Інформаційно-технічний метод захисту стратегічних об’єктів України від засобів повітряного нападу

Information-Technical Method for Protecting Ukraine’s Strategic Facilities Against Aerial Attacks

Геннадій Камишенцев [A]
доктор технічних наук, провідний науковий співробітник відділу науково-методичного забезпечення діяльності, e-mail: genana1976@ukr.net, ORCID ID: https://orcid.org/0000-0002-5780-3539

Михайло Прокофьєв [B]
доктор технічних наук, професор, професор кафедри прикладної математики та кібербезпеки, e-mail: m.prokofiev@donnu.edu.ua, ORCID ID: https://orcid.org/0000-0001-9388-3735

Василь Малярчук [A]
кандидат технічних наук, доцент, доцент кафедри компютерних систем та мереж, e-mail: vasyl.maliarchuk@npp.nau.edu.ua, ORCID ID: https://orcid.org/0009-0008-5435-4601

Ольга Шевченко [A]
Corresponding author: доктор технічних наук, старший науковий співробітник, e-mail: shevchenkoolga2008@gmail.com, ORCID ID: https://orcid.org/0000-0003-2106-5009

Юлія Погрібна [C]
ад’юнкт, e-mail: pohribna.yuliia_2025phd@nuczu.edu.ua, ORCID ID: https://orcid.org/0009-0007-2746-6459

Hennadii Kamyshentsev [A]
Doctor of Technical Sciences, Leading Researcher of the Department of Scientific and Methodological Support of Activities, e-mail: genana1976@ukr.net, ORCID ID: https://orcid.org/0000-0002-5780-3539

Mykhailo Prokofiev [B]
Doctor of Technical Sciences, Associate Professor, Professor of the Department, e-mail: m.prokofiev@donnu.edu.ua, ORCID ID: https://orcid.org/0000-0001-9388-3735

Vasyl Maliarchuk [A]
Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Computer Systems and Networks, e-mail: vasyl.maliarchuk@npp.nau.edu.ua, ORCID ID: https://orcid.org/0009-0008-5435-4601

Olha Shevchenko [A]
Corresponding author: Doctor of Technical Sciences (D.Sc. in Engineering),Senior Research Fellow, e-mail: shevchenkoolga2008@gmail.com, ORCID ID: https://orcid.org/0000-0003-2106-5009

Yuliia Pogribna [C]
PhD Student, e-mail: pohribna.yuliia_2025phd@nuczu.edu.ua, ORCID ID: https://orcid.org/0009-0007-2746-6459

[A] Державне некомерційне підприємство “Державний університет ‘Київський авіаційний інститут’”, м. Київ, Україна
[B] Донецький національний університет імені Василя Стуса, м. Вінниця, Україна
[C] Національний університет цивільного захисту України, м. Черкаси, Україна

[A] State Non-Commercial Company “State University ‘Kyiv Aviation Institute’”, Kyiv, Ukraine
[B] Vasyl’ Stus Donetsk National University, Vinnytsia, Ukraine
[C] National University of Civil Protection of Ukraine, Cherkasy, Ukraine

Received: August 22, 2026 | Revised: September 26, 2026 | Accepted: October 31, 2026

УДК 351.86

DOI: https://doi.org/10.33445/sds.2026.16.5.48

Мета роботи. Обґрунтувати структуру та зміст інформаційно-технічного методу протидії загрозам національній безпеці України шляхом забезпечення захисту стратегічного об’єкта від засобів повітряного нападу.

Методи дослідження. Застосовано системний і структурно-функціональний підходи, методи аналізу, узагальнення, декомпозиції, математичного моделювання та алгоритмізації. Метод Пампуро використано як математичну основу формалізації режимів функціонування системи захисту стратегічного об’єкта.

Результати дослідження. Набули подальшого розвитку науково-методичні засади побудови інформаційно-технічного методу захисту стратегічного об’єкта. Раніше розроблену математичну модель інтегровано в єдину структуру управління, що охоплює семимодульний керуючий алгоритм і сім процедур практичного застосування. Математична модель описує шість режимів функціонування системи безпеки: чотири у повсякденних умовах і два під час безпосереднього повітряного нападу. Керуючий алгоритм забезпечує формалізоване представлення процесів аналізу обстановки, поповнення ресурсів, вибору режиму функціонування, виявлення

Purpose. To substantiate the structure and content of an information-technical method for countering threats to Ukraine’s national security by protecting a strategic facility against aerial attacks.

Research methods. Systems and structural-functional approaches, analysis, generalization, decomposition, mathematical modelling, and algorithm development were employed. The Pampuro method was used as the mathematical basis for formalizing the operating modes of the strategic facility protection system.

Research findings. The scientific and methodological foundations for developing an information-technical method for strategic facility protection were further advanced. A previously developed mathematical model was integrated into a unified management framework comprising a seven-module control algorithm and seven practical application procedures. The mathematical model describes six operating modes of the security system: four under routine conditions and two during a direct aerial attack. The control algorithm provides a formalized representation of situation analysis, resource replenishment, operating mode selection, threat detection, attack response, consequence management, and preparation

небезпеки, відбиття нападу, ліквідації наслідків і підготовки до повторного впливу. Визначено функціональну відповідність між режимами математичної моделі, модулями алгоритму та процедурами практичного застосування.

Теоретична цінність дослідження. Запропоновано цілісне представлення управління системою захисту стратегічного об'єкта в умовах ресурсних обмежень. Результати створюють методологічні передумови для розроблення систем підтримки прийняття управлінських рішень. Практична результативність методу потребує подальшої перевірки шляхом імітаційного моделювання.

Тип статті. Теоретико-методична.

Ключові слова: національна безпека, стратегічний об'єкт, інформаційно-технічний метод, засоби повітряного нападу, математична модель, керуючий алгоритм, система захисту, управління безпекою.

for subsequent attacks. Functional relationships were established among the operating modes of the mathematical model, the algorithm modules, and the practical application procedures.

Theoretical implications. An integrated representation of strategic facility protection management under resource constraints was proposed. The findings provide a methodological basis for developing management decision-support systems. The practical effectiveness of the proposed method requires further verification through simulation modelling.

Article type. Theoretical and methodological.

Key words: national security, strategic facility, information-technical method, aerial attack assets, mathematical model, control algorithm, protection system, security management.

Вступ

Систему безпеки стратегічного об'єкта — підприємства, обмеженої території, хвостосховища або комплексу об'єктів атомної електростанції — можна представити як сукупність чотирьох взаємопов'язаних складових: об'єкта захисту, підсистеми моніторингу небезпеки, підсистеми підтримки прийняття рішень і підсистеми виконання прийнятих рішень, яка здійснює керуючий вплив на об'єкт та змінює його стан [1, 2]. Такий підхід застосовують для забезпечення техногенної, радіаційної та екологічної безпеки, організації фізичного захисту й протидії навмисним впливам на об'єкти критичної інфраструктури [1–3].

Правові засади відповідної діяльності визначено законодавством України у сфері національної безпеки та захисту критичної інфраструктури [4, 5]. Для ядерних установок, ядерних матеріалів, радіоактивних відходів та інших джерел іонізуючого випромінювання встановлено спеціальні вимоги до створення та функціонування систем фізичного захисту [3]. Нормативно-правовими положеннями також передбачено координацію та взаємодію суб'єктів, залучених до виконання відповідних завдань [4, 5].

Практична реалізація такої взаємодії ускладнюється організаційною та технічною неоднорідністю підсистем моніторингу, управління й реагування, які можуть належати різним відомствам і використовуватися для виконання різних завдань [1, 2]. Це ускладнює своєчасний обмін інформацією, формування узгоджених управлінських рішень і спільне використання наявних сил та засобів.

Необхідність удосконалення наявних підходів додатково зумовлена зміною характеру загроз в умовах бойових дій. Ракетно-артилерійські ураження створюють воєнно-техногенне навантаження, спричиняють порушення стану територій і можуть мати довготривалі небезпечні наслідки [6]. Застосування ударних безпілотних літальних апаратів характеризується різною інтенсивністю та послідовністю здійснення атак протягом обмежених проміжків часу [7].

Використання безпілотних літальних апаратів для ураження ядерних об'єктів може становити загрозу їхній безпеці та нормальному функціонуванню, що зумовлює необхідність здійснення заходів із виявлення, затримання та нейтралізації таких засобів [8]. За цих умов необхідно забезпечити ідентифікацію засобів повітряного нападу, вибір режиму функціонування системи захисту, розподіл обмежених ресурсів, формування команд щодо протидії загрозам та організацію ліквідації можливих наслідків.

Наявні підходи охоплюють фізичний захист критичної інфраструктури, моніторинг, запобігання виникненню та ліквідацію надзвичайних ситуацій, а також протидію загрозам, пов'язаним із застосуванням безпілотних літальних апаратів [1, 2, 8]. Водночас ці підходи не забезпечують формування єдиного методологічного підґрунтя, яке поєднувало б

математичний опис стану об’єкта, алгоритми оброблення інформації та прийняття управлінських рішень із процедурами практичного застосування наявних сил і засобів.

Таким чином, **метою дослідження** є обґрунтування структури та змісту інформаційно-технічного методу протидії загрозам національній безпеці України шляхом забезпечення захисту стратегічного об’єкта від засобів повітряного нападу.

Для досягнення поставленої мети визначено такі наукові завдання:

1. Обґрунтувати необхідність розроблення інформаційно-технічного методу, визначити його призначення та основні складові.
2. Розглянути математичну модель, покладену в основу інформаційно-технічного методу.
3. Розкрити структуру та зміст керуючого алгоритму запропонованого методу.
4. Охарактеризувати процедури практичного застосування розробленого методу.

Огляд літератури

Дослідження критичної інфраструктури охоплюють визначення взаємозалежностей між її складовими, моделювання поширення порушень, оцінювання вразливості та здатності систем зберігати основні функції. Зміна стану одного елемента може безпосередньо або опосередковано впливати на функціонування інших. Для аналізу таких зв’язків виокремлюють фізичні, кібернетичні, географічні та логічні взаємозалежності [9]. Фізичні взаємозалежності пов’язані з передаванням матеріальних або енергетичних потоків, кібернетичні — з обміном інформацією, географічні — із просторовою близькістю об’єктів, а логічні охоплюють інші організаційні та функціональні зв’язки.

Для моделювання взаємозалежної критичної інфраструктури застосовують, зокрема, емпіричні, агентні, системно-динамічні, економічні та мережеві підходи [10]. Емпіричні моделі залежать від повноти даних про фактичні порушення, агентні — від визначених параметрів і правил взаємодії, системно-динамічні описують зміни в часі та зворотні зв’язки, економічні — міжгалузеві наслідки, а мережеві дають змогу визначати критичні вузли та шляхи поширення відмов. Вибір відповідного підходу залежить від мети дослідження, доступності вихідних даних і необхідного рівня деталізації.

Оцінювання вразливості та ризиків ускладнюється взаємозалежністю компонентів, динамічним характером порушень, недостатністю статистичних даних і невизначеністю можливих сценаріїв [11]. Тому під час аналізу поєднують структурні, функціональні, динамічні та ймовірнісні моделі, що дає змогу враховувати можливість каскадного розвитку порушень, однак підвищує вимоги до складу та повноти вихідної інформації.

Операційна стійкість критичної інфраструктури пов’язана зі здатністю системи виконувати основні функції в умовах порушення її роботи [12]. Відповідні моделі дають змогу порівнювати наслідки різних сценаріїв, визначати критичні компоненти та оцінювати захисні й відновлювальні заходи. Для їх застосування до конкретного стратегічного об’єкта необхідно визначити його склад, функціональні зв’язки, критерії працездатності, можливі сценарії пошкодження та доступні ресурси.

Перехід від оцінювання вразливості до управління захистом передбачає визначення пріоритетних компонентів і розподіл обмежених ресурсів. Для цього використовують дворівневі та трирівневі оптимізаційні моделі, які враховують послідовну взаємодію захисника, нападника та системи після пошкодження [13]. Теоретико-ігрові моделі також дають змогу визначати умови, за яких попереднє посилення захисту окремих об’єктів може зменшити очікувані втрати або стримати напад [14]. Отримані результати залежать від вартості захисних заходів, можливих цілей, наслідків пошкодження та прийнятої послідовності дій сторін. Водночас такі моделі переважно зосереджені на стратегічному розподілі ресурсів і не описують оперативної зміни режимів функціонування системи під час розвитку небезпечної події.

Для протидії загрозам, пов'язаним із застосуванням безпілотних літальних апаратів, запропоновано концептуальну архітектуру захисту ядерних об'єктів, яка поєднує засоби виявлення, реагування та зменшення можливих наслідків [15]. Такий підхід передбачає використання сенсорних і виконавчих засобів, однак має переважно концептуальний характер і не визначає критеріїв розподілу обмежених ресурсів між складовими системи.

Для виявлення та класифікації безпілотних літальних апаратів використовують радіолокаційні, радіочастотні, оптичні, інфрачервоні й акустичні засоби [16, 17]. Радіолокаційне виявлення малорозмірних цілей може ускладнюватися відбиттям сигналів від навколишніх об'єктів. Ефективність радіочастотних засобів залежить від наявності сигналів керування або передавання даних, оптичних та інфрачервоних — від умов видимості, а акустичних — від дальності виявлення та рівня фонового шуму. Отже, використання окремого каналу спостереження не забезпечує однакової ефективності за всіх умов.

Для підвищення достовірності виявлення застосовують об'єднання інформації від кількох сенсорів і методи глибокого навчання [18]. Багатосенсорний підхід дає змогу зіставляти ознаки різної фізичної природи та частково компенсувати обмеження окремих каналів спостереження. Його практична реалізація потребує узгодженого оброблення інформаційних потоків і передавання отриманих результатів до підсистеми підтримки прийняття рішень.

Придатність сенсорів оцінюють за ймовірністю виявлення, частотою хибних спрацювань, похибками вимірювання та конфігурацією їх розміщення [19]. Імітаційне моделювання дає змогу попередньо обґрунтувати склад і схему розташування засобів моніторингу. Для міського середовища окремо розглядають пасивні радіочастотні, акустичні та візуальні системи [20]. Їх застосування ускладнюється щільною забудовою, фоновим шумом, перекриттям сигналів та обмеженнями прямої видимості, що впливає на точність визначення координат і безперервність супроводження безпілотних літальних апаратів.

У вітчизняних дослідженнях розглянуто застосування радіолокаційних і відеоінформаційних засобів для захисту об'єктів критичної інфраструктури. Зокрема, для імпульсної радіолокаційної станції проаналізовано структуру, принцип функціонування, технічні характеристики та складові енергетичного потенціалу, які визначають можливу дальність виявлення повітряних об'єктів [21].

Інформаційно-технічні методи із застосуванням зовнішнього відеоспостереження забезпечують отримання та оброблення інформації про стан контрольованої території, а також виявлення ознак небезпечного впливу [22, 23]. Активні імпульсні радіолокаційні засоби використовують для виявлення та контролю переміщення потенційно небезпечних об'єктів незалежно від умов природного освітлення [24, 25].

Алгоритмічний підхід до побудови інформаційно-технічних методів застосовано для запобігання виникненню надзвичайних ситуацій на територіях, що зазнали ракетно-артилерійських уражень [26]. Він охоплює збирання та аналіз даних, визначення пріоритетних ділянок, вибір схеми моніторингу, проведення контролю та прийняття управлінських рішень.

Подальший розвиток цього підходу передбачає поєднання математичної моделі, керуючого алгоритму та процедур практичного застосування в межах організаційно-технічного методу [27]. Водночас дослідження [26, 27] орієнтовані на моніторинг територій після ракетно-артилерійських уражень і не враховують особливостей функціонування засобів виявлення та протидії безпосередньо під час повітряного нападу.

Для формалізації взаємодії технічно різнорідних елементів системи управління запропоновано метод Пампуро, який ґрунтується на представленні матеріальних, енергетичних та інформаційних потоків через відповідні інформаційні змінні [28].

На основі цього методу сформовано математичну модель забезпечення максимально можливого рівня безпеки стратегічного об'єкта за обмеженого обсягу виділених коштів [29].

Модель описує чотири варіанти використання засобів безпеки у повсякденних умовах і два режими функціонування під час атаки: зі зростанням інтенсивності впливу за експоненціальним законом та зі збереженням її максимального рівня протягом обмеженого проміжку часу.

Таким чином, наявні дослідження охоплюють моделювання взаємозалежностей і стійкості критичної інфраструктури, розподіл ресурсів захисту, архітектуру протидії безпілотним літальним апаратам, технічні засоби їх виявлення, алгоритмічні процедури моніторингу та математичне представлення режимів функціонування системи безпеки. Проте в розглянутих працях не сформовано єдиного інформаційно-технічного методу, який поєднував би математичну модель, багаторівневий керуючий алгоритм і процедури вибору режиму функціонування, застосування обмежених сил і засобів, ліквідації наслідків та відновлення готовності системи захисту стратегічного об’єкта.

Методологія дослідження

Методологічну основу дослідження становлять системний і структурно-функціональний підходи, відповідно до яких захист стратегічного об’єкта розглядається як цілісна система взаємопов’язаних засобів виявлення небезпеки, протидії засобам повітряного нападу, ліквідації можливих наслідків та управління їх застосуванням. Методи аналізу й узагальнення використано для обґрунтування призначення інформаційно-технічного методу, визначення його основних складових, а також складу сил і засобів забезпечення безпеки стратегічного об’єкта.

Дослідження проведено послідовно у три етапи.

На першому етапі із застосуванням методу декомпозиції визначено три взаємопов’язані складові інформаційно-технічного методу: математичну модель, керуючий алгоритм і процедури практичного застосування.

На другому етапі за допомогою математичного моделювання та методу Пампуро формалізовано режими функціонування системи захисту стратегічного об’єкта у повсякденних умовах і під час безпосереднього повітряного нападу.

На третьому етапі із застосуванням методу алгоритмізації визначено послідовність отримання та оброблення інформації, оцінювання стану сил і засобів, вибору режиму функціонування системи захисту, формування управлінських рішень, ліквідації наслідків повітряного нападу та відновлення готовності системи до можливого повторного впливу.

На основі структурно-функціонального аналізу сформовано семимодульний керуючий алгоритм і визначено прямі та зворотні інформаційні зв’язки між його модулями. Узгодження режимів математичної моделі з модулями керуючого алгоритму стало основою для формування семи процедур практичного застосування інформаційно-технічного методу. Це дало змогу поєднати математичне представлення процесів функціонування системи захисту з послідовністю прийняття управлінських рішень і практичного застосування наявних сил та засобів в умовах ресурсних обмежень.

Результати дослідження

Відповідно до положень, викладених у праці [1], структура інформаційно-технічного методу охоплює три взаємопов’язані елементи.

Першим елементом є модель, яка формалізує досліджуваний процес, у цьому випадку — процес управління безпекою стратегічного об’єкта. Залежно від характеру завдання та застосованого методологічного апарату модель може бути когнітивною, математичною, імітаційною або іншого типу.

Другим елементом є керуючий алгоритм, який забезпечує реалізацію моделі, відображає взаємозв’язки між складовими досліджуваного процесу та створює основу для розроблення програмного забезпечення, призначеного для практичного застосування методу.

Третім елементом є процедури, які визначають порядок практичного застосування інформаційно-технічного методу для досягнення встановленого результату. Вони охоплюють сукупність відповідних протоколів і послідовність їх виконання.

В основу інформаційно-технічного методу протидії загрозам національній безпеці України шляхом забезпечення захисту стратегічного об'єкта від засобів повітряного нападу покладено математичну модель захисту стратегічного об'єкта від терористичних загроз за умови обмеженого обсягу виділених коштів.

Математична модель складається з двох взаємопов'язаних підсистем. Перша підсистема описує чотири варіанти функціонування засобів забезпечення безпеки об'єкта у повсякденних умовах за наявності потенційної загрози терористичного впливу. Друга підсистема характеризує два варіанти функціонування системи під час безпосередньої терористичної атаки.

Кожний варіант представлено системою двох співвідношень: частотною характеристикою абстрактного чотириполюсника та відповідною характеристикою, визначеною за методом Пампуро.

Перший варіант першої підсистеми характеризує функціонування системи безпеки у денний час із використанням чергових засобів. Для цього режиму математичні співвідношення наведено у формулі (1).

$$\begin{cases} K_0(j\omega) = \frac{K_0}{1+j\omega t_0}, \\ T_0 = \sqrt{\frac{N_0}{N_0+2}}, \end{cases} \quad (1)$$

де $K_0(j\omega)$ – частотна характеристика абстрактного чотириполюсника;

K_0 – коефіцієнт спряження абстрактного чотириполюсника;

j – уявна одиниця;

ω – кругова частота;

t_0 – стала часу абстрактного чотириполюсника, що характеризує його інерційність;

T_0 – характеристика абстрактного чотириполюсника, визначена за методом Пампуро;

N_0 – числова характеристика, що враховує всі засоби, залучені до забезпечення безпеки об'єкта: засоби виявлення небезпеки, засоби її запобігання або знищення та засоби ліквідації наслідків у разі реалізації небезпеки.

Другий варіант першої підсистеми описує функціонування системи безпеки в нічний час та за умов обмеженої видимості з використанням чергових засобів. У цьому випадку враховуються параметри корисного інформаційного сигналу та інформаційного шуму (2).

$$\begin{cases} K_0(j\omega) = \frac{2\alpha{\sigma_s}^2}{2\alpha{\sigma_s}^2+\alpha^2H_0+H_0(\omega-\omega_0)^2} + \frac{2\alpha{\sigma_s}^2}{2\alpha{\sigma_s}^2+\alpha^2H_0+H_0(\omega+\omega_0)^2} \\ T_0 = \sqrt{\frac{N_0}{N_0+2}} \end{cases}, \quad (2)$$

де α – коефіцієнт, що показує відношення результату інформаційного впливу на абстрактний чотириполюсник до квадрата мінімальної похибки трансформації всього інформаційного потоку, який проходить через чотириполюсник;

${\sigma_s}^2$ – середній квадрат похибки;

H_0 – інтенсивність інформаційного шуму;

ω_0 – початкова кругова частота.

Третій варіант першої підсистеми передбачає залучення всіх наявних засобів захисту об'єкта. Для фізично реалізованого абстрактного чотириполюсника відповідну систему співвідношень наведено у формулі (3).

$$\begin{cases} K(j\omega) = \frac{\beta}{\beta + j\omega} \\ T_0 = \frac{1}{\beta} = \frac{\sqrt{N_0}}{2\sigma_s\sqrt{\alpha} - \alpha\sqrt{N_0}} \end{cases}, \quad (3)$$

де $K(j\omega)$ – коефіцієнт, що показує відношення результату інформаційного впливу на абстрактний чотириполюсник до квадрата мінімальної похибки трансформації всього інформаційного потоку, який проходить через чотириполюсник;

β – величина, що визначається інформаційним потоком, який надходить на вхід системи.

Четвертий варіант першої підсистеми характеризує оптимальне використання власних засобів захисту об'єкта та зовнішніх сил і засобів. У цьому випадку частотна характеристика зберігає форму, прийняту для третього варіанта, однак відповідне співвідношення додатково враховує часовий зсув (4).

$$\begin{cases} K(j\omega) = \frac{\beta}{\beta + j\omega} \\ T_0 = \frac{1}{[\frac{4\alpha\sigma_S{}^2}{N_0}(2\mathrm{e}^{-\alpha\Delta} - 1)]^{0,5} - \alpha} \end{cases}, \quad (4)$$

де $K\Delta$ – зсув у часі, що визначається робочим часом абстрактного чотириполюсника;

e – основа натурального логарифма.

Перший варіант другої підсистеми відповідає ситуації, за якої інтенсивність терористичного впливу зростає за експоненціальним законом протягом обмеженого проміжку часу. Для цього випадку систему співвідношень наведено у формулі (5).

$$\begin{cases} K_0(j\omega) = \frac{A}{j\omega}\exp(j\omega t_v) \\ T_0 = \frac{N_0}{2At_v} \end{cases}, \quad (5)$$

де A – інтенсивність впливу;

t_v – тривалість впливу;

$\exp(j\omega t_v)$ – експоненціальний множник, що враховує часові параметри впливу. Інші позначення відповідають наведеним раніше.

Другий варіант другої підсистеми характеризує терористичний вплив, інтенсивність якого досягає максимального значення та залишається на цьому рівні протягом обмеженого проміжку часу. Відповідну систему співвідношень наведено у формулі (6).

$$\begin{cases} K_0(j\omega) = A\exp(j\omega t_v) \\ T_0 = \frac{N_0}{2eAt_v} \end{cases}, \quad (6)$$

Таким чином, системи співвідношень (1)–(4) описують чотири варіанти функціонування засобів забезпечення безпеки стратегічного об'єкта у повсякденних умовах, тоді як системи (5) і (6) характеризують два варіанти функціонування під час безпосередньої терористичної атаки.

Послідовне застосування зазначених співвідношень дає змогу формалізувати вибір режиму функціонування системи захисту залежно від умов обстановки, параметрів інформаційного впливу та складу наявних сил і засобів.

Керуючий алгоритм інформаційно-технічного методу

Керуючий алгоритм інформаційно-технічного методу протидії загрозам національній безпеці України шляхом захисту стратегічного об'єкта від засобів повітряного нападу реалізує математичну модель захисту стратегічного об'єкта від терористичних загроз в умовах обмеженого фінансування. Схему алгоритму наведено на рис. 1.

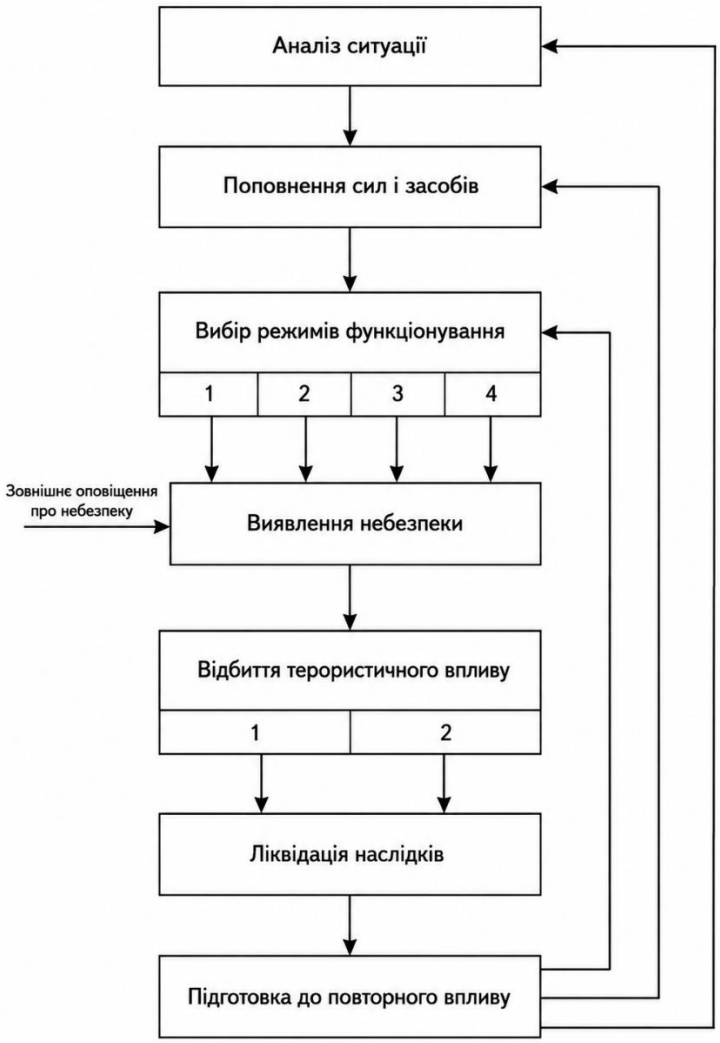


Рисунок 1. Схема керуючого алгоритму інформаційно-технічного методу протидії загрозам національній безпеці України

Джерело: розроблено авторами.

Структура керуючого алгоритму охоплює сім взаємопов'язаних модулів, розташованих на відповідних ієрархічних рівнях.

Перший ієрархічний рівень – модуль аналізу ситуації.

На цьому рівні здійснюється оброблення інформації, що надходить із зовнішніх і внутрішніх джерел.

До зовнішніх джерел належать органи та структури, які здійснюють керівництво об'єктом критичної інфраструктури або управління його безпекою. Від них надходить інформація про можливі чи очікувані терористичні атаки, технічні характеристики засобів нападу, імовірну тактику їх застосування та наявні способи протидії. Крім того, враховуються відомості про заплановане постачання запасних частин, боєкомплектів, продовольства, води, побутового приладдя та інших ресурсів, необхідних для тривалого функціонування системи безпеки.

Внутрішню інформацію поділяють на оперативну та організаційно-технічну.

Оперативна інформація охоплює відомості про появу ознак небезпеки або наближення засобів терористичного впливу, зокрема виникнення радіоперешкод, появу світлових сигналів, застосування сигнальних чи піротехнічних засобів, а також виявлення та ідентифікацію ракет, безпілотних літальних апаратів або інших повітряних цілей. Після підтвердження небезпеки відповідні дані передають керівництву та підрозділам, призначеним для запобігання загрозі або її нейтралізації.

Організаційно-технічна інформація характеризує стан засобів виявлення небезпеки, протидії загрозам та ліквідації можливих наслідків. Її аналіз дає змогу оцінити готовність системи безпеки й визначити потребу в поповненні сил і ресурсів. Узагальнені результати передають на другий ієрархічний рівень.

Другий ієрархічний рівень – модуль поповнення сил і засобів.

Призначення цього модуля полягає в підтриманні необхідного складу та готовності трьох основних складових системи безпеки: засобів виявлення небезпеки, засобів її запобігання або нейтралізації та засобів ліквідації наслідків.

До першої складової належать стаціонарні, мобільні та переносні засоби виявлення повітряних цілей, які використовують радіолокаційні, інфрачервоні, акустичні, оптико-електронні, оптичні та інші методи контролю повітряного простору. Вона охоплює як технічні системи, так і обслуги, які забезпечують їх безперервне функціонування шляхом організації позмінної роботи.

Другу складову утворюють засоби запобігання небезпеці або її нейтралізації. До них належать стаціонарні, пересувні та переносні зенітні ракетні комплекси, великокаліберні й малокаліберні зенітні гармати, позиції із зенітною стрілецькою зброєю, засоби радіоелектронної боротьби та маскування. Їх готовність залежить від технічного стану озброєння, наявності боєкомплекту та організації позмінної роботи обслуг.

Третя складова охоплює сили й засоби ліквідації наслідків. До неї належать пожежно-рятувальні підрозділи, спеціальна техніка для знешкодження боєприпасів та інших вибухонебезпечних предметів, інженерні машини для розбирання завалів і визволення людей, а також автомобілі екстреної медичної допомоги з відповідними бригадами.

За результатами оцінювання фактичного стану зазначених складових формують заявки на поповнення ресурсів із запасів об’єкта або органу управління вищого рівня. Інформацію про укомплектованість системи передають до модуля вибору режиму функціонування.

Третій ієрархічний рівень – модуль вибору режиму функціонування.

На підставі даних про поточну обстановку та готовність сил і засобів визначають один із чотирьох варіантів повсякденного функціонування системи безпеки.

Перший варіант застосовують у денний час із використанням чергових засобів. Основу спостереження в цьому режимі становлять радіолокаційні та панорамні оптико-електронні системи, можливості яких доповнюються візуальним контролем.

Другий варіант передбачено для нічного часу та умов обмеженої видимості. У цьому випадку пріоритет надають інфрачервоним і акустичним засобам, здатним виявляти повітряні цілі за відсутності належних умов для візуального спостереження.

Третій варіант передбачає залучення всіх наявних засобів об’єкта. Його застосовують у разі надходження інформації про підготовку повітряного нападу, зокрема після оголошення повітряної тривоги в регіоні розташування об’єкта критичної інфраструктури.

Четвертий варіант полягає в оптимальному поєднанні власних і зовнішніх сил та засобів. Його застосування доцільне після відбою повітряної тривоги, якщо терористична атака не відбулася, однак імовірність її здійснення зберігається.

Інформацію про вибраний режим функціонування передають до модуля виявлення небезпеки.

Четвертий ієрархічний рівень – модуль виявлення небезпеки.

Цей модуль отримує інформацію з попереднього рівня та від зовнішніх систем оповіщення. У разі підтвердження загрози забезпечується формування стандартизованих повідомлень і команд щодо переведення структурних підрозділів об'єкта у вищий ступінь готовності. Після виявлення та ідентифікації повітряної цілі формалізовані дані передають до модуля відбиття терористичного впливу.

П'ятий ієрархічний рівень – модуль відбиття терористичного впливу.

У межах цього модуля формують управлінські команди щодо застосування засобів протидії, захисту об'єкта та виконання першочергових заходів у разі його пошкодження.

Залежно від характеру атаки передбачено два варіанти розвитку ситуації.

Перший варіант характеризується експоненціальним зростанням інтенсивності терористичного впливу протягом обмеженого проміжку часу. Такий сценарій може розвиватися внаслідок послідовного застосування розвідувальних безпілотних літальних апаратів, які виявляють уразливі елементи системи захисту, та подальшого спрямування на них ударних безпілотних літальних апаратів і крилатих ракет. У міру залучення додаткових засобів нападу інтенсивність впливу зростає.

Другий варіант відповідає ситуації, за якої інтенсивність впливу досягає максимального значення та зберігається протягом певного проміжку часу. Це відбувається в разі зосередження основних засобів нападу на одному напрямку або на окремій ділянці об'єкта. За таких умов частина повітряних цілей може подолати систему захисту та спричинити пошкодження. Відомості про характер і масштаби пошкоджень передають на наступний ієрархічний рівень.

Шостий ієрархічний рівень – модуль ліквідації наслідків.

У межах цього модуля формують управлінські рішення щодо локалізації небезпечних чинників, рятування людей, надання допомоги постраждалим, усунення пошкоджень і відновлення функціонування основних та допоміжних елементів об'єкта в найкоротший строк. Інформацію про характер виконаних робіт, залишкові пошкодження та наявні ресурси передають на сьомий ієрархічний рівень.

Сьомий ієрархічний рівень — модуль підготовки до повторного терористичного впливу.

Призначення цього модуля полягає у відновленні готовності об'єкта та системи його захисту до функціонування в умовах збереження або повторного виникнення загрози.

У межах модуля оцінюють стан сил і засобів після відбиття атаки та ліквідації її наслідків, уточнюють уразливі ділянки, відновлюють працездатність засобів виявлення і протидії, поповнюють боєкомплект, запасні частини, матеріально-технічні та медичні ресурси, а також здійснюють перерозподіл обслуг і технічних засобів.

За результатами оцінювання формують пропозиції щодо зміни режиму функціонування системи безпеки, посилення окремих напрямків захисту та залучення зовнішніх сил і засобів.

Оновлена інформація, отримана через зворотний зв'язок, надходить до модулів аналізу ситуації, поповнення сил і засобів та вибору режиму функціонування. Це забезпечує циклічність керуючого алгоритму та підтримання готовності системи до можливого повторного терористичного впливу.

Функціональний зв'язок між математичною моделлю, керуючим алгоритмом і процедурами практичного застосування визначається умовами вибору режиму функціонування системи захисту, складом залучених модулів, відповідними практичними процедурами та результатами їх виконання.

У таблиці 1 номери модулів відповідають семи ієрархічним рівням керуючого алгоритму, описаним вище, а номери процедур — семи процедурам практичного застосування методу, наведеним після таблиці.

Таблиця 1. Відповідність умов обстановки режимам математичної моделі, модулям керуючого алгоритму та процедурам практичного застосування

Умова вибору	Режим математичної моделі	Задіяні модулі алгоритму	Процедури практичного застосування	Результат
Безпосередню загрозу не виявлено; денний час і достатня видимість	Режим 1	1–3 із передаванням даних до модуля 4	1–3	Функціонування чергових засобів у денному режимі
Безпосередню загрозу не виявлено; нічний час або обмежена видимість	Режим 2	1–3 із передаванням даних до модуля 4	1–3	Застосування засобів виявлення, ефективність яких не залежить від природного освітлення
Надійшла інформація про підготовку нападу або оголошено повітряну тривогу	Режим 3	1–3 із передаванням даних до модуля 4	1–4	Залучення всіх наявних сил і засобів об’єкта
Власних сил і засобів недостатньо або виникла потреба в посиленні захисту	Режим 4	1–3 із передаванням даних до модуля 4	1–4	Поєднання власних і зовнішніх сил та засобів
Повітряну ціль ідентифіковано; інтенсивність нападу зростає	Режим 5	4–5	5	Нарощування протидії відповідно до зростання інтенсивності впливу
Інтенсивність нападу досягла максимального рівня та залишається незмінною	Режим 6	4–5	5	Зосередження засобів протидії на визначених напрямках
Об’єкт зазнав пошкоджень; загроза повторного нападу зберігається	Повторний вибір режиму з урахуванням стану системи	6–7 із поверненням до модулів 1–3	6–7	Ліквідація наслідків, відновлення готовності та уточнення подальшого режиму

Джерело: розроблено авторами.

Вибір одного з перших чотирьох режимів здійснюється третім модулем на підставі інформації про поточну обстановку, умови спостереження, готовність і достатність наявних сил та засобів.

Після виявлення та ідентифікації повітряної цілі здійснюється перехід до п’ятого або шостого режиму залежно від характеру зміни інтенсивності нападу. За умов неповної або суперечливої інформації обирається режим, який передбачає вищий рівень готовності системи захисту.

Між модулями передається інформація про характер загрози, стан об’єкта, склад і готовність сил та засобів, вибраний режим функціонування, параметри виявленої повітряної цілі, наслідки впливу та наявні ресурси.

Після ліквідації наслідків оновлена інформація через зворотні зв’язки надходить до модулів аналізу ситуації, поповнення сил і засобів та вибору режиму функціонування.

Практичне застосування інформаційно-технічного методу протидії загрозам національній безпеці України шляхом забезпечення захисту стратегічного об'єкта від засобів повітряного нападу передбачає послідовне виконання таких процедур:

1. Розподіл сил і засобів забезпечення безпеки об'єкта, що охороняється, відповідно до визначених завдань.
2. Організація системи зв'язку та управління між підрозділами забезпечення безпеки за різних умов обстановки на об'єкті, що охороняється, і прилеглій території.
3. Вибір варіанта застосування сил і засобів забезпечення безпеки під час повсякденного функціонування об'єкта.
4. Приведення об'єкта та системи його захисту в стан готовності до відбиття терористичного впливу.
5. Застосування сил і засобів для виявлення небезпеки та відбиття терористичного впливу.
6. Ліквідація наслідків терористичного впливу, зокрема локалізація небезпечних чинників, рятування людей, надання допомоги постраждалим та усунення першочергових пошкоджень.
7. Відновлення основних і допоміжних виробничих засобів об'єкта, сил і засобів забезпечення його безпеки та підготовка системи захисту до можливого повторного терористичного впливу.

Наукова новизна одержаних результатів полягає в подальшому розвитку науково-методичних засад побудови інформаційно-технічних методів захисту стратегічних об'єктів від засобів повітряного нападу шляхом інтеграції раніше розробленої математичної моделі функціонування системи безпеки в єдину структуру управління, що охоплює семимодульний керуючий алгоритм і сім процедур практичного застосування.

На відміну від попередніх досліджень, у яких основну увагу приділено математичному представленню режимів функціонування системи безпеки, у запропонованому методі визначено функціональні зв'язки між шістьма режимами математичної моделі, сімома модулями керуючого алгоритму та відповідними процедурами практичного застосування. Це забезпечує формалізоване представлення послідовності управлінських дій від аналізу обстановки, оцінювання наявних ресурсів і вибору режиму функціонування до застосування сил і засобів, ліквідації наслідків повітряного нападу та відновлення готовності системи захисту в умовах ресурсних обмежень.

Обговорення

Одержані результати свідчать про можливість комплексного представлення процесу захисту стратегічного об'єкта від засобів повітряного нападу шляхом поєднання математичного моделювання, алгоритмізації управлінських процесів і формалізації процедур практичного застосування сил та засобів. Запропонований інформаційно-технічний метод розглядає забезпечення безпеки не як сукупність окремих заходів виявлення та протидії, а як взаємопов'язаний процес, що охоплює оцінювання обстановки, вибір режиму функціонування, реагування на загрозу, ліквідацію наслідків і відновлення готовності системи захисту.

На відміну від досліджень [9–12], у яких основну увагу приділено взаємозалежності елементів критичної інфраструктури, оцінюванню її вразливості та операційної стійкості, у цій роботі акцент зроблено на організації управління системою захисту конкретного стратегічного об'єкта. Запропонований підхід дає змогу представити управлінський процес як послідовність взаємопов'язаних функціональних модулів із визначеними інформаційними зв'язками. Водночас розроблений метод не замінює моделі оцінювання вразливості та стійкості критичної інфраструктури, а може розглядатися як організаційно-методична основа для використання результатів такого оцінювання під час прийняття управлінських рішень.

Порівняння з оптимізаційними та теоретико-ігровими підходами [13, 14] засвідчує відмінність предметної спрямованості досліджень. Зазначені підходи орієнтовані переважно на визначення пріоритетів захисту та розподіл обмежених ресурсів з урахуванням можливих дій нападника. Натомість запропонований інформаційно-технічний метод передбачає узгодження використання наявних сил і засобів із поточним режимом функціонування системи безпеки. Це розширює можливості формалізованого опису управлінських процесів, однак не означає автоматичного досягнення оптимального розподілу ресурсів. Для підтвердження оптимальності відповідних рішень необхідно додатково визначити цільову функцію, систему обмежень і критерії оцінювання результативності захисних заходів.

Дослідження [15–20] зосереджені на архітектурі протидії безпілотним літальним апаратам, характеристиках технічних засобів виявлення, багатосенсорному моніторингу та особливостях функціонування систем спостереження за різних умов. Їх результати підтверджують доцільність комплексного використання технічно різнорідних засобів отримання інформації. У запропонованому методі ці засоби розглядаються як функціональні складові системи безпеки, інформація від яких використовується для оцінювання обстановки та вибору відповідного режиму функціонування. При цьому питання точності виявлення, імовірності хибних спрацювань, затримок передавання інформації та достовірності ідентифікації повітряних цілей потребують окремого кількісного дослідження.

Вітчизняні праці [21–25] розкривають можливості застосування радіолокаційних і відеоінформаційних засобів для виявлення потенційно небезпечних об’єктів. Їх результати можуть бути використані для визначення технічних характеристик окремих складових запропонованої системи захисту. Водночас предметом цього дослідження є не вдосконалення конкретного засобу виявлення, а формування узгодженої структури управління різнорідними силами та засобами залежно від характеру загрози й умов функціонування стратегічного об’єкта.

Найближчими за методологічною спрямованістю є дослідження [26, 27], у яких розглянуто алгоритмічні та організаційно-технічні підходи до моніторингу територій і запобігання надзвичайним ситуаціям. Спільною ознакою цих підходів і запропонованого методу є поєднання математичного представлення досліджуваних процесів з алгоритмами управління та процедурами практичного застосування. Відмінність полягає в орієнтації розробленого методу на функціонування системи захисту стратегічного об’єкта не лише у повсякденних умовах, а й безпосередньо під час повітряного нападу та після його завершення.

Особливе значення для одержаних результатів мають положення методу Пампуро [28] і математична модель забезпечення безпеки стратегічного об’єкта в умовах обмеженого фінансування [29]. Зазначена модель становить математичну основу запропонованого інформаційно-технічного методу. Тому науковий внесок цього дослідження доцільно пов’язувати насамперед не зі створенням принципово нової математичної моделі, а з її інтеграцією в структуру управління, що охоплює семимодульний керуючий алгоритм і сім процедур практичного застосування. Така інтерпретація дає змогу чіткіше розмежувати результати попередніх досліджень і положення, які набули подальшого розвитку в цій роботі.

Важливою особливістю запропонованого підходу є встановлення функціональних зв’язків між шістьма режимами математичної моделі, сімома модулями керуючого алгоритму та відповідними процедурами практичного застосування. Наявність прямих і зворотних інформаційних зв’язків створює передумови для циклічного управління системою захисту, за якого результати реагування на загрозу та ліквідації її наслідків використовуються для уточнення подальших управлінських рішень. Така організація управління має принципове значення в умовах зміни обстановки, обмеженості ресурсів і необхідності підтримання готовності до повторного повітряного нападу.

Водночас запропонований метод має низку обмежень. По-перше, його результати отримано на основі теоретичного аналізу, математичного моделювання та структурно-

функціонального представлення управлінських процесів. У межах дослідження не наведено результатів експериментальної перевірки або модельної апробації, які дали б змогу кількісно оцінити ефективність застосування методу. По-друге, потребують подальшого обґрунтування критерії переходу між режимами функціонування системи захисту, зокрема за умов неповної, суперечливої або несвоєчасної інформації. По-третє, необхідно врахувати вплив технічних відмов, втрати інформаційних зв'язків, обмеження пропускної здатності каналів передавання даних і зміни доступності сил та засобів.

Окремого дослідження потребує обґрунтованість використання експоненціального закону зростання інтенсивності повітряного нападу та сценарію збереження її максимального рівня протягом обмеженого часу. Ці припущення дають змогу математично описати визначені варіанти розвитку небезпечної події, однак не охоплюють усіх можливих сценаріїв застосування засобів повітряного нападу. Тому використання відповідних моделей під час практичного планування потребує перевірки їх адекватності конкретним умовам і характеру загроз.

Перспективним напрямом подальших досліджень є проведення імітаційного моделювання функціонування запропонованої системи захисту за різних сценаріїв повітряного нападу. Доцільно оцінити час виявлення загрози, тривалість прийняття управлінських рішень, повноту використання наявних ресурсів, час відновлення готовності системи та стійкість інформаційних зв'язків між її модулями. Порівняння зазначених показників із результатами функціонування системи без застосування запропонованого методу дозволило б визначити його практичну результативність і встановити умови, за яких його використання є доцільним.

Отже, результати дослідження свідчать про методологічну доцільність інтеграції математичної моделі, керуючого алгоритму та процедур практичного застосування в єдиний інформаційно-технічний метод захисту стратегічного об'єкта. Основне значення запропонованого підходу полягає у формалізації послідовності управлінських дій і функціональних взаємозв'язків між складовими системи безпеки. Водночас підтвердження його практичної ефективності потребує подальшої кількісної перевірки та апробації.

Висновки

У дослідженні обґрунтовано структуру та зміст інформаційно-технічного методу протидії загрозам національній безпеці України шляхом забезпечення захисту стратегічного об'єкта від засобів повітряного нападу.

1. Набули подальшого розвитку науково-методичні засади побудови інформаційно-технічного методу захисту стратегічного об'єкта шляхом інтеграції математичної моделі, керуючого алгоритму та процедур практичного застосування в єдину структуру управління. Запропонований метод призначений для забезпечення узгодженого використання сил і засобів захисту на етапах очікування, виявлення й відбиття повітряного нападу, ліквідації його наслідків і підготовки до можливого повторного впливу в умовах ресурсних обмежень.

2. Як математичну основу запропонованого інформаційно-технічного методу використано раніше розроблену модель функціонування системи захисту стратегічного об'єкта, яка складається з двох підсистем та описує шість режимів функціонування. Перша підсистема охоплює чотири режими повсякденного функціонування: використання чергових засобів у денний час; функціонування вночі та за умов обмеженої видимості; залучення всіх наявних засобів об'єкта; поєднання власних і зовнішніх сил та засобів. Друга підсистема описує два варіанти функціонування під час безпосереднього повітряного нападу: зростання інтенсивності впливу за експоненціальним законом і збереження її максимального рівня протягом обмеженого часу. Кожний режим представлено системою співвідношень, що включає частотну характеристику абстрактного чотириполюсника та характеристику, визначену за методом Пампуро.

3. Розроблено керуючий алгоритм, який складається із семи взаємопов'язаних модулів: аналізу ситуації; поповнення сил і засобів; вибору режиму функціонування; виявлення небезпеки; відбиття повітряного нападу; ліквідації наслідків; підготовки до повторного впливу. Визначено прямі інформаційні зв'язки між послідовними модулями та зворотні зв'язки від завершального модуля до модулів аналізу ситуації, поповнення сил і засобів та вибору режиму функціонування. Така структура створює передумови для циклічного управління системою захисту з урахуванням змін обстановки та наявності ресурсів.

4. Сформовано сім процедур практичного застосування інформаційно-технічного методу, які охоплюють розподіл сил і засобів відповідно до визначених завдань; організацію зв'язку та управління; вибір режиму повсякденного функціонування; приведення системи захисту в стан готовності; виявлення небезпеки та відбиття повітряного нападу; ліквідацію його наслідків; відновлення сил і засобів та підготовку до можливого повторного впливу. Визначено функціональну відповідність між режимами математичної моделі, модулями керуючого алгоритму та процедурами практичного застосування.

5. Встановлено, що запропонований інформаційно-технічний метод забезпечує формалізоване представлення процесу управління системою захисту стратегічного об'єкта, однак його практична результативність потребує подальшого підтвердження. Перспективним напрямом досліджень є проведення імітаційного моделювання за різних сценаріїв повітряного нападу з оцінюванням часу виявлення загрози, тривалості прийняття управлінських рішень, повноти використання ресурсів, стійкості інформаційних зв'язків і часу відновлення готовності системи захисту.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Використання штучного інтелекту

Автори заявляють, що не мають конфлікту інтересів щодо даного дослідження, у тому числі, фінансових, особистих, авторських або будь-якого іншого характеру, які б могли вплинути на дане дослідження та його результати.

Список використаних джерел

1. Азаренко Е. В., Гончаренко Ю. Ю., Дивизинюк М. М., Ожиганова М. И. Защита критической инфраструктуры государства от террористического воздействия : монография. Киев : ИГНС НАН Украины, 2018. 84 с. ISBN 978-617-7187-25-6.
2. Дівізінюк М. М., Єременко С. А., Лєфтєров О. А., Пруський А. В., Стрілець В. В., Стрілець В. М., Шевченко Р. І. Теоретичні засади парадигми «цивільний захист» : монографія. Київ : ТОВ «АЗИМУТ-ПРІНТ», 2022. 335 с. ISBN 978-617-8015-20-6.
3. Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання : Закон України від 19.10.2000 № 2064-III. Відомості Верховної Ради України. 2001. № 1. Ст. 1. URL: https://zakon.rada.gov.ua/laws/show/2064-14 (дата звернення: 02.08.2026).
4. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. Відомості Верховної Ради України. 2023. № 5. Ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 02.08.2026).

5. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : редакція від 24.01.2026, підстава — 4603-IX. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 02.08.2026).
6. Рашкевич Н. В. Аналіз сучасного стану попередження надзвичайних ситуацій на територіях України, які зазнали ракетно-артилерійських уражень. Комунальне господарство міст. 2023. Т. 4, вип. 178. С. 232–251. DOI: https://doi.org/10.33042/2522-1809-2023-4-178-232-251.
7. Азаренко О., Дівізінюк М., Шевченко О., Рашкевич Н., Гузь А., Олефіренко О. Хронологія терористичних атак по території України ударними дронами в січні 2025 року. Social Development and Security. 2025. Vol. 15, No. 6. P. 175–189. DOI: https://doi.org/10.33445/sds.2025.15.6.17.
8. Solodov A., Williams A. D., Al Hanaei S., Goddard B. Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities. Security Journal. 2018. Vol. 31, No. 1. P. 305–324. DOI: https://doi.org/10.1057/s41284-017-0102-5.
9. Rinaldi S. M., Peerenboom J. P., Kelly T. K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine. 2001. Vol. 21, No. 6. P. 11–25. DOI: https://doi.org/10.1109/37.969131.
10. Ouyang M. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. Reliability Engineering & System Safety. 2014. Vol. 121. P. 43–60. DOI: https://doi.org/10.1016/j.ress.2013.06.040.
11. Zio E. Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures. Reliability Engineering & System Safety. 2016. Vol. 152. P. 137–150. DOI: https://doi.org/10.1016/j.ress.2016.02.009.
12. Alderson D. L., Brown G. G., Carlyle W. M. Operational Models of Infrastructure Resilience. Risk Analysis. 2015. Vol. 35, No. 4. P. 562–586. DOI: https://doi.org/10.1111/risa.12333.
13. Brown G., Carlyle M., Salmerón J., Wood K. Defending Critical Infrastructure. Interfaces. 2006. Vol. 36, No. 6. P. 530–544. DOI: https://doi.org/10.1287/inte.1060.0252.
14. Wu M., Amin S. Securing Infrastructure Facilities: When Does Proactive Defense Help? Dynamic Games and Applications. 2019. Vol. 9. P. 984–1025. DOI: https://doi.org/10.1007/s13235-018-0280-8.
15. Islam M. S., Ahmed M. M., Islam S. A Conceptual System Architecture for Countering the Civilian Unmanned Aerial Vehicles Threat to Nuclear Facilities. International Journal of Critical Infrastructure Protection. 2018. Vol. 23. P. 139–149. DOI: https://doi.org/10.1016/j.ijcip.2018.10.003.
16. Lykou G., Moustakas D., Gritzalis D. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. Sensors. 2020. Vol. 20, No. 12. Art. 3537. DOI: https://doi.org/10.3390/s20123537.
17. Seidaliyeva U., Ilipbayeva L., Taissariyeva K., Smailov N., Matson E. T. Advances and Challenges in Drone Detection and Classification Techniques: A State-of-the-Art Review. Sensors. 2024. Vol. 24, No. 1. Art. 125. DOI: https://doi.org/10.3390/s24010125.
18. Samaras S., Diamantidou E., Ataloglou D., Sakellariou N., Vafeiadis A., Magoulianitis V., Lalas A., Dimou A., Zarpalas D., Daras P., Votis K., Tzovaras D. Deep Learning on Multi-Sensor Data for Counter-UAV Applications – A Systematic Review. Sensors. 2019. Vol. 19, No. 22. Art. 4837. DOI: https://doi.org/10.3390/s19224837.
19. Besada J. A., Campaña I., Carramiñana D., Bergesio L., de Miguel G. Review and Simulation of Counter-UAS Sensors for Unmanned Traffic Management. Sensors. 2022. Vol. 22, No. 1. Art. 189. DOI: https://doi.org/10.3390/s22010189.

20. Yan X., Fu T., Lin H., Xuan F., Huang Y., Cao Y., Hu H., Liu P. UAV Detection and Tracking in Urban Environments Using Passive Sensors: A Survey. Applied Sciences. 2023. Vol. 13, No. 20. Art. 11320. DOI: https://doi.org/10.3390/app132011320.
21. Diviziniuk M., Kamyshentsev H., Yeremenko S., Riabokon Y., Artemchuk V., Andreitsev V. Energy Potential Components of Radar Station that Ensure Security of Protected Objects of Critical Infrastructure of Ukraine. Systems, Decision and Control in Energy VII / eds. V. Babak, A. Zaporozhets. Studies in Systems, Decision and Control. Cham : Springer, 2025. Vol. 596. P. 153–162. DOI: https://doi.org/10.1007/978-3-031-90462-2_8.
22. Azarenko O. V., Divizinyuk M. M., Farrakhov O. V., Levterov O. A., Lukashenko V. V., Shevchenko R. I., Shevchenko O. S. Information and Technical Methods of Physical Protection of Critical Infrastructure Facilities Using External Video Surveillance Systems : monograph. Kyiv : FOP Yamchynskyi, 2025. 114 p. ISBN 978-617-8718-84-4.
23. Азаренко О. В., Гончаренко Ю. Ю., Дівізінюк М. М., Камишенцев Г. В., Лукашенко В. В. Інформаційно-технічні методи забезпечення державної безпеки України. Частина 2. З використанням відеосистем зовнішнього спостереження : монографія. Київ : ДУ «ІГНС НАН України», 2023. 128 с. ISBN 978-617-7187-78-2.
24. Азаренко Е. В., Гончаренко Ю. Ю., Дивизинюк М. М., Лазаренко С. В., Ожиганова М. И. Информационно-технические методы предотвращения чрезвычайных ситуаций террористического характера на объектах критической инфраструктуры. Часть 1. С использованием активных импульсных радиолокационных средств : монография. Киев : ИГНС НАН Украины, 2019. 164 с. ISBN 978-617-7187-33-1.
25. Azarenko O. V., Divizinyuk M. M., Levterov O. A., Lukashenko V. V., Shevchenko R. I., Shevchenko O. S., Farrakhov O. V. Information and Technology Methods for Preventing Terrorist Emergencies at Critical Infrastructure Facilities Using Active Pulse Radar Systems : monograph. Kyiv : 7БЦ, 2025. 155 p. ISBN 978-617-8794-19-4.
26. Рашкевич Н. В., Шевченко Р. І., Нешпор О. В. Формування алгоритму інформаційно-технічного методу попередження надзвичайної ситуації на територіях, що зазнали ракетно-артилерійських уражень. Комунальне господарство міст. 2024. Т. 3, вип. 184. С. 223–228. DOI: https://doi.org/10.33042/2522-1809-2024-3-184-223-228.
27. Rashkevich N., Shevchenko R., Yeremenko S. Development of an Organizational and Technical Method of Emergency Prevention of Technological Character on the Territory Which Was Attacked by Rocket and Artillery Impacts. Systems, Decision and Control in Energy VII. Volume II: Power Engineering and Environmental Safety / eds. V. Babak, A. Zaporozhets. Studies in Systems, Decision and Control. Cham : Springer, 2025. Vol. 595. P. 717–747. DOI: https://doi.org/10.1007/978-3-031-90466-0_33.
28. Азаренко О. В., Гвоздь В. М., Гончаренко Ю. Ю., Дівізінюк М. М., Фаррахов О. В., Сівоха І. М. Метод побудови систем управління аналоговими об’єктами (метод Пампуро). Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realtà domestiche : Raccolta di articoli scientifici «ΛΌΓΟΣ» con gli atti della IV Conferenza scientifica e pratica internazionale, Bologna, 29 settembre 2023. Bologna–Vinnytsia : Associazione Italiana di Storia Urbana & Piattaforma scientifica europea, 2023. P. 95–98. DOI: https://doi.org/10.36074/logos-29.09.2023.25.
29. Азаренко О. В., Гвоздь В. М., Гончаренко Ю. Ю., Дівізінюк М. М., Мирошник О. М., Фаррахов О. В. Математична модель забезпечення найбільшої безпеки стратегічного об’єкта, що охороняється, при ліміті виділених коштів. Scientific Collection «InterConf+». 2023. № 38 (175). С. 417–435. DOI: https://doi.org/10.51582/interconf.19-20.10.2023.037.

References

1. Azarenko, E. V., Goncharenko, Yu. Yu., Divizinyuk, M. M., & Ozhiganova, M. I. (2018). Zashchita kriticheskoi infrastruktury gosudarstva ot terroristicheskogo vozdeistviia [Protection of the state's critical infrastructure from terrorist impact]. IGNS NAN Ukrainy.
2. Diviziniuk, M. M., Yeremenko, S. A., Lieftierov, O. A., Pruskyi, A. V., Strilets, V. V., Strilets, V. M., & Shevchenko, R. I. (2022). Teoretychni zasady paradyhmy «tsyvilnyi zakhyst» [Theoretical foundations of the "civil protection" paradigm]. AZYMUT-PRINT.
3. Verkhovna Rada Ukrainy. (2000). Pro fizychnyi zakhyst yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia [On the physical protection of nuclear installations, nuclear materials, radioactive waste and other sources of ionizing radiation] (Law No. 2064-III). https://zakon.rada.gov.ua/laws/show/2064-14
4. Verkhovna Rada Ukrainy. (2021). Pro krytychnu infrastrukturu [On critical infrastructure] (Law No. 1882-IX). https://zakon.rada.gov.ua/laws/show/1882-20
5. Verkhovna Rada Ukrainy. (2018). Pro natsionalnu bezpeku Ukrainy [On the national security of Ukraine] (Law No. 2469-VIII, as amended). https://zakon.rada.gov.ua/laws/show/2469-19#Text
6. Rashkevich, N. V. (2023). Analiz suchasnoho stanu poperedzhennia nadzvychainykh sytuatsii na terytoriiakh Ukrainy, yaki zaznaly raketno-artyleriiskykh urazhen [Analysis of the current state of emergency prevention in the territories of Ukraine affected by rocket and artillery strikes]. Komunalne hospodarstvo mist, 4(178), 232–251. https://doi.org/10.33042/2522-1809-2023-4-178-232-251
7. Azarenko, O., Diviziniuk, M., Shevchenko, O., Rashkevich, N., Huz, A., & Olefirenko, O. (2025). Khronolohiia terorystychnykh atak po terytorii Ukrainy udarnymy dronamy v sichni 2025 roku [Chronology of terrorist attacks on the territory of Ukraine by strike drones in January 2025]. Social Development and Security, 15(6), 175–189. https://doi.org/10.33445/sds.2025.15.6.17
8. Solodov, A., Williams, A. D., Al Hanaei, S., & Goddard, B. (2018). Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities. Security Journal, 31(1), 305–324. https://doi.org/10.1057/s41284-017-0102-5
9. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11–25. https://doi.org/10.1109/37.969131
10. Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety, 121, 43–60. https://doi.org/10.1016/j.ress.2013.06.040
11. Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, 137–150. https://doi.org/10.1016/j.ress.2016.02.009
12. Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015). Operational models of infrastructure resilience. Risk Analysis, 35(4), 562–586. https://doi.org/10.1111/risa.12333
13. Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. Interfaces, 36(6), 530–544. https://doi.org/10.1287/inte.1060.0252
14. Wu, M., & Amin, S. (2019). Securing infrastructure facilities: When does proactive defense help? Dynamic Games and Applications, 9, 984–1025. https://doi.org/10.1007/s13235-018-0280-8
15. Islam, M. S., Ahmed, M. M., & Islam, S. (2018). A conceptual system architecture for countering the civilian unmanned aerial vehicles threat to nuclear facilities. International Journal of Critical Infrastructure Protection, 23, 139–149. https://doi.org/10.1016/j.ijcip.2018.10.003

16. Lykou, G., Moustakas, D., & Gritzalis, D. (2020). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. Sensors, 20(12), Article 3537. https://doi.org/10.3390/s20123537
17. Seidaliyeva, U., Ilipbayeva, L., Taissariyeva, K., Smailov, N., & Matson, E. T. (2024). Advances and challenges in drone detection and classification techniques: A state-of-the-art review. Sensors, 24(1), Article 125. https://doi.org/10.3390/s24010125
18. Samaras, S., Diamantidou, E., Ataloglou, D., Sakellariou, N., Vafeiadis, A., Magoulianitis, V., Lalas, A., Dimou, A., Zarpalas, D., Daras, P., Votis, K., & Tzovaras, D. (2019). Deep learning on multi-sensor data for counter-UAV applications – A systematic review. Sensors, 19(22), Article 4837. https://doi.org/10.3390/s19224837
19. Besada, J. A., Campaña, I., Carramiñana, D., Bergesio, L., & de Miguel, G. (2022). Review and simulation of counter-UAS sensors for unmanned traffic management. Sensors, 22(1), Article 189. https://doi.org/10.3390/s22010189
20. Yan, X., Fu, T., Lin, H., Xuan, F., Huang, Y., Cao, Y., Hu, H., & Liu, P. (2023). UAV detection and tracking in urban environments using passive sensors: A survey. Applied Sciences, 13(20), Article 11320. https://doi.org/10.3390/app132011320
21. Diviziniuk, M., Kamyshentsev, H., Yeremenko, S., Riabokon, Y., Artemchuk, V., & Andreitsev, V. (2025). Energy potential components of radar station that ensure security of protected objects of critical infrastructure of Ukraine. In V. Babak & A. Zaporozhets (Eds.), Systems, decision and control in energy VII (Studies in Systems, Decision and Control, Vol. 596, pp. 153–162). Springer. https://doi.org/10.1007/978-3-031-90462-2_8
22. Azarenko, O. V., Divizinyuk, M. M., Farrakhov, O. V., Levterov, O. A., Lukashenko, V. V., Shevchenko, R. I., & Shevchenko, O. S. (2025). Information and technical methods of physical protection of critical infrastructure facilities using external video surveillance systems. FOP Yamchynskyi.
23. Azarenko, O. V., Goncharenko, Yu. Yu., Diviziniuk, M. M., Kamyshentsev, H. V., & Lukashenko, V. V. (2023). Informatsiino-tekhnichni metody zabezpechennia derzhavnoi bezpeky Ukrainy. Chastyna 2. Z vykorystanniam videosystem zovnishnoho sposterezhennia [Information and technical methods for ensuring the state security of Ukraine. Part 2. Using external video surveillance systems]. DU «IHNS NAN Ukrainy».
24. Azarenko, E. V., Goncharenko, Yu. Yu., Divizinyuk, M. M., Lazarenko, S. V., & Ozhiganova, M. I. (2019). Informatsionno-tekhnicheskie metody predotvrashcheniia chrezvychainykh situatsii terroristicheskogo kharaktera na obektakh kriticheskoi infrastruktury. Chast 1. S ispolzovaniem aktivnykh impulsnykh radiolokatsionnykh sredstv [Information and technical methods for preventing terrorist emergencies at critical infrastructure facilities. Part 1. Using active pulse radar systems]. IGNS NAN Ukrainy.
25. Azarenko, O. V., Divizinyuk, M. M., Levterov, O. A., Lukashenko, V. V., Shevchenko, R. I., Shevchenko, O. S., & Farrakhov, O. V. (2025). Information and technology methods for preventing terrorist emergencies at critical infrastructure facilities using active pulse radar systems. 7BTs.
26. Rashkevich, N. V., Shevchenko, R. I., & Neshpor, O. V. (2024). Formuvannia alhorytmu informatsiino-tekhnichnoho metodu poperedzhennia nadzvychainoi sytuatsii na terytoriiakh, shcho zaznaly raketno-artyleriiskykh urazhen [Formation of an algorithm for an information and technical method of emergency prevention in territories affected by rocket and artillery strikes]. Komunalne hospodarstvo mist, 3(184), 223–228. https://doi.org/10.33042/2522-1809-2024-3-184-223-228
27. Rashkevich, N., Shevchenko, R., & Yeremenko, S. (2025). Development of an organizational and technical method of emergency prevention of technological character on the territory which was attacked by rocket and artillery impacts. In V. Babak & A. Zaporozhets (Eds.), Systems,

decision and control in energy VII: Vol. II. Power engineering and environmental safety (Studies in Systems, Decision and Control, Vol. 595, pp. 717–747). Springer. https://doi.org/10.1007/978-3-031-90466-0_33

28. Azarenko, O. V., Hvozd, V. M., Goncharenko, Yu. Yu., Diviziniuk, M. M., Farrakhov, O. V., & Sivokha, I. M. (2023). Metod pobudovy system upravlinnia analohovymy obiektamy (metod Pampuro) [A method for constructing control systems for analog objects (the Pampuro method)]. In Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realtà domestiche: Raccolta di articoli scientifici «ΛΌΓΟΣ» con gli atti della IV Conferenza scientifica e pratica internazionale (pp. 95–98). Associazione Italiana di Storia Urbana & Piattaforma scientifica europea. https://doi.org/10.36074/logos-29.09.2023.25
29. Azarenko, O. V., Hvozd, V. M., Goncharenko, Yu. Yu., Diviziniuk, M. M., Myroshnyk, O. M., & Farrakhov, O. V. (2023). Matematychna model zabezpechennia naibilshoi bezpeky stratehichnoho obiekta, shcho okhoroniaietsia, pry limiti vydilenykh koshtiv [A mathematical model for ensuring the maximum security of a protected strategic facility under a limited budget]. Scientific Collection «InterConf+», 38(175), 417–435. https://doi.org/10.51582/interconf.19-20.10.2023.037

This is an open access journal and all published articles are licensed under a Creative Commons «Attribution» 4.0.