Оптимізаційне проєктування об'ємно-планувальних і конструктивних рішень об'єктів критичної інфраструктури з урахуванням їх вразливостей

Дмитро Кузьминський, магістр[1] (ORCID: 0009-0005-7125-685X), **Данило Павлик**, магістр [1] (ORCID: 0009-0002-3858-6599), **Володимир Скочко**, проф., д-р техн. наук, професор[1] (ORCID: 0000-0002-1709-2621)

[1] *Київський національний університет будівництва та архітектури, Україна*

АНОТАЦІЯ

Критична інфраструктура сучасних міст і регіонів охоплює широкий спектр об'єктів – від енергетичних систем і транспортних вузлів до об'єктів водопостачання, зв'язку та інформаційних технологій. Її стійкість та захищеність є визначальними факторами національної безпеки, а питання оптимізації проєктування конструктивних і об'ємно-планувальних рішень виходить на перший план у контексті військових загроз, природних катастроф і техногенних аварій.

Ключові слова: критична інфраструктура, оптимізаційне проєктування, об'ємно-планувальні рішення, конструктивні рішення, вразливості, захист, стійкість, BIM-технології, інженерна безпека.

1. ВСТУП

Умови функціонування суспільства характеризуються зростанням ризиків, пов'язаних із військовими загрозами, природними катастрофами та техногенними аваріями. У цих умовах питання стійкості та безпечної експлуатації об'єктів критичної інфраструктури (КІ) набувають особливої актуальності.

Об'єкти КІ є основою життєзабезпечення населення, економіки та державного управління, а їх вихід із ладу може спричинити масштабні соціально-економічні наслідки [1]. Тому під час проектування важливо враховувати не лише функціональні потреби та економічні аспекти, а й потенційні вразливості та загрози.

Оптимізаційне проєктування об'ємно-планувальних і конструктивних рішень розглядається як один із найефективніших шляхів забезпечення стійкості та захищеності КІ. Використання сучасних інженерних методів, цифрових технологій (BIM-моделювання, цифрові двійники), а також інтеграція систем безпеки вже на стадії архітектурно-планувального проєктування дозволяє зменшити ризики, підвищити надійність і забезпечити безперервність функціонування об'єктів у кризових ситуаціях.

2. ВРАЗЛИВОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Об'єкти критичної інфраструктури [1, 2] є складними системами, які одночасно зазнають впливу техногенних, природних і антропогенних загроз. Їхня уразливість визначається не лише конструктивними характеристиками, а й взаємозалежністю з іншими системами. Виділяють такі ключові групи вразливостей:

- функціональні вразливості, залежність від зовнішніх джерел енергопостачання та зв'язку; відсутність або недостатня кількість резервних систем (генератори, канали комунікацій); уразливість до кібератак на інформаційні системи управління;
- конструктивні вразливості, недостатня стійкість до динамічних навантажень (сейсміка, вибухова хвиля, вібрація); використання застарілих матеріалів із низьким рівнем вогнестійкості чи ударостійкості; обмежена здатність до локалізації пошкоджень (ефект «ланцюгової реакції» при руйнуванні окремих елементів);
- об'ємно-планувальні вразливості, нераціональне зонування: концентрація життєво важливих функцій у єдиному приміщенні; вузькі коридори, обмежена кількість евакуаційних виходів; недостатня ізоляція критичних приміщень (серверних, вузлів управління) від загальнодоступних зон;
- експлуатаційні вразливості, зношеність обладнання та інженерних мереж; відсутність сучасних систем моніторингу та раннього виявлення пошкоджень; недостатній рівень підготовки персоналу до дій у кризових ситуаціях;
- соціальні та організаційні вразливості; людський фактор: помилки обслуговуючого персоналу, відсутність планів евакуації та інструкцій; недостатня координація між різними установами, що відповідають за безпеку об'єктів; відсутність системи навчань і тренувань для населення, яке перебуває поблизу КІ.

2.1. Принципи оптимізації проєктування

Оптимізаційний підхід [3] до проєктування об'єктів критичної інфраструктури передбачає не лише технічну чи економічну ефективність, але й урахування комплексної стійкості до потенційних загроз. Це багатокритеріальний процес, у якому необхідно досягти балансу між вартістю, надійністю, функціональністю та безпекою.

Основними принципами такого підходу виступають:

1. Інтеграція захисту на етапі проєктування.

Захисні заходи повинні бути закладені ще на стадії архітектурно-планувальних рішень, а не додаватися як додаткові системи після завершення будівництва. Це передбачає: врахування впливу ударної хвилі, вібрацій, пожеж, сейсмічних навантажень; мінімізацію наслідків кібератак через захищені інформаційні мережі; формування архітектурних рішень, які знижують імовірність прогресуючих руйнувань.

2. Модульність та резервування.

Модульний підхід дозволяє створювати автономні функціональні блоки, здатні продовжувати роботу навіть у разі виходу з ладу окремих елементів. Прикладом є: резервні серверні кімнати та енергоцентри; дублюючі комунікаційні канали; розподілені інженерні системи (опалення, вентиляція, пожежогасіння). Така структура суттєво підвищує живучість об'єкта та його здатність до відновлення.

3. Раціональне зонування.

Планувальні рішення повинні базуватися на функціональному поділі території та приміщень. Найбільш критичні елементи (серверні, вузли управління, системи енергозабезпечення) розташовуються в ізольованих, захищених частинах будівлі, відокремлених від зон загального доступу. Це знижує ризик навмисного чи випадкового впливу на стратегічно важливі системи.

У міжнародній практиці застосовуються концепції «ядер безпеки» (security cores), які розміщуються в центральних або підземних частинах будівель.

Приклад наведено на рис. 1, де показано поділ на громадську, функціональну та захищену зони.

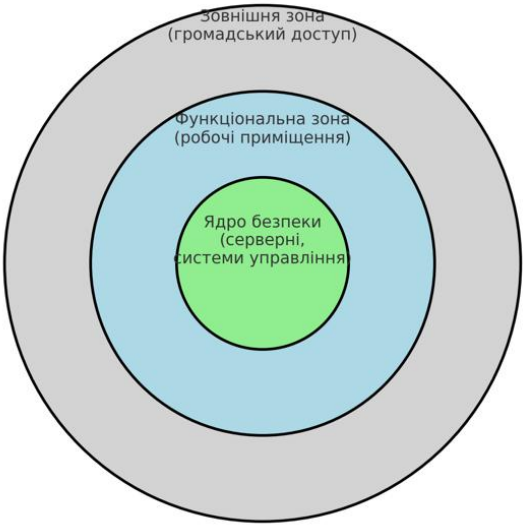

Рисунок 1. Зонування об’єкта критичної інфраструктури

4. Оптимізація евакуаційних рішень.

Ефективна евакуація персоналу та користувачів об’єкта є ключовим чинником зниження втрат у кризових ситуаціях. Оптимізація передбачає: мінімізацію відстаней та часу до виходу; наявність дублюючих маршрутів та аварійних виходів; впровадження автоматизованих систем навігації (динамічні покажчики, системи підказок через мобільні додатки); застосування мультиагентного моделювання для розрахунку потоків людей у різних сценаріях надзвичайних ситуацій..

2.2. Методи оптимізації

Математичне моделювання: аналіз поведінки конструкцій при різних сценаріях навантажень (вибух, пожежа, сейсміка).

Використання BIM-технологій: цифрові двійники для перевірки рішень ще до етапу реалізації.

Мультиагентне моделювання евакуаційних процесів: дозволяє оптимізувати планування з урахуванням людського фактору.

Системний аналіз життєвого циклу: оцінка стійкості на всіх етапах – від проєктування до експлуатації й реконструкції..

2.3. Практичні приклади

У сучасній світовій практиці активно використовуються: комбіновані конструктивні системи (сталезалізобетонні каркаси з високою вогнестійкістю та здатністю поглинати ударні навантаження); захисні фасадні системи з елементами енергозбереження; інтеграція інженерних систем безпеки (системи контролю доступу, відеоаналітики, пожежогасіння) у архітектурно-планувальне рішення (рис. 2).

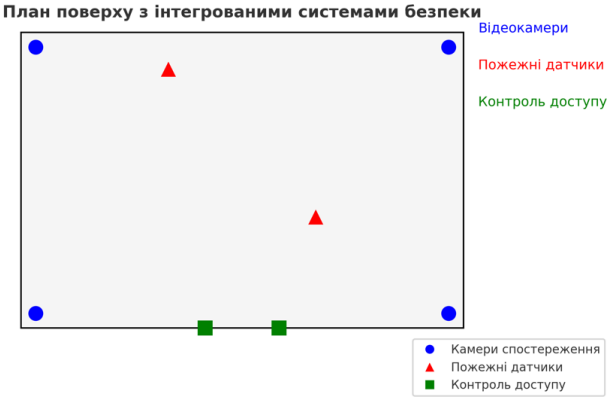

Рисунок 2. Інтеграція інженерних систем безпеки

3. ВИСНОВКИ

Поєднання комбінованих конструктивних систем, захисних фасадів та інтегрованих інженерних систем дозволяє створювати стійкі об’єкти, які відповідають сучасним викликам. Вони забезпечують не лише фізичний захист, а й підвищують енергоефективність, знижують експлуатаційні витрати та сприяють безперервності функціонування критичної інфраструктури.

4. ПЕРСПЕКТИВИ РОЗВИТКУ

Подальші дослідження будуть спрямовані на: використання штучного інтелекту для багатокритеріальної оптимізації рішень; розробку адаптивних конструкцій з можливістю змінювати конфігурацію під впливом зовнішніх навантажень; впровадження стандартів «стійкого будівництва» для об’єктів КІ у національну нормативну базу.

Список літератури

[1] Класифікація об'єктів критичної інформаційної інфраструктури держави : thesis / О. Г. Корченко та ін. 2018. URL: http://er.nau.edu.ua/handle/NAU/33201 (дата звернення: 03.10.2025).

[2] Закон України. Про критичну інфраструктуру. (Відомості Верховної Ради (ВВР), 2023, № 5, ст.13) URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

[3] Уряднікова І. В., Заплатинський В. М. Наукові підходи до визначення терміну «критична інфраструктура». *Вісті Донецького гірничого інституту*. 2020. № 2 (47). URL: https://doi. org/10.31474/1999-981X-2020-2-184-193.

[4] Суходоля О. М. Стійкість критичної енергетичної інфраструктури та життєдіяльності громад. Національний інститут стратегічних досліджень, 2024. URL: https://doi.org/10.53679/niss-analytrep.2024.04 (дата звернення: 03.10.2025).