Методика оцінювання загроз об’єктам критичної інфраструктури під час вогневого впливу противника

Methodology for assessing threats to critical infrastructure objects during enemy fire

Ілля Капля [A]
Corresponding author: ад’юнкт кафедри, e-mail: kaplia1607@gmail.com, ORCID: 0000-0002-1424-4175
Богдан Тертишний [A]
доктор філософії, старший викладач кафедри, e-mail: hlor2007@gmail.com, ORCID:0000-0002-9060-761X

IlliaKaplia [A]
Corresponding author: Graduate Student of the Department, e-mail: kaplia1607@gmail.com, ORCID: 0000-0002-1424-4175
Bohdan Tertyshnyy [A]
Doctor of Philosophy, Senior Lecturer of the Department, e-mail: hlor2007@gmail.com, ORCID:0000-0002-9060-761X

[A] Національний університет оборони України, м. Київ, Україна
[A]National Defense University of Ukraine, Kyiv, Ukraine

Received: October 4, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.21

Мета роботи: мінімізація наслідків загроз об’єктам критичної інфраструктури від вогневого впливу противника.
Метод: експертних оцінок, статистичного аналізу, теорії ймовірності.
Результати дослідження: розробка методики оцінювання загроз об’єктам критичної інфраструктури під час вогневого впливу противника з урахуванням їх сумарного ефекту, яка враховує об’єднаний вплив різних загроз при їх одночасній дії.
Теоретична цінність дослідження: попередження надзвичайних ситуацій від вогневого впливу противника шляхом подальшої пріоритезації загроз та розробки заходів захисту.
Тип статті: огляд і дослідження.

Purpose: minimization of the consequences of threats to critical infrastructure objects from a concentrated enemy fire strike.
Method: expert assessments, statistical analysis, probability theory.
Findings: development of a methodology for assessing threats to critical infrastructure objects during enemy fire, taking into account their total effect, which takes into account the combined impact of various threats when they act simultaneously.
Theoretical implications: prevention of emergency situations from enemy attacks by further prioritization of threats and development of protection measures.
Papertype: review and research.

Ключові слова: критична інфраструктура, надзвичайна ситуація, оцінювання загроз, вогневий вплив, захист.

Key words: critical infrastructure, emergency, threat assessment, fire impact, protection.

Вступ

Загрози для об’єктів критичної інфраструктури в сучасному світі, стають більш складними та різноманітними. Це обумовлено як розвитком технологій, так і збільшенням кількості загроз різного характеру, які можуть створити небезпеку – від воєнних дій до терористичних актів. Внаслідок цього виникає актуальна потреба яка полягає в оцінці ризиків для об’єктів критичної інфраструктури, що в свою чергу потребують розроблення нових математичних моделей для їх оцінки. Сучасні загрози часто мають синергетичний характер, і їх одночасна дія може істотно посилити негативний вплив на об’єкти критичної інфраструктури. Тому важливо не тільки визначити ці загрози, а й розробити методи їх комплексного аналізу.

В рамках даного дослідження пропонується удосконалена методика оцінювання загроз об’єктів критичної інфраструктури, що включає використання факторів сумарного впливу. Ці фактори визначаються коефіцієнтом сумарного впливу, який дозволяє більш точно оцінити загальний ризик, враховуючи взаємодію кількох загроз об’єктам критичної інфраструктури та їх вплив одна на одну. Запропонована методика складається з кількох основних етапів, серед яких ідентифікація об’єктів критичної інфраструктури, визначення ймовірності виникнення загрози об’єктам критичної інфраструктури на основі статистичних даних, оцінка впливу загрози

об’єктам критичної інфраструктури, моделювання комбінованого впливу, а також оцінка сукупності впливу на об’єкти критичної інфраструктури.

Теоретичні основи дослідження

Огляд останніх публікацій [1–8] показує, що, на думку багатьох провідних експертів, які досліджували питання оцінки загроз та ризиків для об’єктів критичної інфраструктури (ОКІ), загальноприйнятого підходу для оцінки ризиків та загроз для цих об’єктів досі не існує. Існують тільки часткові рішення, які охоплюють окремі типи об'єктів або конкретні варіанти техногенних загроз. Реалізація таких рішень призводить до зменшення наслідків надзвичайних ситуацій на ОКІ. Однак дані методики оцінки ризиків ОКІ зосереджені на реактивних діях для ліквідації наслідків атак на ці об’єкти, а не на проактивних заходах для попередження загроз.

У сучасних умовах де ризики значно ускладнюються масованими ракетно-дроновими ударами, наявні методики оцінки загроз для ОКІ залишаються недостатньо дієвими. Ці підходи часто не враховують комплексний характер взаємодії різних загроз ОКІ і обмежуються аналізом ризиків на локальному рівні, що не забезпечує інтегрованого підходу до управління ризиками. З досвіду міжнародної практики також видно, що увага більшого зосереджується на відновленні об’єктів після нападу, а не на попередженні або мінімізації загроз на ці об’єкти.

Загалом, аналіз зазначених наукових джерел свідчить, що сучасні підходи до захисту ОКІ мають бути орієнтованими на запобігання та зниження ймовірності загроз на ці об’єкти. Це вимагатиме розробки нових стандартів у сфері управління ризиками, які б інтегрували всі види загроз на ОКІ, передбачали можливість одночасної взаємодії різних типів ризиків і забезпечили комплексний підхід до стійкості ОКІ.

Постановка проблеми

У сучасних умовах глобалізації та технологічного прогресу ОКІ піддаються численним загрозам, які залишаються дедалі складнішими та різноманітнішими. Системи енергетики, транспорту, водопостачання, а також інформаційні технології можуть знати як фізичні, так і кібернетичні атаки, які можуть мати серйозні наслідки для національної безпеки. В умовах вогневого впливу противника виникає потреба не тільки в ефективному захисті цих об’єктів, а й у комплексному аналізі ризиків для цих об’єктів, пов’язаних із їх діяльністю. Класичні підходи до оцінки ризиків для ОКІ часто не враховують складні взаємозв’язки між більшістю типів загроз які впливають на ці об’єкти. В умовах, коли загрози для ОКІ можуть діяти синергетично, просто підсумовування ймовірностей ризиків для цих об’єктів не відображає реального стану справ та важко передбачити за допомогою традиційних моделей.

Таким чином, метою цієї роботи є удосконалення методики оцінювання загроз ОКІ під час вогневого впливу противника з урахуванням сумарного впливу загроз на ці об’єкти, яка враховує сукупний вплив різних загроз, зокрема синергетичний ефект від їх одночасної дії.

Результати

Загрози для ОКІ стають дедалі складнішими та різноманітнішими, що потребує розробки нових математичних моделей для їх оцінки. Зокрема, сучасні загрози часто є сумарними – тобто їх одночасна дія може значно підсилити негативний вплив. У цій моделі запропоновано врахувати коефіцієнт сумарного впливу K_{sum}, який дозволить більш повно оцінити загальний ризик при одночасній дії кількох загроз.

Основними етапами розробки методики оцінювання загроз ОКІ під час вогневого впливу противника з урахуванням сумарного коефіцієнту загроз яка представлена на рис. 1, є:

- ідентифікація ОКІ та потенційних загроз для цих об’єктів.

- обчислення ймовірності виникнення загроз ОКІ на основі статистичних даних та експертних оцінок.
- оцінка впливу загроз ОКІ з урахуванням індивідуальних характеристик для цих об'єктів.
- моделювання комбінованого впливу загроз ОКІ з урахуванням нової компоненти – коефіцієнта сумарного впливу.
- оцінка сукупного ризику та пріоритезація загроз ОКІ для оптимізації ресурсів захисту.

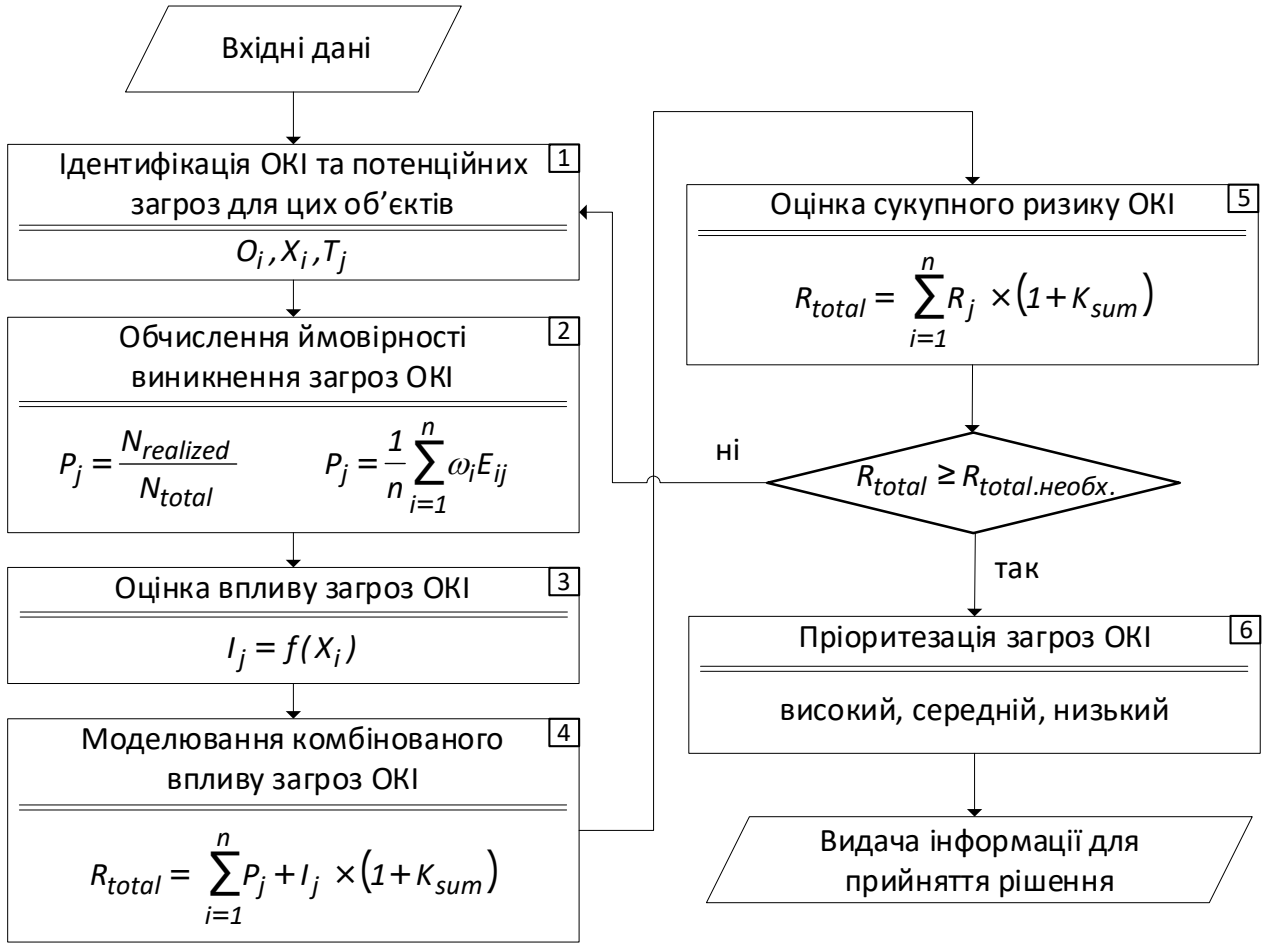

Рисунок 1– Структурно-логічна схема методики оцінювання загроз ОКІ під час вогневого впливу противника з урахуванням сумарного коефіцієнту загроз

Блок 1. Ідентифікація ОКІ та потенційних загроз для цих об'єктів.

Нехай існує множина об'єктів критичної інфраструктури O, де кожен об'єкт O_i характеризується набором параметрів X_i, що включають такі фактори, як фізична вразливість, кібернетична захищеність, критичність для національної безпеки тощо.

Загрози представляються множиною T, де кожна загроза T_j може бути фізичною, техногенною або кібернетичною. Для кожної загрози можна оцінити ймовірність виникнення P_j та її вплив на об'єкт I_j.

Блок 2. Обчислення ймовірності виникнення загроз ОКІ на основі статистичних даних та експертних оцінок.

Ймовірність виникнення кожної загрози P_j можна визначити на основі статистичних даних або експертних оцінок:

$$P_j = \frac{N_{realized}}{N_{total}}, \quad (1)$$

де, $N_{realized}$ – кількість випадків реалізації загрози за певний період,

N_{total} – загальна кількість випадків.

Якщо немає достатньо даних, використовуються експертні оцінки:

$$P_j = \frac{1}{n}\sum_{i=1}^{n}\omega_i E_{ij}, \quad (2)$$

де, E_{ij} – оцінка ймовірності загрози експертом i,

ω_i – ваговий коефіцієнт, що відображає досвід експерта.

Блок 3. Оцінка впливу загроз ОКІ з урахуванням індивідуальних характеристик для цих об’єктів.

Для кожної загрози оцінюється її можливий вплив на ОКІ I_j. Вплив може бути оцінений в економічних показниках (вартість збитків), руйнуванні інфраструктури або втратах людських життів. Вплив описується як функція від параметрів об’єкта:

$$I_j = f(X_i), \quad (3)$$

де, X_i – набір характеристик об'єкта O_i.

Блок 4. Моделювання комбінованого впливу загроз ОКІ з урахуванням нової компоненти – коефіцієнта сумарного впливу.

Загрози не завжди діють ізольовано. Часто вони взаємодіють, що може посилювати або послаблювати загальний негативний ефект. Для врахування цього синергетичного ефекту вводимо **коефіцієнт сумарного впливу** K_{syn}.

Загальний ризик для об'єкта при одночасній дії кількох загроз можна обчислити за формулою:

$$R_{total} = \sum_{i=1}^{n} P_j + I_j \times \left(1 + K_{sum}\right), \quad (4)$$

де, P_j – ймовірність виникнення загрози j,

I_j – вплив загрози j,

K_{sum} – коефіцієнт, що враховує сумарний ефект.

Приклад сумарного впливу:

Кібернетична атака на ОКІ може призвести до вимкнення систем управління, що робить його вразливішим для фізичної атаки. У такому випадку коефіцієнт K_{sum} може мати позитивне значення, скажімо K_{sum} = 0,2, що збільшує загальний ризик.

Блок 5. Оцінка сукупного ризику ОКІ.

Для кожної загрози T_j оцінюється індивідуальний ризик:

$$R_j = P_j \times I_j, \quad (5)$$

де, R_j – ризик для загрози j,

P_j – ймовірність виникнення загрози,

I_j – вплив загрози на об'єкт.

Сукупний ризик для ОКІ визначається з урахуванням всіх загроз на цей об’єкт:

$$R_{total} = \sum_{i=1}^{n} R_j \times (1 + K_{sum}), \quad (6)$$

Якщо коефіцієнт K_{sum} = 0**,** ризики загроз ОКІ не взаємодіють, і їх сумарний ефект є простим додаванням. Якщо K_{sum} > 0, загрози ОКІ підсилюють одна одну, якщо K_{sum} < 0, загрози ОКІ послаблюють одна одну.

Блок 6. Пріоритезація загроз ОКІ.

Після розрахунку сукупного ризику для кожного ОКІ можна виконати пріоритезацію загроз на цей об’єкт. Це дозволяє визначити, на які загрози ОКІ слід зосередити увагу першочергово для розробки відповідних заходів захисту.

Пріоритезація проводиться за рівнем ризику:

1. Високий ризик (потрібні негайні заходи).
2. Середній ризик (необхідні заходи протягом певного часу).
3. Низький ризик (достатньо стандартних заходів захисту).

Таким чином, запропонована в статті методика дозволяє систематично підходити до оцінки ризиків для ОКІ в умовах складних і комбінованих загроз для цих об’єктів. З урахуванням сумарного впливу вона забезпечує більш точну і гнучку оцінку, яка відображає реальні умови взаємодії різних типів загроз ОКІ. Застосування такої методики дозволяє більш ефективно розподілити ресурси, спрямовані на захист ОКІ, визначити пріоритети щодо захисних заходів та забезпечити готовність до можливих сценаріїв під час вогневого впливу противника.

Крім того, врахування коефіцієнта сумарного впливу робить можливим оцінювання ситуацій, де з’єднання загроз ОКІ створює нові, більш небезпечні умови для цих об’єктів. Це дозволяє системі захисту переходити від реактивних заходів до превентивних, забезпечуючи випереджувальне планування та підвищуючи загальний рівень надійності й стійкості ОКІ.

Висновки

У статті запропонована методика оцінювання загроз об’єктам критичної інфраструктури під час вогневого впливу противника з урахуванням сумарного коефіцієнту загроз. Дана методика дозволяє:

- оцінити загрози, які взаємодіють і мають підсилюючий або послаблюючий ефект на ОКІ;
- передбачити складні сценарії атак і більш точно планувати заходи захисту ОКІ;
- адаптувати її для різних типів ОКІ та різних типів загроз для цих об’єктів.

Описана методика може бути використана для підвищення стійкості ОКІ та ефективнішого розподілу ресурсів для їх захисту а також створить підґрунтя для вдосконалення існуючої національної системи безпеки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Фурсенко О.М., Чумаченко С.М. та Кармазин С.В. (2015). Експертна оцінка загроз для об’єктів критичної інфраструктури газотранспортної системи України з використанням методу

аналізу ієрархій. Техногенно-екологічна безпека та цивільний захист, 9, 68-77. URL : http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [Дата перегляду 1.10.2024].
2. Мурасов Р. (2023). Методика оцінки ризиків для критичної інфраструктури в умовах бойових дій з урахуванням їх руйнівного та кумулятивного потенціалу. Соціальний розвиток і безпека, 13 (1), 152-160. https://doi.org/10.33445/sds.2023.13.1.13 [Дата звернення 1.10.2024].
3. Куртсеітов, Т., Мурасов, Р., & Мельник, Я. (2022). Обчислення надійності системи критичної інфраструктури шляхом декомпозиції її як складної системи. Social Development and Security, 12(5), 84-92. https://doi.org/10.33445/sds.2022.12.5.8 [Дата звернення 1.10.2024].
4. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. (2024). Удосконалення науково-методичного апарату для розрахунку ризиків виникнення та аналізу сценаріїв надзвичайних ситуацій на об'єктах критичної інфраструктури. Social Development and Security, 14 (1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17 [Дата звернення 1.10.2024].
5. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. (2024). Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій. Сучасні інформаційні технології у сфері безпеки та оборони, 3(48), 35-43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [Дата звернення 1.10.2024].
6. Мурасов Р., Мещеряков І. (2023). Інформаційно-технічний спосіб попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості поступового наростання руйнівних явищ, викликаних каскадними наслідками первинного терористичного впливу. Соціальний розвиток і безпека, 13 (5), 180-191. https://doi.org/10.33445/sds.2023.13.5.17 [Дата звернення 1.10.2024].
7. Яременко О.І., Страхніцький Я.О. (2022). Визначення та управління загрозами у структурі державної політики захисту критичної інфраструктури. Університетські наукові записки, 3 (87), 73-82. https://doi.org/10.37491/UNZ.87.6 [Дата звернення 1.10.2024].
8. Бобро Д. (2015). Визначення критеріїв оцінки та загроз критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка, 4, 83-93. URL : http://nbuv.gov.ua/UJRN/spe_2015_4_12 [Дата звернення 1.10.2024].

References

1 Fursenko O.M., Chumachenko S.M. & Karmazyn S.V. (2015). Expert assessment of threats to objects of critical infrastructure of the gas transportation system of Ukraine using the method of analysis of hierarchies. *Technogenic and ecological safety and civil protection*, 9, 68-77. Available from : http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [View date 1.10.2024].
2. Murasov, R. (2023). The method of risk assessment for critical infrastructure in the conditions of hostilities, taking into account their destructive and cumulative potential. *Social Development and Security*, 13(1), 152-160. https://doi.org/10.33445/sds.2023.13.1.13 [Accessed date 1.10.2024].
3. Kurtseitov, T., Murasov, R., & Melnyk, Y. (2022). Calculating the reliability of a critical infrastructure system by decomposing it as a complex system. *Social Development and Security*, 12(5), 84-92. https://doi.org/10.33445/sds.2022.12.5.8 [Accessed date 1.10.2024].
4. Murasov, R., Nikitin, A., Meshcheriakov, I., Pidhorodetskyi, M., & Poplavets, S. (2024). Improvement of the scientific and methodological apparatus for calculating the risks of occurrence and analyzing scenarios of emergency situations at critical infrastructure facilities.

Social Development and Security, 14(1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17 [Accessed date 1.10.2024].

5. Murasov, R., Nikitin, A., Meshcheriakov, I., Pidhorodetskyi, M., & Poplavets, S. (2024).Methodology for assessing threats and risks for critical infrastructure objects under emergency development scenarios. *Modern Information Technologies in the Sphere of Security and Defence*, 3(48), 35-43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [Accessed date 1.10.2024].
6. Murasov, R., & Meshcheriakov, I. (2023). The information and technical method of preventing emergency situations of a terrorist nature by assessing the possibility of gradual growth of destructive events caused by the cascading consequences of the primary terrorist impact. *Social Development and Security*, 13(5), 180-191. https://doi.org/10.33445/sds.2023.13.5.17 [Accessed date 1.10.2024].
7. Yaremenko O., Strahnitskyi Y. (2022). Detection and Management of Threats in the Structure of State Policy for Critical Infrastructure Protection. University Scientific Notes, 3 (87), 73-82. https://doi.org/10.37491/UNZ.87.6 [Accessed date 1.10.2024].
8. Bobro D. (2015). Determination of assessment criteria and threats to critical infrastructure. *Strategic priorities. Series: Economics*, 4, 83-93. Available from : http://nbuv.gov.ua/UJRN/spe_2015_4_12 [View date 1.10.2024].