публікують команди у шину повідомлень;
- рівень подій – керована шина (Azure Event Grid чи Service Bus), що гарантує доставку команд до edge-шлюзів і збір телеметрії від пристроїв;
- рівень даних та аналітики – функціонує як PaaS. Тут використовується БД (Azure SQL / Cosmos DB) з даними конфігурації, а дані телеметрії та логи пишуться до Azure Data Explorer або Blob Storage. Також наявна потокова аналітика (Azure Stream Analytics), що виявляє аномалії й автоматично запускає сценарії;
- рівень безпеки – секрети й ключі зберігаються в Azure Key Vault, мережевий доступ обмежено приватними кінцевими точками та Azure Firewall; резервні копії автоматично реплікуються у вторинний регіон.

Робочі місця операторів взаємодіють із хмарою через веб-інтерфейс або мобільний застосунок; доступ можливий з будь-якого місця на основі захищеного каналу HTTPS/VPN. Критичні мікросервіси розгортаються у декількох регіонах з автоматичним переключенням трафіку (Azure Front Door / Traffic Manager). Така хмарно-орієнтована архітектура усуває потребу у дорогому локальному дата-центрі, спрощує масштабування системи разом із розширенням мережі сирен і мінімізує час відновлення після відмови.

Основні компоненти та їх функції. Програмна платформа МАСЦО складається з кількох ключових компонентів (рис. 2).

Рис. 2. Основні компоненти програмної платформа МАСЦО

На даному рисунку:

- рівень управління – набір керованих сервісів PaaS (веб-API, мікросервіси сценаріїв оповіщення, шина повідомлень і база даних конфігурації), розгорнутих у кількох регіонах хмари. Шар забезпечує централізовану логіку оповіщення, аутентифікацію користувачів і інтеграцію з національною системою ДСНС. Дані зберігаються у керованих БД (Azure SQL / Cosmos DB) з автоматичним резервуванням, журнали подій – у Data Lake;
- комунікаційний рівень – набір апаратно-програмних засобів, що здійснюють передачу сигналів від сервера до кінцевих пристроїв. Він підтримує декілька типів інтерфейсів: мережеві (TCP/IP), радіоінтерфейси (через радіомодеми DMR чи інші), телефонні лінії. Комунікаційний модуль кодує повідомлення оповіщення у відповідний формат для кожного каналу (наприклад, формує пакет для увімкнення сирени через радіоканал або SIP-повідомлення для VoIP оповіщення по мережі);
- пристрої оповіщення – апаратні пристрої які безпосередньо доводять сигнал до населення. Найбільш розповсюджені – це електросирени, які можуть подавати гучний звуковий сигнал тривоги (сирени потужністю 400–1200 Вт, встановлені на дахах будівель чи окремих опорах) [5]. Сучасні сирени забезпечують дистанційне керування режимами звучання і можуть мати вбудовані гучномовці для трансляції мовних повідомлень. Окрім сирен, до кінцевих пристроїв можуть належати системи гучномовного зв'язку (вуличні гучномовці), пристрої передачі повідомлень на локальне FM-радіо або кабельне телебачення, SMS- або Cell Broadcast шлюзи для розсилки оповіщень на мобільні телефони, інформаційні електронні табло, а також спеціальні пристрої для оповіщення установ (наприклад, внутрішні сирени на промислових об'єктах, школи тощо). Усі такі пристрої оснащені модулями зв'язку для прийому команд від центрального серверу;
- інтерфейс оператора (програмне забезпечення АРМ) – призначений для користувачів системи (чергових диспетчерів, адміністраторів). Інтерфейс надає можливості запуску оповіщення (вручну чи вибором заздалегідь підготовленого сценарію), контролю за перебігом оповіщення, а також моніторингу стану системи. Важливою функцією є візуалізація: на екрані оператора відображається електронна карта місцевості з позначками всіх точок встановлення сирен та інших пристроїв, їх поточний статус (справний, несправний, активований тощо) [5]. Оператор може вибірково вмикати оповіщення в окремих зонах або для окремих груп пристроїв, що особливо корисно при локальних надзвичайних ситуаціях. Інтерфейс також дозволяє скласти текст екстреного повідомлення, який потім буде передано каналами зв'язку (наприклад, як SMS чи голосове повідомлення). Окрім ручного введення, підтримується вибір шаблонів повідомлень і попередньо збережених сценаріїв, що значно спрощує роботу оператора в умовах стресу або обмеженого часу на реагування.

Пропонована програмна платформа повинна забезпечувати декілька режимів роботи для різних ситуацій. Основний режим – автоматизоване оповіщення при надзвичайній ситуації. Система цілодобово моніторить канали отримання сигналів тривоги: це можуть бути сигнали від регіонального центру (територіальної автоматизованої системи), команди від ДСНС України або натискання "тривожної кнопки" місцевим черговим. При надходженні сигналу "Увага всім" система негайно запускає алгоритм оповіщення: передає команду на увімкнення всіх електросирен у зоні відповідальності, а також розсилає інші повідомлення згідно зі сценарієм. Сценарій може передбачати паралельне відправлення голосового оповіщення по телекомунікаційних мережах (наприклад, автоматичний обдзвін керівного складу по телефону, розсилка SMS населенню тощо). Важливо, що сучасна система може надавати не лише звуковий сигнал сирени, а й супровідну інформацію. Зокрема, після звучання сирени може слідувати мовне повідомлення з інструкціями для населення (через гучномовці), або текстові повідомлення для різних груп отримувачів. Наприклад, керівники установ отримають повідомлення з вимогою ввімкнути локальні системи оповіщення і провести евакуацію, а населення – інформацію про характер небезпеки та найближчі укриття.

Окрім аварійного режиму, платформа підтримує режим планового інформування і тестування. Регламентні випробування системи (щомісячні чи щоквартальні перевірки сирен) можуть здійснюватися автоматично у попередньо запланований час [4]. Програмне забезпечення проводить дистанційне тестування: короткочасно запускає сигнали або здійснює беззвучний тест

(перевіряючи підключення і стан кожної сирени), фіксує результати і формує звіт для технічного персоналу. Такі можливості суттєво полегшують обслуговування системи.

Оскільки система оповіщення є критично важливою, особлива увага приділяється захисту від несанкціонованого доступу, збоїв та кібератак. В програмній платформі реалізовано багаторівневий захист, який охоплює ідентифікацію користувачів, захищені канали обміну, фізичну та програмну надійність компонентів, а також заходи щодо відновлення після збоїв.

Аутентифікація та авторизація реалізуються шляхом використання надійних паролів і двофакторної автентифікації, з диференціацією прав доступу відповідно до ролей користувачів. Усі дії операторів фіксуються в журналі подій для подальшого аудиту.

Передача команд до кінцевих пристроїв здійснюється із застосуванням шифрування, зокрема протоколів SSL/TLS для IP-мереж або захищених радіоалгоритмів, що виключає можливість перехоплення або фальсифікації сигналів оповіщення.

Серверна частина платформи працює в захищеному хмарному середовищі з використанням міжмережевих екранів, засобів антивірусного захисту, автоматичного резервного копіювання та регулярного оновлення програмного забезпечення. Критичні компоненти резервуються: передбачено дублюючий сервер і альтернативні канали зв'язку на випадок виходу з ладу основного обладнання.

Фізичну надійність забезпечують кінцеві пристрої, які мають автономні джерела живлення (акумулятори, сонячні панелі) та автоматичне перемикання на резерв у разі зникнення основного живлення [4].

Завдяки узгодженому застосуванню цих заходів досягається цілісний рівень інформаційної безпеки та стійкості системи до зовнішніх і внутрішніх загроз.

Розроблювана програмна платформа спроєктована з відкритою архітектурою, що полегшує її інтеграцію з іншими системами та розширення функціональності. Зокрема, підтримується сумісність з обладнанням різних виробників, що вже використовується на об'єктах цивільного захисту. На основі стандартизованих протоколів (NAPAPI – National Alerting Protocol API, або міжнародний стандарт CAP – Common Alerting Protocol) система може автоматично приймати сигнали від загальнодержавної системи оповіщення та передавати їх далі на місцевий рівень без втручання людини. Аналогічно, місцева система здатна ретранслювати екстрені повідомлення до широкого кола інших каналів: автоматично оприлюднювати повідомлення на офіційних веб-сайтах органів влади, у мобільних додатках, надсилати їх до централізованих медіасистем (телебачення, радіо) тощо.

Важливою функцією є інтеграція з джерелами даних про небезпеки – наприклад, з автоматизованими системами моніторингу (метеорологічними давачами, системами спостереження за станом дамб, давачами на підприємствах). Програмна платформа може отримувати від них попереджувальні сигнали і за визначеними алгоритмами автоматично ініціювати оповіщення при перевищенні порогових значень (наприклад, сигнал від сейсмографа про землетрус). Така взаємодія перетворює систему оповіщення на частину ширшої екосистеми "розумного" протистояння надзвичайним ситуаціям.

Розроблювана платформа МАСЦО забезпечує п'ять взаємопов'язаних груп функцій, що охоплюють повний цикл оповіщення – від формування сигналу до післяаварійного аналізу. До таких функціональних груп належать:

1. Формування та ініціація оповіщення – створення сигналів тривоги вручну або автоматично на основі зовнішніх подій, шаблонів сценаріїв або даних з моніторингових систем;
2. Багатоканальне доведення інформації – передача повідомлень через сирени, гучномовці, мобільні повідомлення (SMS, Cell Broadcast, push), радіо, телебачення, електронні табло, вебінтерфейси та інші засоби;
3. Моніторинг і самодіагностика – контроль стану кінцевих пристроїв у реальному часі, виявлення несправностей, ведення журналів подій і технічних перевірок;
4. Адміністрування та управління конфігурацією – налаштування зон оповіщення, прав доступу, розкладів тестувань і сценаріїв сповіщення через централізований інтерфейс;
5. Аналітика та аудит подій – збір телеметрії, оцінка ефективності оповіщення, формування звітів і аналіз післяаварійних дій, зокрема із залученням засобів штучного інтелекту.

Платформа забезпечує централізоване й дистанційне керування процесом оповіщення: оператор через веб-консоль або мобільний застосунок може одним клацанням активувати всі сирени чи обрати конкретні групи сирен, а також запустити попередньо налаштовані сценарії для різних типів надзвичайних ситуацій. Одночасно реалізується принцип мультиканальності, що поєднує звукові сирени, мовні повідомлення через гучномовці, SMS-, Cell-Broadcast- та push-сповіщення на мобільні телефони, електронні листи, інтеграцію з інформаційними табло, локальним FM-радіо й кабельним телебаченням, забезпечуючи максимальне охоплення аудиторії та дублювання критичної інформації різними носіями [9].

Безперервний моніторинг і самодіагностика обладнання дають змогу у реальному часі відстежувати параметри кожного кінцевого пристрою оповіщення (живлення, заряд акумулятора, стан корпусу, температура тощо); результати регламентних тестів автоматично фіксуються у журналі, а у разі відхилень генерується сповіщення про технічну тривогу [4]. Гнучкість та масштабованість досягаються завдяки можливості легкого додавання нових пристроїв, перегрупування зон оповіщення, призначення ролей користувачам і підключення додаткових каналів (наприклад, 5G/LTE-M або інтеграції з мобільним застосунком «Дія») без зупинки сервісу. Відмовостійкість і безпека гарантуються резервуванням каналів зв'язку, джерел живлення та хмарних сервісів, що забезпечує безперервність оповіщення навіть за умови часткового пошкодження інфраструктури у воєнний час чи під час стихійних лих.

Завдяки такій композиції функцій платформа досягає високого рівня автоматизації, залишаючи за оператором контроль критичних рішень. У підсумку така локальна система здатна оперативно реагувати на зовнішні команди та внутрішні сигнали небезпеки, доводячи до населення як загальний сигнал тривоги, так і детальні інструкції щодо дій у надзвичайній ситуації.

Висновки та перспективи подальших досліджень. Проведений аналіз підходів до побудови МАСЦО та розроблена концепція програмної платформи підтверджують досяжність створення уніфікованого рішення на місцевому рівні. Запропонована хмарно-орієнтована архітектура «cloud-edge» із управлінським функціоналом в державній або публічній хмарі та периферійними edge-шлюзами забезпечує масштабованість, георезервування та функцію управління безпекою. Поєднання багатоканальних засобів зв'язку з інтелектуальними кінцевими пристроями (цифровими сиренами, табло, мобільними сповіщеннями) створює комплексне рішення, що відповідає сучасним вимогам швидкості, надійності та кіберстійкості. Рішення узгоджується з державною Концепцією модернізації оповіщення [1] і може стати технічною основою для практичної реалізації Плану заходів [2].

Подальший розвиток платформи передбачає декілька взаємопов'язаних векторів:

- Перший – впровадження AI-підтримки прийняття рішень на основі застосування модулів машинного навчання, здатних прогнозувати розвиток надзвичайних ситуацій, визначати зони ураження за телеметрією сенсорних мереж і формувати рекомендації щодо оптимальних сценаріїв оповіщення;
- Другий – поглиблення інтеграції з геоінформаційними системами (ArcGIS, QGIS, Azure Maps) для візуалізації зон небезпеки у реальному часі, планування маршрутів евакуації та автоматизованого вибору пристроїв оповіщення;
- Третій – розширення функціоналу шляхом підтримки 5G/LTE-M для IoT-сирен, інтеграції з мобільним застосунком «Дія» та системою e-SMS, запровадження блокчейн-аудиту журналів і забезпечення мультимовних та інклюзивних каналів (субтитри, TTS-синтез);
- Четвертий – заходи щодо поглиблення рівня кібербезпеки, зокрема впровадження zero-trust-моделі доступу, використання апаратних модулів безпеки (HSM) для підписування команд і застосування AI-систем виявлення аномалій;
- П'ятий – міжрегіональна та міжнародна інтероперабельність на основі стандартизації форматів обміну даними між рівнями системи та сумісності із платформами сусідніх країн для координації дій у прикордонних зонах.

Практична реалізація зазначених напрямів досліджень дозволить підвищити ефективність і технологічну зрілість місцевих систем оповіщення, зробити їх частиною єдиної цифрової екосистеми безпеки та цивільного захисту.

Список бібліографічного опису:

1. Кабінет Міністрів України. Розпорядження від 31.01.2018 № 43-р «Про схвалення Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій». – 2018. – URL: https://zakon.rada.gov.ua/laws/show/43-2018-р (дата звернення: 15.04.2025).
2. Кабінет Міністрів України. Розпорядження від 11.07.2018 № 488-р «Про затвердження плану заходів щодо реалізації Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій». – 2018. – URL: https://zakon.rada.gov.ua/laws/show/488-2018-р.
3. Кабінет Міністрів України. Постанова від 27.09.2017 № 733 «Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту». – 2017. – URL: https://zakon.rada.gov.ua/laws/show/733-2017-п.
4. Створення місцевої автоматизованої системи оповіщення та забезпечення цивільного захисту населення м. Чернігів : звіт / ТОВ «ІНЛ Компані». – URL: https://chernigiv-rada.gov.ua/storage/files/22/00/00/03/a30cec24a4ffdceed6463241ca75fb20.pdf (дата звернення: 15.04.2025).
5. Міністерство внутрішніх справ України. Наказ від 08.02.2019 № 93 «Про затвердження Інструкції щодо ... проектування, введення в експлуатацію, експлуатації та технічного обслуговування автоматизованих систем централізованого оповіщення» (зареєстрований в Мін'юсті 25.02.2019 за № 418/33289). – URL: https://zakon.rada.gov.ua/laws/show/z0418-19.
6. Дем'янчук І.Я. Оповіщення населення великих міст про загрозу або виникнення надзвичайних ситуацій: реалізація повноважень органів управління // *Ефективність державного управління*. – 2019. – №3(60), с.82–93.
7. Australian Government. *Emergency Alert – National Telephone Warning System*. – URL: https://www.emergencyalert.gov.au (дата звернення: 15.04.2025).
8. Federal Communications Commission (USA). *Wireless Emergency Alerts (WEA) – FCC Consumer Guide*. – URL: https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea (дата звернення: 15.04.2025).
9. European Emergency Number Association (EENA). Public Warning in Europe: EECC Article 110 implementation. – 2022. – URL: https://eena.org/our-work/eena-special-focus/public-warning/ (дата звернення: 15.04.2025).

References:

1. Kabinet Ministriv Ukrainy. Rozporiadzhennia vid 31.01.2018 No. 43-r "Pro skhvalennia Kontseptsii rozvytku ta tekhnichnoi modernizatsii systemy tsentralizovanoho opovishchennia pro zahrozu vynyknennia abo vynyknennia nadzvychainykh sytuatsii". – 2018. – Available at: https://zakon.rada.gov.ua/laws/show/43-2018-p (Accessed: 15 April 2025).
2. Kabinet Ministriv Ukrainy. Rozporiadzhennia vid 11.07.2018 No. 488-r "Pro zatverdzhennia planu zakhodiv shchodo realizatsii Kontseptsii rozvytku ta tekhnichnoi modernizatsii systemy tsentralizovanoho opovishchennia". – 2018. – Available at: https://zakon.rada.gov.ua/laws/show/488-2018-p (Accessed: 15 April 2025).
3. Kabinet Ministriv Ukrainy. Postanova vid 27.09.2017 No. 733 "Pro zatverdzhennia Polozhennia pro orhanizatsiiu opovishchennia pro zahrozu vynyknennia abo vynyknennia nadzvychainykh sytuatsii ta orhanizatsiiu zviazku u sferi tsyvilnoho zakhystu". – 2017. – Available at: https://zakon.rada.gov.ua/laws/show/733-2017-п (Accessed: 15 April 2025).
4. INL Kompani LLC. Stvorennia mistsevoi avtomatyzovanoi systemy opovishchennia ta zabezpechennia tsyvilnoho zakhystu naselennia m. Chernihiv: zvit. – Available at: https://chernigiv-rada.gov.ua/storage/files/22/00/00/03/a30cec24a4ffdceed6463241ca75fb20.pdf (Accessed: 15 April 2025).
5. Ministerstvo vnutrishnikh sprav Ukrainy. Nakaz vid 08.02.2019 No. 93 "Pro zatverdzhennia Instruktsii shchodo proiektuvannia, vvedennia v ekspluatatsiiu, ekspluatatsii ta tekhnichnoho obsluhovuvannia avtomatyzovanykh system tsentralizovanoho opovishchennia". – 2019. – Available at: https://zakon.rada.gov.ua/laws/show/z0418-19 (Accessed: 15 April 2025).
6. Demianchuk I.Ya. Opovishchennia naselennia velykykh mist pro zahrozu abo vynyknennia nadzvychainykh sytuatsii: realizatsiia povnovazhen orhaniv upravlinnia // Efektyvnist derzhavnoho upravlinnia. – 2019. – No. 3(60), pp. 82–93.
7. Australian Government. Emergency Alert – National Telephone Warning System. – Available at: https://www.emergencyalert.gov.au (Accessed: 15 April 2025).
8. Federal Communications Commission (USA). Wireless Emergency Alerts (WEA) – FCC Consumer Guide. – Available at: https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea (Accessed: 15 April 2025).
9. European Emergency Number Association (EENA). Public Warning in Europe: EECC Article 110 implementation. – 2022. – Available at: https://eena.org/our-work/eena-special-focus/public-warning/ (Accessed: 15 April 2025).