УДК 711.4:355.58:316.77

В. В. Любич

ІНФОРМАЦІЙНА СТІЙКІСТЬ МІСЬКОЇ МЕРЕЖІ УКРИТТІВ В УМОВАХ ВОРОЖИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Анотація. *Запропоновано підхід до врахування інформаційних загроз у плануванні міської мережі укриттів. Дезінформацію розглянуто як чинник затримки реагування та порушення маршрутного вибору. Поєднано перевірені відомості про укриття, сценарне оцінювання часу їх досягнення й розподіл населення з урахуванням місткості. Визначено напрями підвищення інформаційної стійкості системи цивільного захисту міста.*

Ключові слова: *цивільний захист; мережа укриттів; містобудівне планування; інформаційна стійкість; дезінформація.*

Abstract. *An approach is proposed to incorporate information threats into urban shelter network planning. Disinformation is considered a factor that delays protective action and disrupts route choice. The approach combines verified shelter information, scenario assessment of access times, and population allocation subject to shelter capacity. Measures to strengthen the information resilience of urban civil protection are outlined.*

Keywords: *civil protection; shelter network; urban planning; information resilience; disinformation.*

Вступ

Інтеграція цивільного захисту в планувальну структуру міста передбачає узгодження розміщення укриттів, маршрутів доступу, інженерної інфраструктури та управлінських рішень. Необхідність такого підходу обґрунтовано в дослідженні В. В. Швеця та В. В. Любича [1].

Інформаційно-психологічний вплив може порушувати реалізацію просторово обґрунтованого рішення: повідомлення про нібито недоступне укриття або недостовірне скасування загрози здатне затримати початок руху. Для міського планування це означає потребу оцінювати не лише розташування захисних споруд, а й умови своєчасного використання їх населенням. Неправдиве повідомлення саме по собі не доводить наявності організованої ворожої операції; встановлення його походження потребує окремої перевірки.

Положення, затверджене постановою Кабінету Міністрів України № 733, визначає організацію оповіщення та подальшого інформування населення. Пункти 18 і 20 передбачають доведення повідомлень доступними засобами та наведення в них відомостей про характер і місце загрози, можливу зону надзвичайної ситуації й заходи безпеки [2].

У рекомендаціях UNDRR наголошено, що шкідлива інформація може послаблювати захисні дії, порушувати реагування та підривати довіру. Її врахування потребує підготовки до кризи, узгодженої комунікації та оцінювання інформаційних загроз [3].

Мета роботи — запропонувати методичне доповнення до просторової моделі міської мережі укриттів, яке враховує інформаційні порушення та дає змогу порівнювати заходи збереження своєчасного доступу населення до захисту.

Методичний підхід

Інформаційна стійкість визначається як здатність системи цивільного захисту підтримувати достовірне, зрозуміле та своєчасне інформування, необхідне для використання доступної захисної місткості.

Пропонується розмежовувати фізичний стан споруди, достовірність відомостей про неї та поведінкову реакцію населення. Хибна інформація про закриття не змінює фактичної місткості укриття, але може змінювати попит на нього й збільшувати навантаження на сусідні об’єкти. Втрата зв’язку також не означає автоматичної втрати захисних властивостей споруди. Таке розмежування запобігає подвійному врахуванню однієї події як фізичної та інформаційної відмови.

Для сценарію s час досягнення укриття j населенням зони i описується співвідношенням

$$T^s_{ij} = \tau^s_i + t^s_{ij} + q^s_j \le \theta^s \quad (1)$$

де τ — час від початку відліку сценарію до початку руху, включно з отриманням повідомлення та прийняттям рішення; t — час руху фактично обраним маршрутом; q — час очікування й входу; θ — часовий поріг конкретного сценарію. Усі складові задаються в однакових одиницях. Поріг є параметром дослідження, а його значення потребує окремого обґрунтування для відповідної загрози. Для маломобільних груп параметри руху та входу визначаються окремо.

Інформаційне порушення відображається зміною затримки початку руху та вибору маршруту. Фізичне пошкодження мережі враховується вилученням непрохідних зв'язків. Час очікування залежить від потоку людей і пропускної здатності входів, тому в детальній імітації він перераховується після зміни розподілу попиту. Сценарії доцільно порівнювати за незмінного складу населення та однакової точки початку відліку часу.

Для оцінювання потенційної забезпеченості застосовується розподіл людей між доступними укриттями, що максимізує кількість своєчасно забезпечених місцями. Невід'ємна цілочислова змінна x позначає кількість людей із зони i, призначених до укриття j у сценарії s. Сума призначень із кожної зони не перевищує її населення, а сума призначень до кожного укриття — його фактичної доступної місткості. Для недоступної споруди або пари «зона — укриття», що порушує умову (1), призначення дорівнює нулю. Одна людина враховується лише один раз. У поведінкових сценаріях допустимі призначення додатково обмежуються напрямками руху, заданими моделлю вибору укриття; це обмеження не змінює фізичного статусу споруди.

Частку населення, потенційно забезпеченого захистом, і найгірше значення серед досліджуваних сценаріїв визначають так:

$$K_s = \frac{\sum_i \sum_j x_{ij}^s}{\sum_i P_i}, \quad R = \min_s K_s \quad (2)$$

де P — чисельність населення зони; K — частка забезпечених у відповідному сценарії; R — показник стійкості на заданому наборі сценаріїв. Розрахунок характеризує можливість узгодженого розподілу, тоді як фактичне досягнення укриттів потребує поведінкової імітації. Якщо досліджуваний набір сценаріїв не охоплює певної загрози, значення R не характеризує стійкості до неї.

Напрями практичного застосування

Першим напрямом є узгодження муніципального реєстру укриттів із засобами інформування. Для кожного об'єкта потрібні перевірені відомості про вхід, режим доступу, місткість і відповідального за оновлення. Час останньої перевірки та історія змін дають змогу відокремити актуальний статус від застарілого повідомлення. Зміни маршрутних рекомендацій мають спиратися на підтвердження стану об'єкта та мережі, а не на неперевірене повідомлення в соціальних мережах.

Другим напрямом є резервування інформування на рівні кварталів: зрозумілі покажчики, попереднє ознайомлення з найближчими укриттями, друковані схеми й погоджені резервні канали повідомлень. Їх розміщення пов'язується з реальною вулично-дорожньою мережею, бар'єрами доступності та місцями перебування вразливих груп. Перевірка чуток і коригування реєстру виконуються відповідальними службами паралельно із захисними заходами; для населення вони не мають створювати додаткової затримки реагування.

Третім напрямом є регулярне навчання та зворотний зв'язок: пояснення способів розпізнавання офіційних джерел, повідомлення про помилки в реєстрі та перевірка зрозумілості інструкцій. Прозорість оновлень і можливість отримати підтверджені відомості узгоджуються з принципами суспільної довіри, стійкості та розширення спроможності громадян, викладеними ООН [4].

Для подальшої апробації на м. Вінниця доцільно порівняти базовий режим, затримку реагування, зміну маршрутного вибору через недостовірні відомості та поєднання інформаційних порушень із втратою окремих зв'язків мережі. Параметри затримки слід визначати за результатами навчань або знеособлених опитувань. Для розвитку дослідження пропонується сценарний модуль, який зіставлятиме дефіцит місць, час досягнення укриттів і перевантаження входів.

Порядок апробації передбачає перевірку входів і маршрутів, формування базового розподілу населення, введення сценарних змін та повторний розрахунок після реалізації

комунікаційних заходів. Фізична місткість у парних інформаційних сценаріях зберігається однаковою, щоб відокремити ефект інформування від ефекту будівництва нових об'єктів. Для оцінювання невизначеності затримку реагування слід змінювати в обґрунтованому діапазоні, а висновки перевіряти для різних періодів перебування населення в місті.

Результативність заходів доцільно оцінювати за зміною частки своєчасно забезпеченого населення, кількості перевантажених укриттів і нерівності доступу між зонами. Додатковими організаційними показниками можуть бути частка актуалізованих записів реєстру та час виправлення підтвердженої помилки. Вони характеризують якість інформаційної підтримки, проте самі по собі не доводять зростання захищеності. Планувальну перевагу має рішення, яке поліпшує доступ до захисту в досліджуваних сценаріях і зберігає здійсненність маршрутів для різних груп населення.

Висновки

Зв'язок напряму протидії ворожим інформаційно-психологічним операціям із містобудівним дослідженням полягає у збереженні своєчасного використання мережі укриттів за інформаційних порушень. Запропонований підхід доповнює просторову доступність параметрами реагування, маршрутного вибору та входу. Це створює основу для спільного обґрунтування планувальних рішень, резервування інформування й організації навчань. Науковий результат роботи має методичний характер і потребує перевірки на міських даних.

Список використаних джерел:

1. Швець В. В., Любич В. В. Системи цивільного захисту як складова міського планування: проблемні аспекти, стан впровадження та перспективи формування стійких міст у воєнний і післявоєнний періоди. Сучасні технології, матеріали і конструкції в будівництві. 2026. Т. 40, №

1. С. 168–178. DOI: https://doi.org/10.31649/2311-1429-2026-1-168-178 (дата звернення: 04.11.2026).

2. Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту : постанова Кабінету Міністрів України від 27.09.2017 № 733. URL: https://zakon.rada.gov.ua/laws/show/733-2017-%D0%BF#Text (дата звернення: 04.11.2026).

3. UNDRR. Harmful information in disasters: Risk communication for safer decisions. Guidance note. 2026. 27 p. URL: https://www.undrr.org/publication/documents-and-publications/harmful-information-disasters-risk-communication-safer (дата звернення: 04.11.2026).

4. United Nations. United Nations Global Principles for Information Integrity. New York, 2024. URL: https://www.un.org/sites/un2.un.org/files/un-global-principles-for-information-integrity-en.pdf (дата звернення: 04.11.2026).

Любич Володимир Володимирович – *аспірант, асистент кафедри промислового та цивільного будівництва, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: mr.lyubich1988@gmail.com.*

Volodymyr Volodymyrovych Lyubich – *Postgraduate Student, Assistant, Department of Industrial and Civil Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: mr.lyubich1988@gmail.com.*