

DOI: <https://doi.org/10.36910/6775-2524-0560-2025-59-13>

УДК 004.9

Готович Володимир Анатолійович, к.т.н., доцент

<https://orcid.org/0000-0003-2143-6818>

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 ім. І.Пулля, м Тернопіль, Україна

ІННОВАЦІЙНІ ВЕКТОРИ РОЗВИТКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МІСЦЕВОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО ОПОВІЩЕННЯ (МАСЦО)

Готович В. А., Максим'як Ю. Б., Матійчук Л. П. Інноваційні вектори розвитку програмного забезпечення місцевої автоматизованої системи централізованого оповіщення (МАСЦО). В роботі проведено системний аналіз потенціалу розвитку програмного забезпечення місцевої автоматизованої системи централізованого оповіщення (МАСЦО) шляхом впровадження сучасних цифрових технологій. Дослідження ґрунтується на огляді наукових публікацій, технічної документації та практичного досвіду у сфері систем оповіщення, штучного інтелекту, IoT, Smart City, мобільних застосунків і блокчейн-технологій. На основі проведеного дослідження виокремлено п'ять інноваційних напрямів модернізації ПЗ МАСЦО: застосування штучного інтелекту (ШІ) та машинного навчання для інтелектуалізації оповіщення; інтеграція системи з інфраструктурою Smart City; використання Інтернету речей (IoT) як мережі датчиків-тригерів; розробка мобільних застосунків та відкритих API для розширення каналів оповіщення; впровадження технології блокчейн для підвищення надійності та прозорості. Вперше комплексно розглянуто міждисциплінарний підхід до розвитку ПЗ МАСЦО, що охоплює ШІ, IoT, Smart City, мобільні технології та блокчейн. Програмне забезпечення МАСЦО слід розвивати як адаптивну платформу цифрової трансформації громад, здатну до самонавчання, автоматичного реагування та безпечної взаємодії з іншими системами. Необхідне державне стимулювання інновацій – нормативне, фінансове та організаційне – для впровадження розроблених напрямів у практику цивільного захисту.

Ключові слова: система оповіщення, інформування населення, місцева автоматизована система централізованого оповіщення, МАСЦО, штучний інтелект, IoT, Smart City, мобільний застосунок, блокчейн-технологія.

Gotovych V., Maksymyak Yu., Matychuk L. Innovative Vectors for the Development of Software for the Local Automated Centralized Notification System (LACNS). This paper conducts a systematic analysis of the potential development of software for the Local Automated Centralized Notification System (LACNS) through the implementation of modern digital technologies. The research is based on a review of scientific publications, technical documentation, and practical experience in the fields of notification systems, artificial intelligence, IoT, Smart City, mobile applications, and blockchain technologies. Based on the conducted research, five innovative directions for modernizing LACNS software have been identified: Application of artificial intelligence (AI) and machine learning to enhance notification intelligence; Integration of the system with Smart City infrastructure; Use of the Internet of Things (IoT) as a network of trigger sensors; Development of mobile applications and open APIs to expand notification channels; Implementation of blockchain technology to improve reliability and transparency. For the first time, a comprehensive interdisciplinary approach to the development of LACNS software has been considered, covering AI, IoT, Smart City, mobile technologies, and blockchain. The LACNS software should be developed as an adaptive platform for the digital transformation of communities, capable of self-learning, automatic response, and secure interaction with other systems. State incentives for innovation-regulatory, financial, and organizational-are necessary for implementing these directions in civil protection practices.

Keywords: notification system, public information, Local Automated Centralized Notification System (LACNS), artificial intelligence, IoT, Smart City, mobile application, blockchain technology.

Постановка наукової проблеми. Сучасні виклики – від стихійних лих до техногенних аварій і воєнних загроз – вимагають від систем оповіщення більшої інтелектуальності та інтегративності. Існуючі програмно-технічні комплекси оповіщення потребують модернізації через впровадження новітніх IT-рішень. Зокрема, актуальним є використання штучного інтелекту для інтелектуального аналізу даних про надзвичайні ситуації в режимі реального часу. Важливим напрямом є зв'язок МАСЦО з компонентами Smart City – міськими інформаційними системами, датчиками та пристроями керування інфраструктурою. Перспективи відкриває повсюдне впровадження Інтернету речей (Internet of Things, IoT) – мережі датчиків, що можуть автоматично генерувати сигнали тривоги. Паралельно, розвиток мобільних технологій дозволяє розробити зручні застосунки та відкриті API для охоплення максимальної аудиторії та інтеграції різних платформ (наприклад, державних сервісів на кшталт «Дія»). Окремо слід зазначити потенціал

блокчейн-технологій у контексті систем оповіщення – вони можуть забезпечити незмінність і верифікованість повідомлень, прозорий аудит дій системи під час НС.

Мета роботи. Розкрити інноваційні напрями розвитку програмного забезпечення МАСЦО, що дозволять значно підвищити функціональність, надійність і адаптивність систем оповіщення. Для досягнення мети вирішуються такі завдання як аналіз можливості застосування ШІ/машинного навчання у програмному забезпеченні МАСЦО, дослідження шляхів інтеграції ПЗ оповіщення з концепцією Smart City, визначення ролі IoT як джерела автоматичних тригерів НС, оцінка переваг розробки мобільних застосунків та відкритих API для МАСЦО, з'ясування потенціалу блокчейн для забезпечення цілісності та довіри в системах оповіщення.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Проблематика оперативного оповіщення населення про надзвичайні ситуації (НС) є критичною для забезпечення безпеки громад. В Україні функціонує багаторівнева система оповіщення у сфері цивільного захисту, де місцева автоматизована система централізованого оповіщення (МАСЦО) відповідає за оповіщення на рівні територіальних громад, міст та селищ [1]. МАСЦО забезпечує передачу інформації на локальному рівні з метою оперативного попередження мешканців про можливі небезпеки [1]. Традиційно такі системи спираються на стаціонарні сирени, радіо- і телетрансляцію, однак у цифрову епоху зростають вимоги до їх функціональності, надійності й адаптивності.

Інтеграція штучного інтелекту та машинного навчання в системи оповіщення. Рис. 1. пропонує конкретні кроки впровадження ШІ та глибинного навчання у ПЗ МАСЦО.

Розвиток штучного інтелекту (ШІ) створює нові можливості для автоматизації та інтелектуалізації процесів оповіщення про надзвичайні ситуації. Глибинне навчання (deep learning) та інші методи машинного навчання дозволяють обробляти великі масиви даних у реальному часі і виявляти складні закономірності, недоступні традиційним алгоритмам. У контексті МАСЦО це означає, що система може навчитися розрізняти типи загроз, прогнозувати розвиток ситуації та пріоритизувати тривожні сповіщення.

За допомогою алгоритмів машинного зору та аналізу сигналів ШІ здатен автоматично розпізнавати ознаки різних надзвичайних ситуацій. Наприклад, система відеомоніторингу з навченою нейромережею може виявити ознаки лісової пожежі на ранній стадії (дим, вогонь) ще до того, як люди отримають повідомлення, і тим самим дати більше часу на реагування. У Каліфорнії вже використовують ШІ для аналізу зображень з камер спостереження з метою виявлення осередків займання лісу раніше за людину[2]. Аналогічно, акустичні сенсори, проаналізовані за допомогою глибинних нейромереж, можуть розрізняти звуки (наприклад, вибух, сирена, скло, що розбивається) та класифікувати подію як вибуховий інцидент, аварію чи акт вандалізму. Така класифікація в режимі реального часу забезпечує вибір правильного сценарію оповіщення для кожного типу загрози.



Рис. 1. Схема впровадження ШІ та глибинного навчання у ПЗ МАСЦО

Штучний інтелект здатен не лише виявити факт надзвичайної ситуації, а й швидко оцінити її можливі наслідки. Модель, натренована на даних про попередні надзвичайні події, може миттєво

спрогнозувати зону ураження або кількість потенційно постраждалих. Наприклад, при виявленні землетрусу визначеної магнітуди система на основі даних про забудову і населеність районів прогнозує ймовірні руйнування та потребу в евакуації. У випадку хімічної аварії алгоритми можуть оцінити напрямок розповсюдження небезпечних речовин (з урахуванням метеоданих) та згенерувати попередження для зон ураження. Таким чином, інтеграція моделей прогнозування в ПЗ МАСЦО дозволяє автоматично генерувати сценарії оповіщення з урахуванням очікуваних наслідків, що суттєво підвищує ефективність реагування.

В умовах одночасного надходження великої кількості сигналів (наприклад, множинні спрацювання датчиків або кілька паралельних НС) ІІІ може допомогти визначити пріоритетність оповіщень. Машинне навчання здатне враховувати такі фактори, як масштаб загрози, достовірність джерела сигналу, густота населення в зоні ризику тощо, і на основі цього вирішувати, які оповіщення повинні бути надіслані негайно і яким каналом. Крім того, інтелектуальні фільтри на базі ML можуть відсіювати хибні спрацювання датчиків або дублюкатні повідомлення, зменшуючи інформаційне навантаження на операторів та населення. В результаті система оповіщення стає більш надійною і сфокусованою на найбільш критичних загрозах.

Отже, впровадження ІІІ та глибинного навчання у ПЗ МАСЦО дозволяє системі «навчитися думати» – самостійно розпізнавати типи загроз, прогнозувати розвиток подій і оптимально керувати потоком сповіщень. Це переводить оповіщення на якісно новий рівень *проактивності*: якщо традиційна система просто передає заздалегідь запрограмований сигнал, то інтелектуалізована система аналізує ситуацію і вибирає найдоречніший спосіб оповіщення для мінімізації наслідків НС. Важливо, що людський фактор не усувається повністю – найкращі результати дає співпраця ІІІ та оператора, коли ІІІ пропонує рішення, а людина-керівник НС затверджує або коригує їх на основі свого досвіду та контексту.

Доповіді свідчать, що вже нині можливе створення автоматизованих систем сповіщення, які самі генерують оповіщення на основі аналізу даних від зовнішніх джерел. Так, аналітики Deloitte описують концепцію, за якою ІІІ-модуль приймає метеорологічні дані (наприклад, від Національного управління океанічних і атмосферних досліджень NOAA), проганяє їх через модель прогнозу погоди і автоматично формує серію попереджень для відповідних районів – тим самим мешканці отримують більше часу на підготовку до урагану чи іншого стихійного лиха[3]. Подібні рішення демонструють потенціал ІІІ у підвищенні оперативності та точності систем оповіщення.

Інтеграція ПЗ МАСЦО з концепцією Smart City. Рис. 2 відображає схему інтеграції МАСЦО в цифрову інфраструктуру Smart City

Концепція *Smart City* («розумного міста») передбачає застосування сучасних ІТ-рішень для управління міською інфраструктурою та сервісами з метою підвищення якості життя мешканців. Система оповіщення як критичний компонент безпеки міста повинна органічно інтегруватися в цю концепцію. Інтеграція МАСЦО зі Smart City означає взаємодію програмного забезпечення оповіщення з іншими міськими інформаційними платформами та керуючими пристроями в реальному часі.

У сучасних містах функціонують ситуаційні центри та платформи моніторингу (міський дата-центр, геоінформаційні системи, системи відеоспостереження тощо). ПЗ МАСЦО може бути підключене до єдиної міської платформи, отримуючи від неї аналітику і дані про інциденти. Навзаєм, система оповіщення надає інформацію про активовані тривоги та їх статуси в міський центр управління. Така обмінна інтеграція забезпечує узгодженість дій: наприклад, якщо МАСЦО виявила загрозу і розпочала оповіщення, місто може автоматично перевести служби екстреного реагування у підвищену готовність, опираючись на сигнал від системи оповіщення. В ідеалі, МАСЦО стає частиною *єдиного інформаційного простору міста*, де всі системи «розмовляють однією мовою» через відкриті стандартизовані протоколи (наприклад, Common Alerting Protocol, CAP).

Інтеграція дозволяє МАСЦО безпосередньо задіяти *актуатори* міської інфраструктури для доведення сигналів та забезпечення безпеки. Зокрема, система оповіщення може автоматично вмикати електронні інформаційні табло на вулицях і в громадських місцях з відображенням повідомлень про небезпеку. Відомо, що у багатьох сучасних містах екстрені повідомлення можуть перебивати трансляцію реклами на цифрових білбордах та екранах, аби донести критичну інформацію до населення. Аналогічно, МАСЦО, інтегрована зі системою керування дорожнім рухом, може переводити світлофори в особливий режим під час евакуації (наприклад, відкривати

“зелену хвилю” на виїздах з небезпечної зони або блокувати в’їзд). Через інтеграцію з системами оповіщення громадського транспорту ПЗ МАСЦО може передавати екстрені оголошення безпосередньо в автобуси, тролейбуси, метро. Такий рівень взаємодії значно підвищує охоплення оповіщення і сприяє *скоординованим заходам реагування* на рівні всього міста.



Рис. 2. Схема інтеграції МАСЦО в цифрову інфраструктуру Smart City

Концепція Smart City передбачає не лише передачу команд до пристроїв, а й збирання інформації від них (принцип двостороннього зв'язку). У випадку системи оповіщення це може проявлятися у формі отримання підтверджень та даних від різних кінцевих точок. Наприклад, “розумні” інформаційні панелі можуть повідомляти в центр, чи успішно вони показали сигнал тривоги. Смарт-камери можуть надати зображення ситуації на евакуаційних шляхах в режимі реального часу для оцінки, як населення реагує на сигнали. Ба більше, мешканці міста через мобільні застосунки або спеціальні сенсори можуть надсилати зворотній сигнал (наприклад, кнопки екстреного виклику, підключені до міської мережі). Отримання такого фідбеку дозволяє оперативно коригувати дії: якщо з певного району масово надходять повідомлення від користувачів про відсутність сирен чи проблеми, система оповіщення може дублювати сигнал іншими каналами для цієї зони. За даними фахівців, сучасна система оповіщення має забезпечувати не лише передачу повідомлень в один бік, але й дати отримувачам можливість відповісти, надавши статус чи запит про допомогу[4]. Такий двосторонній обмін даними перетворює систему оповіщення з пасивного мовника на активний канал взаємодії влади та громади під час кризи.

Інтеграція систем оповіщення зі Smart City поступово здійснюється у провідних містах світу. В Сеулі та Токіо існують міські інформаційні системи, де сповіщення про землетруси або інші НС автоматично надходять на всі цифрові табло в метро, на зупинках та в торговельних центрах. У європейських містах запроваджується практика, коли сповіщення з міського центру цивільного захисту через API надходять до навігаційних систем автомобілів (інформуючи водіїв про надзвичайну ситуацію і рекомендовані дії). В Україні концепція “розумних міст” лише набирає обертів, але вже є приклади інтеграції: зокрема, у Києві діє міський ситуаційний центр, до якого планують підключити систему оповіщення для централізованого контролю сирен та інформування через міські сервіси.

Отже, синергія МАСЦО та Smart City відкриває можливості для ширшого й ефективнішого оповіщення. Система оповіщення перестає бути ізольованим інструментом, а стає частиною єдиної “нервової системи” міста. Це забезпечує комплексний підхід до безпеки: від автоматичного увімкнення засобів оповіщення до адаптивного керування міськими процесами під час НС. В результаті, мешканці отримують інформацію швидше та зручніше, рішення щодо реагування приймаються з урахуванням повної картини, а наслідки надзвичайних ситуацій мінімізуються завдяки злагодженим діям усіх елементів міської інфраструктури.

Інтернет речей (IoT) як джерело автоматичних тригерів НС. Рис. 3 відображає Інтеграція IoT у програмне забезпечення МАСЦО



Рис. 3. Інтеграція IoT у програмне забезпечення МАСЦО

Інтернет речей (Internet of Things, IoT) – це мережа фізичних пристроїв, обладнаних датчиками, підключених до Інтернету для збору і обміну даними. У сфері систем оповіщення IoT виконує роль “очей і вух” – тобто розгалуженої сенсорної інфраструктури, яка здатна автоматично виявляти ознаки небезпеки та генерувати сигнали тривоги без участі людини. Впровадження IoT-технологій у ПЗ МАСЦО дозволить реалізувати автоматичне спрацювання системи оповіщення при настанні певних умов (тригерів), що істотно скорочує затримку між виникненням надзвичайної ситуації та початком оповіщення.

Різноманітні датчики можуть безперервно контролювати критичні параметри довкілля та об'єктів. Серед найпоширеніших типів сенсорів, релевантних для НС:

- Датчики диму і вогню – виявляють задимлення, підвищення температури, полум'я; встановлюються в будівлях, лісах (протипожежні вежі з IoT), на промислових об'єктах.
- Газові сенсори – реєструють витік небезпечних газів (природного газу, хлору, аміаку тощо) на хімічних підприємствах, в газорозподільних мережах.
- Радіаційні датчики – контролюють рівень радіаційного фону, сигналізують про витік радіоактивних матеріалів або аварії на АЕС.
- Сейсмометри і датчики руху ґрунту – виявляють коливання земної поверхні, зсуви ґрунтів, передвісники землетрусів або обвалів.
- Гідрологічні датчики – вимірюють рівень води у річках, водосховищах, опади; важливі для попередження паводків.
- Датчики тиску та вібрації – можуть сигналізувати про вибухи або структурні руйнування будівель, шахтний обвал тощо.

Об'єднання таких сенсорів у єдину IoT-мережу і підключення її до МАСЦО створює систему раннього виявлення: як тільки якийсь показник перевищує безпечний поріг, сигнал від датчика через мережу передається на сервер ПЗ МАСЦО, де він інтерпретується як тривожна подія. В дослідженнях зазначається, що сучасні системи оповіщення стають проактивними: вони покликані збирати дані з навколишнього середовища за допомогою необхідних інструментів (тобто датчиків), попереджати визначених отримувачів про небезпеку та навіть пропонувати необхідні дії[5]. Деякі системи, як підкреслюють автори, також активують автоматичні реакції на основі цих даних[5]. Таким чином, IoT виступає «нервовою системою» МАСЦО, що відчуває навколишнє середовище.

Головна перевага IoT-тригерів – швидкість реакції. На відміну від людини-оператора, який може не одразу помітити загрозу або зволікати з рішенням, автоматизований датчик подає сигнал миттєво при фіксації критичного параметру. Програмне забезпечення МАСЦО, отримавши такий сигнал, може самостійно привести в дію сценарій оповіщення, заздалегідь налаштований для цього типу тригера. Наприклад:

- Якщо кілька пожежних датчиків в будівлі спрацювали одночасно, система одразу надсилає оповіщення про пожежу: вмикає сирени у будівлі, відправляє повідомлення на телефони відповідальних осіб, повідомляє місцеву пожежну службу.

- Якщо сейсмограф зафіксував підземний поштовх заданої сили, автоматично активується протокол оповіщення про землетрус: звучать сирени у місті, приходять push-сповіщення жителям з інструкцією знайти безпечне місце.

- Якщо радіаційний фон на якомусь пості різко підвищився, система генерує тривогу про радіаційну небезпеку: спеціальні сигнали передаються на об'єкти критичної інфраструктури і населенню поблизу.

- Якщо датчики рівня води показують різкий підйом вгору за короткий час, МАСЦО запускає оповіщення про загрозу паводку в прибережних населених пунктах.

Таким чином, IoT дозволяє реалізувати принцип "машина повідомляє машину": сенсор -> мережа -> програма оповіщення -> виконавчі пристрої (сирени, SMS-шлюзи тощо). Людське втручання мінімізується на найкритичнішому етапі – етапі початкового виявлення і сигналізації. Це особливо важливо у випадку раптових подій (вибух, землетрус), де рахунок іде на секунди.

Окрім датчиків, до IoT-екосистеми можуть входити і пристрої, що виконують активні дії у відповідь на тригер. Наприклад, розумні замки можуть автоматично відчиняти аварійні виходи при отриманні сигналу пожежної тривоги від МАСЦО. Або система вентиляції на хімічному підприємстві автоматично вимикається при надходженні сигналу про витік газу. Такі автоматичні реакції тісно пов'язані з оповіщенням: фактично, вони є внутрішніми актами оповіщення машинами одна одну про потребу діяти. Досвід показує, що деякі сучасні системи оповіщення вже зараз можуть ініціювати подібні автоматизовані дії як частину свого сценарію реагування[5].

У ряді країн впроваджено інфраструктуру раннього виявлення землетрусів: тисячі сейсмотатчиків, з'єднаних у мережу, при перших поштовхах посилають сигнал у систему, яка за секунди розсилає сповіщення на смартфони і сирени (приклад – система ShakeAlert у США). В Японії та Каліфорнії існують мережі датчиків цунамі, що автоматично активують берегові сирени. Розумні лічильники газу в деяких країнах у разі землетрусу автоматично перекривають подачу газу та сигналізують мешканцям. У Нідерландах встановлено IoT-сенсори на греблях і дамбах: при небезпечному рівні води надходить автоматизоване оповіщення службам і населенню про загрозу підтоплення.

Таким чином, IoT як складова МАСЦО забезпечує принципово новий рівень автономності та оперативності системи оповіщення. Мережа сенсорів фактично перетворює все місто (або громаду) на єдиний "організм", що сам відчуває небезпеку і рефлекторно реагує на неї через систему оповіщення. Це суттєво доповнює традиційну схему, де людина мала помітити НС і вручну увімкнути сирени. Звичайно, виклики теж присутні – зокрема, важливо уникнути хибних спрацювань і забезпечити кібербезпеку IoT-пристроїв. Але переваги у вигляді виграного часу та ширшого охоплення загроз є надзвичайно вагомими. IoT-тригери роблять систему оповіщення проактивною, здатною почати діяти ще до того, як небезпеку усвідомили люди.

Мобільні застосунки та відкриті API для систем оповіщення

Сучасне суспільство значною мірою покладається на смартфони та інтернет-сервіси для отримання інформації. Це створює нові канали і інтерфейси для систем централізованого оповіщення. Розробка мобільних застосунків для оповіщення населення і надання відкритих API для інтеграції сторонніх платформ дозволяє значно розширити аудиторію та функціонал МАСЦО.

Спеціалізований мобільний додаток, підключений до системи оповіщення, може доставляти тривожні повідомлення безпосередньо у руку користувача – на екран смартфона чи планшета. На відміну від сирени або теле-/радіоголошення, таке повідомлення може містити детальну інформацію (текст, карту, інструкцію) і бути таргетовано під конкретне місцезнаходження. В Україні успішним прикладом є застосунок «Повітряна тривога», запущений у 2022 році, який сповіщає громадян про початок та відбій повітряних, хімічних, техногенних та інших тривог системи цивільної оборони в режимі push-нотифікацій. Цей додаток був швидко впроваджений і довів свою ефективність, рятуючи життя під час ракетних обстрілів. Надалі функціонал мобільних застосунків може розширюватися: наприклад, надання користувачу можливості відповіді – підтвердити, що він у безпеці, або повідомити про надзвичайну ситуацію, тим самим утворюючи двосторонній канал (як згадувалося раніше, це покращує зворотній зв'язок). Мобільні додатки можуть враховувати геолокацію користувача і показувати лише релевантні тривоги для його району (щоб не перевантажувати зайвими сповіщеннями). Вони також можуть мати режим роботи офлайн (буферизація останнього сповіщення) на випадок втрати інтернет-зв'язку.

Для розширення охоплення, систему оповіщення варто підключати до тих цифрових ресурсів, якими масово користуються громадяни. В українському контексті стратегічно важливою є інтеграція сповіщень із додатком «Дія» – єдиним державним порталом електронних послуг, аудиторія якого сягає десятків мільйонів. Вже зроблені кроки у цьому напрямку: критичні повідомлення (зокрема, сповіщення про ракетну небезпеку) надходять користувачам Дії у вигляді спеціальних попереджень. Крім того, варто інтегрувати МАСЦО з Єдиною системою цивільного захисту (наприклад, якщо існує національна платформа оповіщення або центр, відомий як ЄОСМС – умовно, єдина область/оперативна система мобільного сповіщення). Інтеграція може здійснюватися через відкриті API або webhook-запити: коли МАСЦО генерує подію тривоги, зареєстровані зовнішні платформи отримують через API відповідне повідомлення і можуть його ретранслювати своїми каналами. Таким чином, офіційні застосунки, сайти органів влади, месенджери, соціальні мережі можуть слугувати додатковими ретрансляторами сигналів оповіщення. Принцип “єдиного вікна” для користувача (отримання всіх важливих держповідомлень у одному додатку) підвищує ймовірність того, що попередження не залишиться непоміченим.

Надання відкритого програмного інтерфейсу (API) до системи оповіщення дозволяє стороннім розробникам та сервісам інтегруватися з нею. Це стимулює інновації на місцевому рівні. Наприклад, локальні системи оповіщення підприємств чи університетів можуть через API автоматично отримувати сигнали від МАСЦО (про міські чи регіональні загрози) і дублювати їх на своїх територіях. Навпаки, вони ж можуть надсилати в МАСЦО інформацію про свої локальні НС, щоб ті були враховані на загальному рівні. Громадські розробники можуть створювати спеціалізовані застосунки для людей з інвалідністю, підключені до API МАСЦО (наприклад, програми, що при отриманні сигналу вібрають чи блимають на смарт-годиннику для людей з вадами слуху). Відкритий API також дозволяє легко інтегрувати нові канали оповіщення, що з'являються з розвитком технологій: скажімо, в майбутньому це можуть бути розумні колонки (voice assistants), які через API отримують повідомлення і голосом попередять мешканців оселі про небезпеку.

Варто зазначити, що мобільні та інтернет-канали оповіщення доповнюють, але не замінюють традиційні засоби. Адже у разі кібератаки або перебоїв з електроживленням мобільний зв'язок може постраждати. Тому архітектура сучасної системи оповіщення має бути багатоканальною (multi-channel): сирени, радіо, телебачення, мобільні додатки, SMS, месенджери тощо – все працює в комплексі, підвищуючи ймовірність доведення сигналу. Дослідники наголошують, що мультимодальність і масштабованість є ключовими характеристиками системи оповіщення [4]. Система повинна вміти масштабуватися під навантаження (розсилати мільйони повідомлень, не втрачаючи швидкості) та легко додавати нові канали зв'язку по мірі розвитку технологій [4]. Мобільні рішення якраз добре масштабуються хмарними засобами і можуть динамічно адаптуватися.

Отже, розробка мобільних застосунків та відкритих API для МАСЦО є важливим кроком на шляху людино-центричного і гнучкого оповіщення. Це забезпечує доставку сигналів туди, де люди проводять більшість часу – в онлайн-простір та смартфони. Відкритість платформи для інтеграції стимулює появу нових сервісів і підвищує загальну стійкість системи. В умовах цифрової трансформації громад такі підходи дозволяють максимально наблизити систему оповіщення до кожної окремої особи, враховуючи її потреби та поведінку.

Технології блокчейн у системах оповіщення

Блокчейн асоціюється передусім з криптовалютами, але його властивості – децентралізованість, незмінність даних, прозорість – можуть бути використані для підвищення надійності систем оповіщення. Блокчейн – це розподілений реєстр, у якому інформація зберігається у вигляді ланцюжка блоків, захищених криптографічними методами. В контексті ПЗ МАСЦО блокчейн-технології відкривають такі перспективи: створення незмінного логу подій оповіщення, забезпечення довіри до сигналів (захист від фальшивих або несанкціонованих тривог), впровадження смарт-контрактів для автоматизації протоколів реагування, а також покращення координації між різними організаціями.

Кожен факт активації оповіщення, передавання повідомлення чи інша подія може записуватися у блокчейн-реєстр. Завдяки криптографічному зв'язуванню блоків забезпечується, що запис неможливо заднім числом змінити або видалити – будь-яка спроба правки буде відразу помітна. Це надзвичайно корисно для аудиту та розслідувань після НС: всі дії системи оповіщення документовані і їхня достовірність гарантована технологією. Наприклад, після надзвичайної

ситуації можна перевірити точний час увімкнення сирени в кожному районі чи момент відправки SMS-повідомлення – якщо ці дані у блокчейні, то вони однозначно правдиві. Такий журнал може бути відкритим (публічний блокчейн) або доступним для уповноважених органів (приватний або консорціумний блокчейн). Експерти з блокчейну зазначають, що immutable audit trail – одна з ключових переваг: кожна транзакція (дія) записана з міткою часу, формуючи незмінний ланцюжок подій, що дуже важливо для юридичної та управлінської відповідальності[6].

Класичні системи оповіщення залежать від центрального сервера або центру керування. Якщо він виходить з ладу (через збій або атаку), вся система може припинити роботу. Блокчейн же за своєю природою децентралізований: інформація зберігається і обробляється на множині вузлів мережі. У випадку децентралізованої системи оповіщення на блокчейні, сигнал тривоги може ініціюватися та поширюватися відразу через багаточисельні вузли, що підвищує виживаність системи в кризових ситуаціях. Дослідники пропонують концепцію EmergencyBlock – блокчейн-базованої системи публічного оповіщення, що має децентралізовану архітектуру і завдяки цьому зберігає працездатність при високих навантаженнях або пошкодженні частини інфраструктури. Розподілені вузли, розміщені в різних організаціях (ДСНС, оператори зв'язку, місцева влада тощо), спільно підтверджують і поширюють повідомлення тривоги. Це також унеможливило одноосібне блокування чи цензурування сповіщень – влада нижчого рівня чи зловмисник не можуть приховати або сфальсифікувати сигнал, адже його автентичність захищена консенсусом мережі.

Уявімо ризик: зловмисник намагається передати неправдивий сигнал тривоги, зламавши систему, або внутрішній диспетчер зловживає повноваженнями. Блокчейн може запобігти цьому через механізм криптографічної перевірки кожної транзакції (події оповіщення). Кожен вузол або особа, уповноважена генерувати сигнал в МАСЦО, матиме свій криптографічний ключ. Тільки транзакції, підписані належним ключем, будуть вважатися дійсними і включатися до блокчейну. Всі інші – відкидатимуться. Це означає, що сторонній несанкціонований сигнал просто не потрапить до системи. Крім того, сам блокчейн-реєстр дозволяє перевірити цілісність повідомлення: якщо хтось спробує його змінити по дорозі (наприклад, замінити текст або район оповіщення), хеш-перевірка блоку покаже невідповідність. Науковці пропонують використовувати асиметричне шифрування в парі з блокчейном для гарантії, що фальшиві тривоги неможливі, а всі справжні сповіщення захищені від підробки. Таким чином, громадяни і посадовці можуть більше довіряти системі: якщо прийшло повідомлення, то воно точно від справжнього джерела і не було змінено.

Смарт-контракт – це програма, що виконується в блокчейн-мережі автоматично при виконанні заданих умов. В контексті МАСЦО смарт-контракти можуть застосовуватися для формалізації та автоматизації протоколів реагування. Наприклад, можна створити смарт-контракт «Якщо від сенсорної мережі X надходить підтверджений сигнал про землетрус магнітудою > 6 , то: 1) додати запис про надзвичайну ситуацію до блокчейну; 2) оповістити такі-то вузли (місто, область) про необхідність увімкнення сирен; 3) після підтвердження від ≥ 2 вузлів – згенерувати транзакцію про початок оповіщення і виконати розсилку сповіщень через API». Цей умовний сценарій виконається автоматично і прозоро – всі учасники бачать на блокчейні, що умови виконано і контракт спрацював. Смарт-контракти можуть керувати розподілом ресурсів: наприклад, автоматично розблокувати доступ до резервних каналів зв'язку при великій надзвичайній ситуації, або навіть ініціювати страхові виплати/допомогу населенню після фіксації блоку про НС (це ширший міжвідомчий аспект). Хоча використання смарт-контрактів у цій галузі поки експериментальне, потенціал великий – вони усувають затримки і людський фактор у виконанні узгоджених протоколів, гарантуючи, що «кодекс дій» буде дотримано до літери.

Під час ліквідації наслідків НС взаємодіє багато суб'єктів: служби ДСНС, поліція, медики, енергокомпанії, органи місцевої влади тощо. Кожен з них має свої дані і системи. Блокчейн може слугувати єдиним достовірним інформаційним полем для різних учасників, де вони обмінюються даними про інцидент. Наприклад, у разі великої техногенної аварії одна сторона (підприємство) записує у блокчейн параметри аварії, друга (ДСНС) – свої дії та потреби, третя (лікарні) – інформацію про постраждалих. Усі бачать актуальну інформацію і впевнені в її достовірності, бо вона верифікована в розподіленій мережі. У Китаї досліджується застосування блокчейну для спільного використання даних під час надзвичайних ситуацій у сфері охорони здоров'я (наприклад, при епідеміях) – побудовано консорціумний блокчейн, де різні відомства діляться даними про розвиток ситуації, що підвищує ефективність координації. Аналогічно, для МАСЦО блокчейн може об'єднати різні рівні систем оповіщення (державну, регіональну, місцеву) у єдиний захищений

контур обміну сигналами: кожен рівень є вузлом мережі і публікує свої оповіщення, які підтверджуються іншими.

Отже, застосування блокчейн-технологій у ПЗ МАСЦО спрямоване на підвищення довіри, надійності та автоматизації. Децентралізована архітектура забезпечує стійкість системи до відмов і атак, а незмінність даних гарантує прозорість та підзвітність. Хоча впровадження блокчейну потребує додаткових ресурсів і координації (а також вирішення питань конфіденційності даних), потенційний вииграш – дуже значний. Уявлення про систему оповіщення як довірену платформу, де кожен сигнал завірений і зберігається назавжди, доповнює концепцію цифрової трансформації сфери безпеки. Блокчейн може стати тим “каркасом довіри”, на якому будуть реалізовані міжвідомчі та міжрегіональні взаємодії в надзвичайних ситуаціях.

Напрями дослідження та перспективи розвитку. Сучасні виклики безпеки вимагають трансформації місцевих систем централізованого оповіщення з традиційних сиренних комплексів у адаптивні цифрові платформи, здатні навчатися, взаємодіяти та еволюціонувати. Проведений аналіз окреслив п'ять ключових векторів інноваційного розвитку програмного забезпечення МАСЦО:

1. Інтелектуалізація оповіщення (ШІ та ML). Оснащення ПЗ МАСЦО алгоритмами штучного інтелекту дає можливість системі автоматично розпізнавати типи надзвичайних ситуацій, прогнозувати їхні наслідки і оптимально керувати потоками сповіщень. Інтелектуальна система оповіщення переходить від реактивної моделі “сповістити про те, що сталося” до проактивної моделі “передбачити та попередити, поки не пізно”. Це значно підвищує ефективність оповіщення і зменшує втрати під час НС завдяки виграному часу та точнішій інформації.

2. Інтеграція з екосистемою Smart City. ПЗ МАСЦО повинно стати невід'ємною частиною цифрової інфраструктури громади. Інтеграція зі смарт-платформами міста дозволяє автоматизовано задіяти інформаційні табло, транспорт, системи зв'язку та інші ресурси для донесення оповіщення і забезпечення заходів реагування (евакуація, пріоритетні маршрути тощо). Одночасно, через міські датчики та пристрої, система може отримувати зворотний зв'язок про стан виконання оповіщення. Така тісна взаємодія забезпечує синергетичний ефект – ціле (розумне місто) реагує на загрозу як єдиний організм, мінімізуючи хаос і затримки.

3. IoT-орієнтованість (автоматичні тригери). Вбудовування в МАСЦО численних IoT-датчиків створює мережу раннього виявлення, яка миттєво запускає оповіщення при прояві ознак небезпеки. Система отримує “сенсори” для різних видів загроз – від природних (землетрус, повінь) до техногенних (пожежа, хімічний витік) – і може реагувати в автономному режимі. Це особливо важливо для раптових, стрімких НС, де людський ресурс може не встигнути зреагувати. IoT робить оповіщення більш точним (адже сигнали генеруються на основі вимірних параметрів) та оперативним. Водночас, важливою є кібербезпека IoT-середовища, щоб виключити саботаж або масові хибні спрацьовування.

4. Мобільність та відкритість платформи. Розробка дружніх користувацьких мобільних застосунків підвищує довіру населення до системи оповіщення і залученість у процес підготовки до НС. Мобільні канали дозволяють персоналізувати попередження і донести їх навіть до тих, хто може не почути сирен. Відкриті API та інтеграція з популярними сервісами (як-от “Дія”) роблять МАСЦО гнучкою екосистемою, яку можна адаптувати під різні потреби громад та організацій. Залучення сторонніх розробників через API стимулює інновації і створення додаткових корисних сервісів навколо оповіщення – від віджетів погоди з функцією тривоги до систем оповіщення усередині розумних будинків. Таким чином, МАСЦО еволюціонує у платформу цивільної безпеки, на основі якої розбудовується цілий ряд цифрових рішень для громад.

5. Блокчейн та довіра. Впровадження блокчейн-рішень сприяє вирішенню проблеми довіри і прозорості. У критичних системах, до яких належить оповіщення, надзвичайно важливо мати гарантії, що інформація достовірна і процеси відбулися так, як заявлено. Блокчейн забезпечує незмінність записів про оповіщення, унеможливорює приховування чи фальсифікацію подій, надає механізми колективної верифікації сигналів. В довгостроковій перспективі це може стати основою для міжрегіональної та міжнародної взаємодії систем оповіщення, коли різні юрисдикції довіряють сигналам одна одній на основі спільного розподіленого реєстру. Смарт-контракти ж можуть зробити реагування більш автоматичним і об'єктивним, зменшуючи адміністративні затримки.

Висновки. Розвиток ПЗ МАСЦО на стику цих п'яти напрямів охоплює кілька галузей: штучний інтелект, інформаційні технології міського управління, телекомунікації, сенсорні мережі, кібербезпеку, розробку програмного забезпечення, криптографію тощо. Це яскраво ілюструє, що

сучасні системи оповіщення виходять за рамки суто інженерних задач зв'язку – вони перетворюються на кібер-фізичні системи, які поєднують технічні засоби і алгоритми ухвалення рішень. Для успішної реалізації таких проектів потрібна співпраця фахівців різних напрямів: айтишників, рятувальників, міських планувальників, законодавців. Саме міждисциплінарний підхід забезпечить створення збалансованої системи, де технології відповідають реальним потребам цивільного захисту і можуть бути ефективно використані службами НС.

Враховуючи стратегічне значення МАСЦО для безпеки громад, доцільно на державному рівні стимулювати впровадження розглянутих інновацій. По-перше, необхідно оновити нормативно-правову базу: стандартизувати формати даних для оповіщення (наприклад, адаптувати міжнародний стандарт CAP під українські реалії), визначити вимоги до кіберзахисту систем оповіщення, узаконити використання мобільних сповіщень нарівні з сиреною, врегулювати питання відповідальності при автоматизованих рішеннях (смарт-контракти). По-друге, слід реалізувати пілотні проекти в окремих громадах з впровадженням, наприклад, IoT-мережі пожежних датчиків або AI-модуля аналізу відеопотоків для оповіщення – і за їх результатами масштабувати успішні рішення. По-третє, необхідна державна підтримка фінансування і стимулювання бізнесу: закупівля необхідного обладнання (сенсори, сервери), гранти на розробку ПЗ (застосунків, блокчейн-систем), залучення вітчизняних IT-компаній до розробки компонентів МАСЦО.

У рамках цифрової трансформації суспільства, про яку заявлено на найвищому рівні, система оповіщення має трансформуватися однією з перших – адже вона безпосередньо пов'язана з захистом життя людей. Інноваційне ПЗ МАСЦО – це інвестиція у безпеку і стійкість громад до будь-яких викликів. Наведені напрями розвитку демонструють, що вже існують технологічні рішення для створення розумної, надійної та гнучкої системи оповіщення. Важливо об'єднати зусилля науковців, розробників і держави, щоб в найближчі роки ці рішення перейшли з площини концепцій та пілотів у реальну практику цивільного захисту по всій країні.

Список бібліографічного опису

1. Поділ системи оповіщення за рівнями // Техноспектр-Сервіс: [сайт]. – Режим доступу: <https://ts.kiev.ua/podil-systemy-opovishchennia-za-rivniamy/> (дата звернення: 02.05.2025).
2. Leveraging AI in emergency management and crisis response // Deloitte Insights: [веб-сайт]. – Режим доступу: <https://www2.deloitte.com/us/en/insights/industry/public-sector/automation-and-generative-ai-in-government/leveraging-ai-in-emergency-management-and-crisis-response.html> (дата звернення: 02.05.2025).
3. Villegas-Ch, W.; Govea, J. Application of Deep Learning in the Early Detection of Emergency Situations and Security Monitoring in Public Spaces // *Applied System Innovation*. – 2023. – Vol. 6, No. 5. – P. 90. – Режим доступу: <https://www.mdpi.com/2571-5577/6/5/90> (дата звернення: 02.05.2025).
4. What Essential Features Must an Emergency Notification System Maintain? // GovCIO Outlook: [веб-сайт]. – 14 жовтня 2024. – Режим доступу: <https://www.govciooutlook.com/news/what-essential-features-must-an-emergency-notification-system-maintain-nid-2296.html> (дата звернення: 02.05.2025).
5. Olorunfemi T. O. та ін. SEN-IoT: A Smart Emergency Notification System Suitable for Developing Countries using Internet of Things // *International Journal of Computer (IJC)*. – 2020. – Vol. 39, No. 1. – P. 1–9. – Режим доступу: <https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1682> (дата звернення: 02.05.2025).
6. Emergency Care Blockchain Solution – Startup Spotlight // FasterCapital Blog: [веб-сайт]. – Режим доступу: <https://fastercapital.com/content/Emergency-Care-Blockchain-Solution--Startup-Spotlight--Blockchain-Solutions-for-Rapid-Emergency-Response.html> (дата звернення: 02.05.2025).

References:

1. Division of the alert system by levels // Technospectr-Service. <https://ts.kiev.ua/podil-systemy-opovishchennia-za-rivniamy/> (access date: 02.05.2025).
2. Leveraging AI in emergency management and crisis response // Deloitte Insights. <https://www2.deloitte.com/us/en/insights/industry/public-sector/automation-and-generative-ai-in-government/leveraging-ai-in-emergency-management-and-crisis-response.html> (access date: 02.05.2025).
3. Villegas-Ch, W.; Govea, J. Application of Deep Learning in the Early Detection of Emergency Situations and Security Monitoring in Public Spaces // *Applied System Innovation*. – 2023. – Vol. 6, No. 5. – P. 90. <https://www.mdpi.com/2571-5577/6/5/90> (access date: 02.05.2025).
4. What Essential Features Must an Emergency Notification System Maintain? // GovCIO Outlook. <https://www.govciooutlook.com/news/what-essential-features-must-an-emergency-notification-system-maintain-nid-2296.html> (access date: 02.05.2025).
5. Olorunfemi T. O. та ін. SEN-IoT: A Smart Emergency Notification System Suitable for Developing Countries using Internet of Things // *International Journal of Computer (IJC)*. – 2020. Vol. 39, No. 1. – P. 1–9. <https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1682> (access date: 02.05.2025).
6. Emergency Care Blockchain Solution – Startup Spotlight // FasterCapital Blog. <https://fastercapital.com/content/Emergency-Care-Blockchain-Solution--Startup-Spotlight--Blockchain-Solutions-for-Rapid-Emergency-Response.html> (access date: 02.05.2025).