Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Міністерство освіти і науки України

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

БОРЗЕНКОВ ВЛАДИСЛАВ ВАЛЕРІЙОВИЧ

УДК 621.039

ДИСЕРТАЦІЯ

РОЗРОБКА МЕТОДОЛОГІЇ ОЦІНКИ ВРАЗЛИВОСТІ ЯДЕРНОЇ УСТАНОВКИ В УМОВАХ ВІЙНИ

Спеціальність 143 – Атомна енергетика
Галузь знань 14 – Електрична інженерія

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____В. В. БОРЗЕНКОВ

Науковий керівник – **БІБІК Тимофій Вікторович**, кандидат технічних наук, доцент кафедри АЕ

Київ – 2026

АНОТАЦІЯ

Борзенков В. В. Розробка методології оцінки вразливості ядерної установки в умовах війни. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 143 «Атомна енергетика» (галузь знань 14 «Електрична інженерія»). – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, 2026.

Загальна характеристика роботи

Актуальність теми. Забезпечення фізичного захисту (ФЗ) ядерних установок (ЯУ) традиційно базувалося на «парадигмі мирного часу», закріпленій у рекомендаціях МАГАТЕ (зокрема INFCIRC/225/Rev.5). Проте повномасштабна військова агресія проти України та окупація Запорізької АЕС виявили фундаментальну невідповідність міжнародних стандартів реаліям сучасної війни. Сучасні конфлікти характеризуються застосуванням високоточної зброї, засобів радіоелектронної боротьби (РЕБ) та масованим використанням безпілотних літальних апаратів (БпЛА).

Традиційні моделі оцінки вразливості не враховують загрози державного рівня, можливість втрати операційного контролю над об’єктом та цілеспрямоване руйнування систем зовнішнього життєзабезпечення (зовнішнього енергоживлення). Це зумовлює гостру необхідність розробки нової методології оцінки вразливості, яка б дозволяла кількісно визначати рівень захищеності ЯУ в умовах активних бойових дій та деградації державного регулювання.

Зв’язок роботи з науковими програмами. Дослідження виконано в межах науково-дослідних робіт кафедри атомної енергетики НТУУ «КПІ ім. Ігоря Сікорського», спрямованих на підвищення стійкості об’єктів критичної інфраструктури України.

Мета дослідження – розроблення науково обґрунтованих підходів до вдосконалення системи фізичного захисту (СФЗ) ядерних установок України з урахуванням ризиків воєнного часу, зокрема загроз повітряного характеру та руйнування систем зовнішнього життєзабезпечення.

Об'єкт дослідження – система фізичного захисту ядерних установок в умовах воєнних загроз.

Предмет дослідження – методи та моделі оцінки вразливості ЯУ до сучасних воєнних загроз із застосуванням імовірнісних методів аналізу ризику.

Методи дослідження. У роботі використано: системний аналіз нормативно-правової бази; методи імовірнісного аналізу ризику (PSA); математичне моделювання процесів виявлення та нейтралізації повітряних цілей; концепцію «глибокого ешелонування» в нових умовах.

Наукова новизна отриманих результатів

- **Вперше розроблено інтегровану методологію оцінки вразливості ЯУ**, яка поєднує класичні детерміновані сценарії з імовірнісними моделями ризику, що **дозволяє** кількісно оцінювати захищеність об'єкта в динамічних умовах війни.
- **Вперше запропоновано модель «ешелонованої проєктної загрози»**, яка включає параметри виявлення малорозмірних повітряних цілей (БпЛА) та ефективність засобів радіоелектронної боротьби (РЕБ).
- **Удосконалено методологію імовірнісного аналізу ризику (PSA**) через введення коефіцієнта динамічної вразливості, що залежить від стану зовнішньої енергомережі та працездатності систем РЕБ.
- **Дістали подальшого розвитку підходи до ешелонування захисту,** де до традиційних зон обмеження доступу додано зони раннього попередження (5–10 км) та зони некінетичного впливу.

Основний зміст роботи

Розділ 1. Криза класичної парадигми фізичного захисту ЯУ в умовах війни.

У розділі проведено деконструкцію «мирної парадигми». Доведено, що міжнародні конвенції та рекомендації МАГАТЕ (NSS No. 13, No. 20) створюють

юридичний вакуум у ситуаціях окупації, оскільки покладають відповідальність виключно на державу-оператора, не враховуючи втрату нею фактичного контролю.

Критика моделі SNL: Фундаментальна тріада «Виявлення-Затримка-Реагування» (D-D-R) колапсує, коли противник використовує артилерію або БпЛА, які миттєво долають фізичний периметр.

Правовий аналіз: Виявлено «організаційний параліч» у чинних Правилах ФЗ (Наказ ДІЯРУ № 116), які не містять протоколів дій у разі руйнування периметра бойовими діями або дискредитації пропускного режиму силами агресора.

Концептуальна прогалина: Встановлено, що класичний підхід МАГАТЕ розмежовує «nuclear security» та «national security», що робить цивільні ЯУ беззахисними перед державними воєнними загрозами.

Розділ 2. Оцінка сучасних воєнних загроз для об’єктів атомної енергетики.

На основі аналізу подій на Чорнобильській та Запорізькій АЕС (2022-2024 рр.) ідентифіковано критичні вектори атак.

Кейс ЗАЕС: Описано інверсію системи фізичного захисту, коли засоби ФЗ використовуються окупаційними силами для утримання об’єкта, а не для його захисту.

Загроза «Blackout»: Обґрунтовано, що пріоритетною метою ворога є не руйнування реакторного відділення (захищеного контайнментом), а знищення відкритих розподільчих пристроїв (ВРП) та ліній зв’язку, що призводить до зупинки систем охолодження.

БпЛА як основний інструмент: Проаналізовано типи дронів (камікадзе, розвідувальні) та їх здатність обходити традиційні системи РЛС через малу ЕПР та низьку висоту польоту.

Розділ 3. Методологія кількісної оцінки вразливості від повітряних атак.

У цьому розділі представлено головний науковий результат - розширену математичну модель ризику R:

$$R = P_{succ}\, C,$$

де P_{succ} – ймовірність успішної атаки, C – величина наслідків.

- **Параметр виявлення (P_{total_D}):** Розроблено модель кумулятивної ймовірності виявлення, яка базується на поєднанні даних від РЛС та акустичних датчиків. Доведено, що для БпЛА типу «Shahed» або «FPV» ефективність лише радіолокаційних засобів не перевищує 40–50%, що потребує впровадження мультисенсорних систем.
- **Енергетична стійкість:** Введено розрахунок кінетичної енергії удару БпЛА (E_k). Проведено порівняльний аналіз здатності бетонних укриттів витримувати детонацію бойової частини вагою 5–50 кг.
- **Кейс-стаді:** На прикладі автотрансформатора АЕС показано, що встановлення антидронових сіток та засобів локальної РЕБ знижує ймовірність критичного пошкодження з 0,85 до 0,12.

Розділ 4. Висновки та пропозиції щодо вдосконалення нормативної бази.

Сформовано конкретний пакет законодавчих ініціатив:

- **Закон № 2064-IV**: Пропонується розширити визначення «проєктної загрози», включивши до неї засоби повітряного нападу державного рівня.
- **Постанови КМУ (№ 1337, № 625, № 327)**: Обґрунтовано необхідність коригування порядків функціонування державної системи ФЗ для інтеграції засобів РЕБ та ППО.
- **Накази ДІЯРУ (№ 169, № 176, № 179)**: Запропоновано перехід від якісних експертних оцінок вразливості до кількісних імовірнісних моделей, описаних у Розділі 3.

- Економічний ефект: Доведено, що кількісна методика дозволяє оптимізувати витрати на СФЗ, вибираючи конфігурацію засобів із максимальним показником P_{total} при мінімально необхідних ресурсах.

Висновки

Результати дослідження дозволяють вирішити важливу наукову задачу - створення теоретичного та інструментального базису для захисту об'єктів атомної енергетики в умовах сучасної війни. Впровадження запропонованої методології забезпечить:

- Адаптацію систем фізичного захисту до атак БпЛА та засобів повітряного нападу.
- Можливість кількісного обґрунтування інвестицій у засоби РЕБ та ППО для потреб АЕС.
- Підвищення живучості критичної інфраструктури в умовах втрати зовнішнього енергопостачання та деградації логістичних ланцюгів.

Практичне значення роботи підтверджується можливістю використання її результатів органами державного регулювання, експлуатуючими організаціями та військовими підрозділами, що здійснюють охорону ЯУ.

Ключові слова: комплекс інженерно-технічних засобів, ядерна безпека, активна зона, фізичний захист, ядерна установка, ядерний реактор, воєнні загрози, безпілотні літальні апарати, безпека АЕС, АЕС, ударні хвилі, імовірнісний аналіз ризику, проєктна загроза, система фізичного захисту, кваліфікація.

ABSTRACT

Borzenkov V. V. Development of a Methodology for Assessing the Vulnerability of a Nuclear Installation under Wartime Conditions. – Qualifying scientific work on the rights of a manuscript.

Dissertation for the degree of Doctor of Philosophy (PhD) in Specialty 143 "Nuclear Power Engineering" (Field of Study 14 "Electrical Engineering"). – National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, 2025.

General Characteristics of the Work

Relevance of the Topic. The provision of physical protection (PP) for nuclear installations (NIs) has traditionally been based on the "peacetime paradigm" enshrined in IAEA recommendations (specifically INFCIRC/225/Rev.5). However, the full-scale military aggression against Ukraine and the occupation of the Zaporizhzhia NPP have revealed a fundamental discrepancy between international standards and the realities of modern warfare. Contemporary conflicts are characterized by the use of high-precision weapons, electronic warfare (EW) tools, and the mass deployment of unmanned aerial vehicles (UAVs).

Traditional vulnerability assessment models do not account for state-level threats, the possibility of losing operational control over the facility, or the targeted destruction of external life-support systems (external power supply). This necessitates the development of a new vulnerability assessment methodology capable of quantifying the security level of an NI under active combat operations and the degradation of state regulation.

Connection of the Work with Scientific Programs. The research was conducted within the framework of scientific research projects of the Department of Nuclear Power Engineering at NTUU "Igor Sikorsky KPI," aimed at increasing the resilience of Ukraine's critical infrastructure.

Research Objective is to develop scientifically grounded approaches to improving the physical protection system (PPS) of nuclear installations in Ukraine, considering wartime risks, particularly aerial threats and the destruction of external support systems.

Research Object is the physical protection system of nuclear installations under military threats.

Research Subject consists of methods and models for assessing the vulnerability of NIs to modern military threats using probabilistic risk analysis methods.

Research Methods. The study utilizes: systemic analysis of the regulatory and legal framework; probabilistic safety/risk assessment (PSA/PRA) methods; mathematical modeling of aerial target detection and neutralization processes; and the concept of "defense-in-depth" in new environments.

Scientific Novelty of the Results

- **For the first time, an integrated methodology for NI vulnerability assessment has been developed**, combining classical deterministic scenarios with probabilistic risk models, allowing for a quantitative evaluation of facility security in dynamic wartime conditions.
- **For the first time, a "layered design basis threat" model is proposed**, which includes parameters for detecting small-sized aerial targets (UAVs) and the effectiveness of electronic warfare (EW) assets.
- **The probabilistic risk analysis (PSA) methodology has been improved** by introducing a dynamic vulnerability coefficient that depends on the state of the external power grid and the operability of EW systems.
- **Approaches to layered defense have been further developed**, adding early warning zones (5–10 km) and non-kinetic impact zones to traditional access-restricted areas.

Main Content of the Work

Section 1. Crisis of the Classical Paradigm of NI Physical Protection under Wartime Conditions.

This section deconstructs the "peacetime paradigm." It is proven that international conventions and IAEA recommendations (NSS No. 13, No. 20) create a legal vacuum in occupation scenarios, as they place responsibility solely on the operator state without accounting for its loss of actual control.

- **Critique of the SNL Model:** The fundamental "Detection-Delay-Response" (D-D-R) triad collapses when the adversary utilizes artillery or UAVs that bypass the physical perimeter instantaneously.
- **Legal Analysis:** "Organizational paralysis" is identified in current PP Rules (SNRIU Order No. 116), which lack protocols for actions in the event of perimeter destruction by combat operations or the discredit of access control by aggressor forces.
- **Conceptual Gap:** It is established that the classical IAEA approach separates "nuclear security" from "national security," leaving civilian NIs defenseless against state military threats.

Section 2. Assessment of Modern Military Threats to Nuclear Power Facilities.

Based on the analysis of events at the Chornobyl and Zaporizhzhia NPPs (2022–2024), critical attack vectors are identified.

- **Zaporizhzhia NPP Case:** Describes the inversion of the physical protection system, where PP assets are used by occupying forces to hold the facility rather than protect it.
- **"Blackout" Threat:** It is substantiated that the enemy's priority is not the destruction of the reactor building (protected by containment) but the destruction of outdoor switchgear (OSG) and communication lines, leading to the failure of cooling systems.

- **UAVs as a Primary Tool:** Analyzes types of drones (kamikaze, reconnaissance) and their ability to bypass traditional radar systems due to low radar cross-section (RCS) and low-altitude flight.

Section 3. Methodology for Quantitative Vulnerability Assessment against Aerial Attacks.

This section presents the primary scientific result- an expanded mathematical risk model R:

$$R = P_{succ}\, C,$$

where P_{succ} is the probability of a successful attack and C is the magnitude of consequences.

- **Detection Parameter (P_{total_D}):** A cumulative detection probability model has been developed based on the fusion of data from radar and acoustic sensors. It is proven that for UAVs like "Shahed" or "FPV," the efficiency of radar alone does not exceed 40–50%, requiring the implementation of multi-sensor systems.

- **Energy Resilience:** A calculation of the kinetic energy of a UAV impact (E_k) is introduced. A comparative analysis of the ability of concrete shelters to withstand the detonation of warheads weighing 5–50 kg was conducted.

- **Case Study:** Using the example of an NPP autotransformer, it is shown that the installation of anti-drone nets and local EW assets reduces the probability of critical damage from 0.85 to 0.12.

Section 4. Conclusions and Proposals for Improving the Regulatory Framework.

A specific package of legislative initiatives has been formed:

- **Law No. 2064-IV:** It is proposed to expand the definition of "Design Basis Threat" (DBT) to include state-level aerial attack assets.

- **CMU Resolutions (No. 1337, No. 625, No. 327):** The need to adjust the operational procedures of the state PP system to integrate EW and Air Defense assets is justified.

- **SNRIU Orders (No. 169, No. 176, No. 179):** A transition from qualitative expert vulnerability assessments to the quantitative probabilistic models described in Section 3 is proposed.
- **Economic Effect:** It is proven that the quantitative methodology allows for the optimization of PPS costs by selecting the configuration of assets with the maximum P_{total} using minimum necessary resources.

Conclusions

The research results allow for the resolution of a significant scientific task - the creation of a theoretical and instrumental basis for the protection of nuclear power facilities under modern warfare conditions. The implementation of the proposed methodology will ensure:

- Adaptation of physical protection systems to UAV attacks and aerial assault assets.
- The possibility of quantitative justification for investments in EW and Air Defense assets for NPP needs.
- Increased survivability of critical infrastructure under conditions of external power loss and degradation of logistic chains.

The practical significance of the work is confirmed by the possibility of using its results by state regulatory bodies, operating organizations, and military units performing NI security duties.

Keywords: complex of engineering and technical means, nuclear safety, core area, physical protection, nuclear facility, nuclear reactor, military threats, unmanned aerial vehicles, nuclear power plant safety, nuclear power plant, shock waves, probabilistic risk analysis, design threat, physical protection system, qualification.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті з представленими науковими результатами дисертації:

1. Т.В. Бібік, В.В. Борзенков, І.А. Остапенко. / Захищеність ядерних установок та збройні конфлікти. Уроки України. Т.В. Бібік, В.В. Борзенков, І.А. Остапенко.// Ядерна та радіаційна безпека, №1(105) 62-69, 2025, https://doi.org/10.32918/nrs.2025.1(105).07 (Категорія А Scopus Q3), ISSN 2073-6231. Особистий внесок співавторів: Бібік Т.В. - визначив загальний науковий напрям дослідження та надавав методичне керівництво, здійснював наукове редагування статті, сформулював основну наукову ідею дослідження; Борзенков В.В. - розробив аналіз сучасних воєнних загроз для ядерних установок, склав узагальнення досвіду функціонування АЕС України в умовах війни, зробив обґрунтування концепції «живучості ядерної установки», розробив інтерпретацію отриманих результатів та формування висновків; Остапенко І.А. – брав участь у постановці задачі та уточненні концептуальних положень роботи, зробив наукове редагування статті (коригування структури роботи та уточнення формулювань наукових результатів), провів експертну оцінку отриманих результатів і їх відповідності сучасному рівню розвитку науки; приймав участь у доопрацюванні висновків. (у співавторстві).

2. T. Bibik, V. Borzenkov. / Security of critical infrastructure facilities in the fuel and energy sector under martial law. // Nuclear Power and the Environment, 1 (34), 10-21, 2026 , doi.org/10.31717/2311-8253.26.1.2 (стаття фахове видання України Категорія Б), ISSN 2311-8253. Особистий внесок співавторів: Бібік Т.В. – визначив загальний науковий напрям дослідження, приймав участь у постановці задачі та формуванні концепції дослідження, проводив наукове консультування щодо: застосування міжнародного права та інтерпретації документів МАГАТЕ, виконав наукове редагування статті, провів експертну оцінку отриманих результатів, приймав участь у доопрацюванні висновків; Борзенков В.В. – сформував основну ідею дослідження щодо аналізу загроз ядерній та

енергетичній безпеці в умовах збройного конфлікту, виконав основний обсяг наукових досліджень (аналіз впливу воєнних дій на ядерні установки та паливно-енергетичні об’єкти, узагальнення досвіду України, проаналізував нові типи загроз, зокрема застосування БпЛА), проведено аналіз міжнародно-правової бази у сфері ядерної безпеки (документи МАГАТЕ, міжнародні договори), виконав інтерпретацію отриманих результатів та сформував висновки, підготовив основний текст статті (у співавторстві).

Праці з представленими матеріалами апробації дисертації:

3. Т.В. Бібік, В.В. Борзенков. XX Міжнар. наук.-практ. конф. молод. вчених і студ. м. Київ, 25–28 квіт. 2023 р. Безпілотні літальні апарати - загроза для фізичної ядерної безпеки АЕС України. Сучасні проблеми наукового забезпечення енергетики.ISBN 978-966-990-025-8.

4. V. Borzenkov. Second International Symposium on Insider Threat Mitigation 5-7 March 2024 in Brussels, Belgium. Mitigating Insider Threats in Times of Crisis.

5. Т.В. Бібік, В.В. Борзенков. XXI Міжнар. наук.-практ. конф. молод. вчених і студ., м. Київ, 23–26 квіт. 2024 р. Фізична ядерна безпека під час збройних канфліктів. Сучасні проблеми наукового забезпечення енергет .ISBN 978-966-990-111-8.

6. V. Borzenkov. International Conference on Nuclear Security: Shaping the future proceedings of an international conference organized by the International Atomic Energy Agency and held in Vienna. – Vienna: International Atomic Energy Agency, 20–24 MAY 2024. Physical control over critical infrastructure from blockage with the situation. ISBN 978-92-0-124525-0.

7. Т.В. Бібік, В.В. Борзенков. XXII Міжнар. наук.-практ. конф. молод. вчених і студ., м. Київ, 22–25 квіт. 2025 р. Захист ядерних установок в умовах війни. Сучасні проблеми наукового забезпечення енергетики. ISBN 978-966-990-152-1.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Позначення:

C	–	величина наслідків (consequences) від реалізації загрози (радіаційних, економічних тощо)
D	–	відстань між БпЛА та пристроєм виявлення або захищеним об'єктом
L	–	координати або параметри локації об'єкта/загрози
M	–	метод або режим роботи системи захисту/нейтралізації
N	–	загальна кількість засобів (виявлення, нейтралізації або елементів системи)
P	–	імовірність настання певної події
P_{det} (P_D)	–	імовірність виявлення загрози засобами системи фізичного захисту
P_I	–	імовірність переривання (interruption) дій порушника/загрози
P_{neut}	–	імовірність нейтралізації загрози (наприклад, засобами РЕБ або вогневого ураження)
P_{total_D}	–	загальна (кумулятивна) імовірність виявлення цілі інтегрованою системою
P_{ux}	–	імовірність виявлення загрози конкретним (x-м) датчиком або підсистемою
R	–	інтегральний показник ризику вразливості ядерної установки
t	–	час (поточний або тривалість процесу)
T	–	тип або категорія загрози (згідно з класифікацією)
$T_{response}$	–	час реакції сил охорони або автоматизованих систем захисту

Індекси:

det (або *D*)	–	індекс, що стосується процесу виявлення (detection)
f (fire)	–	індекс вогневого впливу або ефективності перехоплення
i	–	порядковий номер критичного елемента установки (вузла) або сценарію
j	–	порядковий номер засобу ураження або типу повітряної цілі
max	–	максимальне значення параметра
min	–	мінімальне допустиме або порогове значення параметра
neut	–	індекс, що стосується процесу нейтралізації (neutralization) загрози
total	–	сумарний або загальний показник для системи в цілому
ux	–	приналежність до *x*-го пристрою виявлення або сенсора
x	–	індекс конкретного технічного засобу або каналу виявлення

Скорочення:

АЕС	–	атомна електростанція
АСКЕРО	–	автоматизована система радіаційного контролю
БпЛА	–	безпілотні літальні апарати;
ВН	–	система відеоспостереження
ВРП	–	відкритий розподільчий пристрій
ВЯП	–	відпрацьоване ядерне паливо
ДІВ	–	джерел іонізуючого випромінювання
ДІЯРУ	–	Державна інспекція ядерного регулювання України
ДНТЦ ЯРБ	–	Державний науково-технічний центр ядерної та радіаційної безпеки
ДПЗ	–	Державна проектна загроза
ЕМО	–	електромагнитна обстановка
ЕМС	–	електромагнітна сумісність

ЗАЕС	–	Запорізька атомна електростанція
ЗСУ	–	Збройні Сили України
ІТЗ ФЗ	–	інженерно – технічні засоби фізичного захисту
КВП і А	–	контрольно-вимірювальні прилади і автоматики
МАГАТЕ	–	Міжнародне агентство з атомної енергії
МВГ	–	мобільні вогневі групи
МВС	–	Міністерство внутрішніх справ
МКЧХ	–	Міжнародний комітет Червоного Хреста
НАН	–	Національна академія наук
НГУ	–	Національна гвардія України
НПУ	–	Національна поліція України
ОЕС	–	об’єднана енергетична система
ППО	–	протиповітряна оборона
РДЕС	–	резервні дизель-електричні станції
РЕБ	–	радіоелектронна боротьба
СБУ	–	Служба безпеки України
СВЯП	–	Сховище відпрацьованого ядерного палива
СКУД	–	система контролю і управління доступом
ФЗ	–	фізичний захист
ЦОД	–	центр обробки даних
ЯМ	–	ядерний матеріал
ЯУ	–	ядерна установка
AdSec	–	Nuclear Security Advisory Committee
CRPA	–	Controlled Reception Pattern Antenna
DBT	–	Design Basis Threat
DOE	–	United States Department of Energy
FHSS	–	Frequency Hopping Spectrum Spreading
EW	–	Electronic Warfare
GNSS	–	Global Navigation Satellite System

IAEA – International Atomic Energy Agency
NRC – Nuclear Regulatory Commission
NWFZ – Nuclear-Weapon-Free Zones
PPS – Physical Protection Systems
RCS – Radar Cross Section
SBO – Station Blackout
SNL – Sandia National Laboratories
WINS – World Institute for Nuclear Security

ВСТУП

Актуальність теми дослідження. Актуальність теми дослідження. Забезпечення фізичного захисту ядерних установок і ядерних матеріалів є одним із ключових елементів глобальної системи ядерної та радіаційної безпеки. Упродовж тривалого часу міжнародна та національні нормативно-правові бази у сфері фізичного захисту формувалися в межах парадигми мирного часу, за якої основними загрозами вважалися дії недержавних суб'єктів - терористичних угруповань, кримінальних організацій або окремих диверсійних груп.

Однією з ключових складових системи національної безпеки є забезпечення ядерної та радіаційної безпеки, зокрема через функціонування ефективної системи фізичного захисту ядерних установок (ЯУ) та ядерних матеріалів (ЯМ). У контексті зростаючих геополітичних загроз, розвитку нових технологій, а також воєнної агресії проти України питання фізичного захисту набуває нового змісту та стратегічного значення.

На міжнародному рівні базові принципи фізичного захисту були закладені в таких документах, як Конвенція про фізичний захист ядерного матеріалу, Кодекс поведінки МАГАТЕ, рекомендації INFCIRC/225/Rev.5, документи серії Nuclear Security Series, які орієнтовані на стабільне інституційне середовище, повний контроль держави над територією розташування ядерних установок та відсутність активних бойових дій. Вони акцентують увагу на загрозах з боку недержавних суб'єктів: терористичних груп, диверсантів, внутрішніх порушників режиму тощо.

Упродовж тривалого часу формувалася концепція «глибоко ешелонованої оборони» - послідовна багаторівнева система фізичного захисту, що спирається на технічні, адміністративні, процедурні та інформаційні бар'єри. Проте така система передбачає стабільність державного управління, збереження

територіального контролю, відсутність бойових дій, функціонування правоохоронних та регуляторних органів у повному обсязі.

Починаючи з 2022 року, Україна опинилася в ситуації, яку не передбачали жодні попередні моделі безпеки: повномасштабна збройна агресія Російської Федерації, окупація територій із розміщеними ядерними об'єктами, обстріли промислових майданчиків, зникнення зовнішнього електропостачання, примус персоналу до дій всупереч інструкціям, а також систематичне блокування доступу регулятора - Держатомрегулювання України.

Особливої уваги потребує ситуація на Запорізькій атомній електростанції (ЗАЕС) - найбільшій у Європі. Її фактичне захоплення, тривала окупація, виведення з-під національного контролю, обстріли реакторних установок та об'єктів фізичного захисту створюють безпрецедентні ризики. Персонал перебуває під тиском, а МАГАТЕ не має повного доступу до обладнання.

Таким чином, перед світовою спільнотою та українською наукою постає нагальна необхідність переосмислення самої концепції фізичного захисту: від класичного «запобігання несанкціонованим діям» - до живучості ЯУ в умовах збройного конфлікту. Необхідно інтегрувати підходи до захисту від збройної агресії, терористичних актів, використання безпілотних літальних апаратів (БпЛА), радіоелектронної боротьби (РЕБ), кіберінтервенцій та комбінаційних атак.

Виявлена системна криза міжнародної та національної нормативно-правової бази полягає у відсутності механізмів забезпечення фізичного захисту ядерних установок у разі втрати державою контролю над територією, блокування дій регуляторних органів та деградації систем реагування. Чинні нормативні документи не враховують сценаріїв застосування регулярних збройних сил, ракетного та артилерійського ураження, кінетично-кіберних атак, а також примусу персоналу до виконання незаконних наказів.

У зв'язку з цим виникає об'єктивна наукова проблема, що полягає у необхідностю наукового осмислення поточної ситуації, виявлення системних прогалин у чинному національному та міжнародному правовому полі,

розроблення нових підходів до забезпечення захищеності ядерних об’єктів, що зможуть працювати навіть за відсутності повноцінного державного управління.. Саме ця проблема зумовлює актуальність даного дисертаційного дослідження.

Мета і завдання дослідження. Метою дисертаційної роботи є наукове обґрунтування підходів до вдосконалення системи фізичного захисту ядерних установок України з урахуванням викликів, пов’язаних із повномасштабною збройною агресією, тимчасовою окупацією та деградацією функцій державного контролю.

Завдання дослідження:

- Провести аналіз еволюції міжнародної нормативно-правової бази з фізичного захисту ядерних установок.
- Визначити межі застосовності рекомендацій МАГАТЕ та інших документів у реальних умовах війни.
- Дослідити функціонування системи фізичного захисту АЕС України в умовах бойових дій.
- Виявити вразливі місця існуючих концепцій охорони.
- Сформулювати принципи нової концепції - «живучість ядерної установки».
- Надати рекомендації щодо внесення змін до національного законодавства та відомчих документів.

Об’єкт і предмет дослідження. Об’єктом дослідження є система фізичного захисту ядерних установок і ядерних матеріалів.

Предметом є організаційні, правові та технічні засади забезпечення фізичного захисту ядерних установок в умовах збройної агресії.

Методи дослідження:

- системний аналіз - для оцінки складових фізичного захисту як єдиної системи;
- порівняльно-правовий аналіз - для зіставлення міжнародного та національного регулювання;

- метод моделювання ситуацій - для прогнозування загроз і ефективності захисту;
- історико-правовий підхід - для простеження еволюції підходів до фізичного захисту;
- експертне оцінювання - для обґрунтування практичної реалізації запропонованих рішень.

Наукова новизна. У межах дисертаційного дослідження:

- вперше обґрунтовано концепцію забезпечення живучості ядерної установки в умовах збройного конфлікту як складову системи фізичного захисту;
- удосконалено класифікацію загроз, що мають вплив на ядерні об’єкти в умовах бойових дій;
- дістала подальший розвиток модель ризик-орієнтованого підходу до побудови фізичного захисту з урахуванням руйнування інфраструктури, психологічного тиску на персонал і втрати зв’язку з державними органами.

Практичне значення отриманих результатів полягає у можливості їх використання при вдосконаленні національної нормативно-правової бази у сфері фізичного захисту, у діяльності органів державного регулювання, а також у процесі підготовки та навчання персоналу ядерних установок.

Отримані результати:

- можуть бути використані при перегляді нормативних документів з питань фізичного захисту;
- ляжуть в основу практичних рекомендацій для Міненерго, ДІЯРУ, НАЕК «Енергоатом»;
- є основою для підготовки навчальних курсів з питань безпеки АЕС в умовах воєнного часу;
- можуть бути інтегровані в діяльність оперативного штабу при надзвичайних ситуаціях на ядерних об’єктах.

Апробація результатів дисертації. Проміжні результати роботи доповідалися на:

- XV, XVI, XVII, XIX Міжнародних науково-практичних конференціях аспірантів, магістрантів, студентів "Сучасні проблеми наукового забезпечення енергетики" (Україна, м. Київ, 2017р., 2018р., 2019р., 2021р.);
- 26th International Conference on Nuclear Engineering ICONE26-82365. (London, England, July 22-26, 2018);
- VI міжнародній науково-практичній конференції «Безпека та ефективність атомної енергетики» (Одеський національний політехнічний університет. (Україна, м. Одеса, вересень 2018р.).
- VI науково-практичній конференції «Комп'ютерна гідромеханіка» (Інститут гідромеханіки НАН України, Україна, м. Київ, вересень 2018)
- II міжнародній науковій мультидисциплінарній конференції студентів та молодих учених "Modern Technologies: Improving the Present and Impacting the Future". (Україна, м. Дніпро, 2018р.)
- 25th International Conference on Structural Mechanics in Reactor Technology. (Charlotte, NC, USA, August 4-9, 2019)
- Міжнародній конференції «International Conference VVER2019 – Recent and Future» (Prague, Czech Republic, листопад 2019).

Публікації. Основні положення і результати дисертаційної роботи представлені у 2 публікаціях наукових робіт, серед яких: 2 статті у наукових фахових виданнях України; 1 стаття у міжнародному виданні, віднесеному до першого - третього квартилів (Q1-Q3); 9 тез доповідей у збірниках матеріалів конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел. Повний обсяг дисертації складає 241 сторінка, у тому числі 19 рисунків, 15 таблиць, список використаної літератури, що включає 141 найменування, 4 додатки на 16 сторінках.

1 КРИЗА КЛАСИЧНОЇ ПАРАДИГМИ ФІЗИЧНОГО ЗАХИСТУ ЯДЕРНИХ УСТАНОВОК В УМОВАХ ВІЙНИ

1.1 Аналітичний огляд та критична оцінка міжнародної нормативно-правової бази: від парадигми мирного часу до кризи системи безпеки

Формування та еволюція сучасної міжнародної нормативної архітектури у сфері фізичного захисту ядерних установок є складним історичним процесом, що тривав протягом останніх п’яти десятиліть. Цей процес відбувався під впливом глобальних геополітичних трансформацій, розвитку ядерних технологій та, передусім, як реакція світової спільноти на ескалацію ризиків, пов’язаних із незаконним обігом радіоактивних матеріалів та загрозами ядерного тероризму. Фундаментом для побудови глобального режиму ядерної фізичної безпеки (Nuclear Security Regime) стала розгалужена система міжнародних конвенцій, стандартів, рекомендацій та технічних керівництв, розроблених під егідою Міжнародного агентства з атомної енергії (МАГАТЕ) [1; 2]. Ця нормативна база мала на меті уніфікацію, гармонізацію та стандартизацію підходів до забезпечення безпеки ядерних об’єктів у різних юрисдикціях світу, створюючи єдиний простір відповідальності держав за безпечне використання атомної енергії.

Разом з тим, проведення системного, глибокого ретроспективного та змістовного аналізу дозволяє стверджувати, що системоутворюючою рисою цієї нормативної бази є її формування виключно на основі базового аксіоматичного припущення про те, що функціонування держав та експлуатація ядерних об’єктів відбуваються у мирний час. Ця «мирна парадигма» передбачає стабільне соціально-політичне середовище, повну інституційну дієздатність державних органів, непорушність національного суверенітету над територією розташування ядерних установок та відсутність ведення бойових дій із

використанням важкого конвенційного озброєння, ракетних систем, бойової авіації чи високоточної зброї [3; 4].

Саме цей концептуальний недолік, який десятиліттями залишався «сліпою зоною» міжнародного права, сьогодні, в умовах повномасштабної агресивної війни проти України, призвів до системного колапсу міжнародних гарантій безпеки. Міжнародні стандарти з фізичного захисту демонструють критичну невідповідність (conceptual gap) реальному спектру загроз, з якими безпосередньо стикаються ядерні об’єкти на театрі бойових дій [5]. Ця невідповідність є не просто технічною проблемою, а фундаментальною кризою всієї системи ядерної безпеки, що вимагає детального розбору на рівні кожного основоположного документа.

1.1.1 Критичний аналіз Конвенційних механізмів: юридичний вакуум воєнного часу

Першочергової уваги та детального критичного аналізу потребує основний міжнародно-правовий інструмент, що регламентує питання фізичного захисту на глобальному рівні та має обов’язкову юридичну силу для держав-учасниць - Конвенція про фізичний захист ядерного матеріалу (Convention on the Physical Protection of Nuclear Material - CPPNM), прийнята у 1979 році, та Поправка до неї, прийнята у 2005 році [1; 2].

Історично Конвенція 1979 року фокусувалася на вузькому сегменті безпеки - захисті ядерного матеріалу під час його міжнародного перевезення. Це відповідало тогочасним уявленням про загрози, де основним сценарієм вважалося викрадення матеріалу злочинними групами з метою шантажу або створення саморобного ядерного вибухового пристрою. Прийняття Поправки 2005 року стало значним кроком уперед, оскільки сфера дії документа була розширена на ядерні установки, що використовуються у мирних цілях, а також на внутрішньодержавне перевезення, використання та зберігання ядерних матеріалів [2]. Поправка також запровадила фундаментальні принципи

фізичного захисту (Fundamental Principles), які держави зобов'язані імплементувати у своє національне законодавство [3].

Однак, попри зовнішню прогресивність, навіть оновлена редакція документа не змінила його концептуальної основи, яка виявилася безпорадною перед лицем державної військової агресії. Аналіз тексту Конвенції та Поправки дозволяє виділити три критичні юридичні вади, що роблять ці документи недієвими в умовах війни в Україні.

По-перше, виключення військових дій зі сфери відповідальності. Найбільш критичною прогалиною є пряме виключення дій збройних сил держави зі сфери регулювання Конвенції. Так, у пункті 4 статті 2 Поправки до Конвенції зазначено: «Ніщо в цій Конвенції не повинно тлумачитись як таке, що обмежує правомірне застосування сили під час збройного конфлікту згідно з міжнародним правом» [2]. Більше того, Конвенція прямо вказує, що її положення не застосовуються до діяльності збройних сил держави під час збройного конфлікту.

Ця юридична норма фактично створює парадоксальну ситуацію: фізичний захист ядерної установки є обов'язковим і суворо регламентованим у випадку загрози з боку терористів або кримінальних елементів, але як тільки джерелом загрози стає регулярна армія іншої держави (як це сталося при окупації Запорізької АЕС), механізми Конвенції де-юре перестають діяти. Міжнародне право, таким чином, саме створює «імунітет» для агресора, виводячи атаки на ядерні об'єкти, здійснені військовими формуваннями, з-під дії спеціального режиму фізичного захисту, перекладаючи це питання у площину загального Міжнародного гуманітарного права (МГП), яке, як показала практика, не має реальних важелів примусу [4].

По-друге, орієнтація на кримінально-правове переслідування фізичних осіб. Вся архітектура Конвенції (стаття 7) побудована навколо зобов'язання держав криміналізувати певні діяння (крадіжка, грабіж, контрабанда ядерних матеріалів, диверсія) та забезпечити покарання або екстрадицію винних осіб [1]. Цей підхід є ефективним проти окремих злочинців, але абсолютно

нерелевантним, коли «порушником» виступає суверенна держава, яка діє через свої збройні сили. Конвенція визначає «диверсію» (sabotage) як будь-яку навмисну дію, спрямовану проти ядерної установки або ядерного матеріалу, що може створити загрозу здоров'ю та безпеці персоналу або населення внаслідок радіаційного впливу [2]. Однак, коли такі дії (наприклад, обстріл реакторного відділення або пошкодження ліній електропередач) вчиняються військовослужбовцями регулярної армії на виконання бойового наказу, вони часто кваліфікуються агресором як «військова необхідність» або «супутні збитки» (collateral damage), що ускладнює або унеможливлює застосування положень Конвенції щодо кримінальної відповідальності та екстрадиції [5].

По-третє, декларативність принципу відповідальності держави. Принцип «Відповідальність держави» (Responsibility of the State), закріплений у Фундаментальному принципі А Поправки, постулює, що відповідальність за створення, впровадження та підтримку режиму фізичного захисту цілком покладається на державу. Ця норма ідеально працює у мирний час, визначаючи суверенітет держави над своїми об'єктами. Проте Конвенція не містить відповіді на питання: хто несе відповідальність за фізичний захист ядерної установки, яка знаходиться на тимчасово окупованій території, де держава-оператор де-факто втратила контроль, а держава-окупант здійснює незаконне управління? [3] Юридичний вакуум призвів до ситуації на Запорізькій АЕС, коли де-юре відповідальність перед МАГАТЕ продовжує нести Україна (як ліцензіат та суверен), але де-факто можливості для реалізації заходів фізичного захисту в неї відсутні через дії окупаційної адміністрації [6]. Конвенція не передбачає механізму передачі відповідальності або запровадження міжнародного мандату управління у разі військової окупації, що робить її норми «мертвими» для окупованих об'єктів.

1.1.2 Криза концепції «Державного режиму фізичної безпеки» в документах серії NSS

Наступним рівнем нормативної піраміди є документи серії IAEA Nuclear Security Series (NSS), зокрема документ «Основи ядерної фізичної безпеки» (Objective and Essential Elements of a State's Nuclear Security Regime - NSS No. 20) [3]. Цей документ визначає архітектуру державного режиму безпеки, що складається з законодавчої бази, компетентного органу, оцінки загроз та системи інспекцій.

Детальний аналіз положень NSS No. 20 крізь призму воєнного стану виявляє критичну вразливість самої моделі побудови державного режиму. Документ базується на припущенні про інституційну стійкість та безперервність (institutional continuity). Передбачається, що:

- Компетентний орган (регулятор) має безперешкодний доступ до об'єкта. В Україні Державна інспекція ядерного регулювання (ДІЯРУ) втратила фізичний доступ до майданчика ЗАЕС та можливість здійснювати інспекційні перевірки систем фізичного захисту, що робить виконання вимог NSS No. 20 неможливим [3; 7].
- Правоохоронні органи функціонують у штатному режимі. Стандарти вимагають тісної співпраці оператора з розвідкою та поліцією для оцінки загроз. В умовах окупації ці національні органи оголошуються окупантом «ворожими» або «терористичними», а обмін інформацією з ними для персоналу станції стає смертельно небезпечним і кваліфікується окупантом як «шпигунство» [6].
- Законодавче поле є єдиним. Документи МАГАТЕ не передбачають ситуації правової колізії, коли на одному об'єкті персонал змушують виконувати вимоги двох суперечливих законодавств (національного та окупаційного), що руйнує нормативну основу фізичного захисту.

Окремої критики заслуговує підхід, викладений у документі IAEA Nuclear Security Series No. 30-G «Управління ризиками для фізичної ядерної

безпеки» (Risk Management for Nuclear Security) [8]. Запропонована методологія оцінки ризиків є суто технократичною та бюрократичною. Вона оперує поняттями «ймовірність» (likelihood) та «наслідки» (consequences), виходячи з того, що ймовірність успішної атаки на ядерний об'єкт є низькою через ефективність сил стримування. Війна спростувала цю аксіому. Ймовірність кінетичного ураження ядерного об'єкта в зоні бойових дій наближається до одиниці (100%), а поняття «прийнятного ризику», яким оперують документи МАГАТЕ, втрачає сенс, коли йдеться про загрозу навмисного підриву реактора або сховища відпрацьованого палива як акту геополітичного шантажу. Методологія NSS No. 30-G не пропонує інструментів для розрахунку ризиків в умовах, коли система захисту вже зруйнована, а об'єкт знаходиться під контролем ворога [8]. Вона розрахована на попередження інцидентів (prevention), а не на виживання (survival) системи в умовах тотального колапсу безпекового середовища.

Таким чином, на рівні фундаментальних конвенцій та основних положень державного режиму міжнародна нормативна база демонструє повну неготовність до сценарію «держава проти держави». Вона сконструйована для світу, де держави співпрацюють проти терористів, а не воюють одна з одною, перетворюючи АЕС на заручників військових амбіцій. Ця концептуальна прірва стає ще більш очевидною при переході від юридичних до технічних аспектів фізичного захисту, викладених у рекомендаціях INFCIRC/225/Rev.5 [9], аналіз яких потребує окремого детального розгляду (рисунок 1.1).

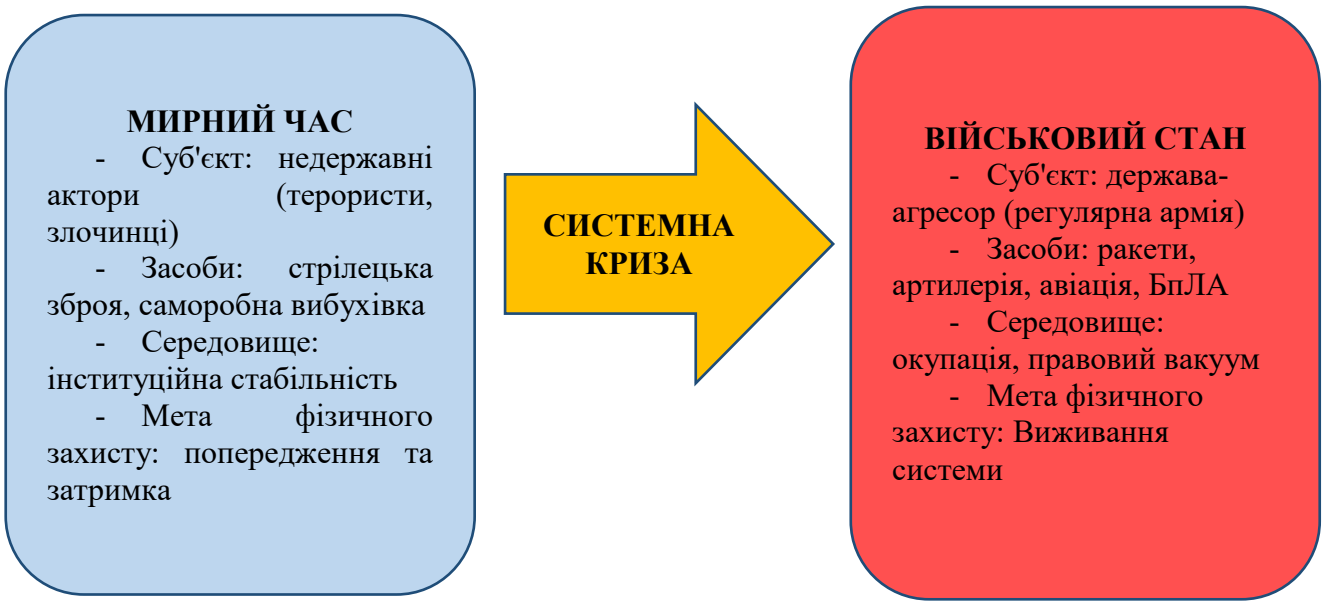

Рисунок 1.1. – Порівняльний аналіз базових припущень міжнародної нормативної бази та реалій військової агресії

1.1.3 Методологічний колапс концепції «Глибокого ешелонування» в умовах застосування важкого озброєння (Аналіз INFCIRC/225/Rev.5)

Центральне місце в архітектурі міжнародних стандартів займає документ МАГАТЕ INFCIRC/225/Revision 5 «Рекомендації з фізичного захисту ядерного матеріалу та ядерних установок» [9]. Цей документ є фактичним стандартом, на основі якого розробляються національні правила в усіх країнах-членах МАГАТЕ. Його філософія базується на концепції глибокого ешелонування (Defense in Depth), яка передбачає створення багаторівневої системи бар’єрів (технічних, організаційних, людських), що мають послідовно виконувати функції: стримування, виявлення, затримки та реагування [9].

Аналіз ефективності цієї концепції в умовах повномасштабної війни, що базується на емпіричних даних конфлікту в Україні, виявляє фундаментальну невідповідність інженерно-технічних рішень характеру військових загроз. Розглянемо деконструкцію функцій фізичного захисту детальніше.

Криза функції «Стримування» (Deterrence). Згідно з INFCIRC/225/Rev.5, функція стримування реалізується через демонстрацію потенційному порушнику надійності системи захисту, що має переконати його у

неможливості успішного виконання задуму. Цей психологічний механізм ефективно працює проти кримінальних елементів або раціонально мислячих терористів. Однак він абсолютно не діє проти регулярних збройних сил держави-агресора. Військові формування, що діють за наказом, не керуються страхом перед системою охорони об'єкта. Навпаки, наявність укріпленого ядерного об'єкта робить його пріоритетною військовою ціллю для захоплення з метою створення плацдарму або шантажу [6]. Таким чином, парадигма стримування, закладена в міжнародних стандартах, трансформується у свою протилежність: засоби захисту не відлякують, а приваблюють агресора, перетворюючи АЕС на «фортецю» для ведення бойових дій.

Технологічна вразливість функції «Виявлення» (Detection). Стандарти МАГАТЕ передбачають розгортання периметрових засобів виявлення (вібраційні, радіохвильові, інфрачервоні сповіщувачі) та систем відеонагляду [9]. Проте ці системи розраховані на фіксацію прихованого проникнення окремих осіб. В умовах сучасної війни функція виявлення нівелюється двома факторами, не врахованими в INFCIRC/225/Rev.5:

- Засоби радіоелектронної боротьби (РЕБ). Масоване застосування засобів РЕБ призводить до "осліплення" систем спостереження, блокування каналів передачі тривожних сигналів та виведення з ладу бездротових датчиків [10].

- Вогнева підготовка атаки. Артилерійський або мінометний обстріл периметра перед штурмом фізично знищує технічні засоби охорони (камери, датчики, освітлення) ще до моменту безпосереднього контакту порушника з бар'єром. Міжнародні рекомендації не містять вимог щодо бронювання або фортифікаційного захисту елементів системи виявлення.

Кінетична неспроможність функції «Затримка» (Delay). Функція затримки базується на створенні фізичних бар'єрів (паркани, стіни, двері, шлюзи), час подолання яких має бути більшим, ніж час прибуття сил реагування [9]. Розрахунок стійкості цих бар'єрів у міжнародних методиках здійснюється виходячи з інструментарію диверсанта: ручний інструмент,

різаки, легка вибухівка. Війна в Україні показала, що проти важкої бронетехніки (танків, БМП) та артилерії ці бар'єри мають нульову ефективність. Залізобетонний паркан, розрахований на затримку порушника з драбиною на 5 хвилин, знищується одним танковим пострілом миттєво. Стандарти МАГАТЕ не передбачають вимог до протитанкової оборони периметра (рів, їжаки, мінування підходів), оскільки це суперечить цивільному статусу ядерного об'єкта у мирний час. Відтак, концепція "часу затримки" втрачає фізичний сенс, коли атакуюча сторона застосовує важке озброєння [11].

Асиметрія функції «Реагування» (Response). Найбільш критичною прогалиною INFCIRC/225/Rev.5 є концепція сил реагування. Документ передбачає, що охорона об'єкта (guards) повинна мати достатню чисельність та озброєння для нейтралізації загрози (терористів) [9, с. 34]. Однак у сценарії військового вторгнення виникає абсолютна асиметрія сил. Підрозділ охорони АЕС, озброєний стрілецькою зброєю (автомати, пістолети), фізично не здатний протистояти механізованій батальйонно-тактичній групі регулярної армії за підтримки авіації та артилерії. Документи МАГАТЕ не розглядають питання переростання фізичного захисту в територіальну оборону. Відсутність у стандартах протоколів взаємодії з важкою артилерією чи ППО призводить до того, що система фізичного захисту стає ізольованою і приреченою на поразку в перші години загальновійськового бою [5; 6].

1.1.4 Операційні вразливості режиму доступу та внутрішньої безпеки в умовах окупації

Окрім інженерних аспектів, документ INFCIRC/225/Rev.5 [9] детально регламентує адміністративні заходи, зокрема контроль доступу та перевірку на благонадійність. Аналіз цих положень крізь призму окупації Запорізької АЕС демонструє повну руйнацію логіки внутрішньої безпеки.

Деградація системи контролю доступу (Access Control). Міжнародні стандарти вимагають суворої ідентифікації осіб при вході в захищені зони

(Protected Areas) та життєво важливі зони (Vital Areas). Передбачається, що право доступу надає оператор [9, с. 28]. В умовах окупації відбувається інверсія контролю: доступ на об'єкт починає контролювати не оператор, а озброєні військові формування агресора. Вони встановлюють власні блокпости, ігнорують системи біометрії та карткового доступу, або примусово вилучають перепустки у персоналу. Стандартна вимога «правила двох осіб» (two-person rule), покликана запобігти діям внутрішнього порушника, коли важливі з точки зору фізичного захисту операції здійснюють двома особами олночасно [9; 12], стає інструментом тиску: окупанти можуть приставити озброєного наглядача до оператора БЩУ, формально виконуючи правило присутності двох осіб, але фактично створюючи ситуацію примусу до виконання злочинних наказів.

Проблема внутрішнього порушника (інсайдера) та перевірки на благонадійність (Trustworthiness). Рекомендації МАГАТЕ наголошують на необхідності перевірки персоналу для виявлення потенційних внутрішніх порушників [12]. Проте вони не розглядають феномен «примусового інсайдера» (coerced insider). Під час війни лояльний та перевірений персонал перетворюється на загрозу не через власні переконання, а через застосування до нього тортур, шантажу (загроза життю сім'ї) або психологічного терору [13]. Документ INFCIRC/225/Rev.5 розглядає мотивацію інсайдера як ідеологічну, фінансову або психологічну (помста), але не враховує фактор виживання в умовах окупаційного терору. Жодна система перевірок (background checks) не здатна прогнозувати поведінку людини, яку тримають у підвалі та катують. Відтак, методологія захисту від внутрішнього порушника, закладена в міжнародних стандартах, стає нерелевантною в умовах терористичних методів ведення війни державою-агресором.

Вразливість життєво важливих зон (Vital Areas Identification). Методологія визначення життєво важливих зон у INFCIRC/225/Rev.5 сфокусована на запобіганні радіологічній диверсії (підрив реактора, басейну витримки) [9]. Однак досвід атак на енергосистему України показав, що критичною вразливістю є не сам реактор (який захищений контейнментом), а

системи видачі потужності - відкриті розподільчі пристрої (ВРП), трансформатори та лінії електропередач. Міжнародні стандарти розглядають ці об’єкти як менш пріоритетні з точки зору фізичного захисту, оскільки їх пошкодження у мирний час не веде до миттєвої радіаційної аварії. Проте у воєнний час цілеспрямоване систематичне знищення зовнішнього енергопостачання (Station Blackout) стає основною тактикою створення аварійної ситуації [5; 6]. Нормативна база не вимагає бункерного захисту для трансформаторів, що робить АЕС вразливими до дистанційних атак безпілотників та ракет, навіть без проникнення порушника на територію.

Таким чином, детальний аналіз INFCIRC/225/Rev.5 свідчить про те, що закладені в ньому інженерні та адміністративні бар’єри розраховані на протидію локальним загрозам низької інтенсивності. При зіткненні з військовою машиною ці бар’єри не просто втрачають ефективність, а стають декоративними, створюючи ілюзію безпеки, яка руйнується з першим артилерійським залпом. Порівняльна характеристика ефективності функцій фізичного захисту наведена в таблиці 1.1

Таблиця 1.1 – Порівняльна характеристика ефективності функцій фізичного захисту за умов мирного часу та військової агресії

Функція системи (згідно з INFCIRC/225)	**Реалізація в парадигмі мирного часу (Загроза: Терорист/Злочинець)**	**Реалізація в умовах війни (Загроза: Регулярна армія/РФ)**	**Оцінка ефективності у воєнний час**
1. Стримування (Deterrence)	Психологічний вплив на порушника через демонстрацію сили та технічних засобів охорони.	Ядерний об’єкт сприймається як пріоритетна ціль для захоплення (плацдарм, шантаж). Система охорони не лякає, а приваблює ворога.	Критично низька / Від’ємна
2. Виявлення (Detection)	Сенсори, датчики руху, відеокамери, розраховані на прихованого порушника.	Системи «сліпнуть» через дію засобів радіоелектронної боротьби (РЕБ) або знищуються артилерійською підготовкою перед штурмом.	Низька (залежить від вцілілої інфраструктури)

Продовження таблиці 1.1

Функція системи (згідно з INFCIRC/225)	**Реалізація в парадигмі мирного часу (Загроза: Терорист/Злочинець)**	**Реалізація в умовах війни (Загроза: Регулярна армія/РФ)**	**Оцінка ефективності у воєнний час**
3. Затримка (Delay)	Інженерні загородження (паркани, ворота), стійкі до ручного інструменту та легкої вибухівки.	Бар'єри миттєво руйнуються важкою бронетехнікою (танками) або дистанційними ракетними ударами. Час затримки наближається до нуля.	Нульова
4. Реагування (Response)	Сили охорони (Guard) та поліція, достатні для нейтралізації малої групи.	Асиметрія сил: стрілецька зброя охорони проти танків, авіації та артилерії. Блокування підкріплення зовнішніми силами.	Критично низька

1.1.5 Проблема вразливості логістичних ланцюгів та транспортування ядерних матеріалів

Окремим, вкрай чутливим кластером проблем, що виявила війна, є безпека транспортування ядерних та радіоактивних матеріалів. Базовим документом у цій сфері є IAEA Nuclear Security Series No. 9 «Безпека радіоактивного матеріалу під час перевезення» (Security of Radioactive Material during Transport) [14]. Філософія цього документа будується на концепції «захищеного маршруту», яка передбачає:

- попереднє оцінювання загроз на шляху слідування;
- безперервний зв'язок транспортного засобу з диспетчерським центром;
- можливість швидкого прибуття груп реагування (поліції) у будь-яку точку маршруту [14, с. 12].

В умовах повномасштабних бойових дій ці передумови стають недійсними. Війна трансформує транспортну мережу з нейтрального середовища у зону підвищеного ризику. По-перше, документ NSS No. 9 не враховує загрозу дистанційного мінування шляхів або руйнування мостової

інфраструктури, що може заблокувати транспорт з ядерним матеріалом у «сірій зоні», відрізаній від своїх сил [11]. По-друге, спеціалізовані транспортні засоби для перевезення відпрацьованого ядерного палива (ВЯП) або джерел іонізуючого випромінювання (ДІВ) є легкими цілями для ударних FPV-дронів та баражуючих боєприпасів. Міжнародні стандарти регламентують стійкість контейнерів до падіння чи пожежі (аварійні умови), але не до кумулятивного пробиття бойовою частиною ракети чи дрона [15]. По-третє, рекомендації МАГАТЕ базуються на секретності маршруту та часу перевезення. У сучасній війні, насиченій засобами аеророзвідки та супутникового спостереження, забезпечити прихованість руху колон спецтранспорту практично неможливо, що робить їх пріоритетними мішенями для терористичних атак держави-агресора.

1.1.6 Недостатність моделі кібербезпеки в умовах кінетичного впливу.

Сучасна парадигма захисту інформаційних активів ядерних установок викладена в документах IAEA Nuclear Security Series No. 17 «Комп'ютерна безпека на ядерних установках» (Computer Security at Nuclear Facilities) [16] та NSS No. 33-T «Комп'ютерна безпека для ядерної фізичної безпеки» [17]. Ці документи розглядають кібербезпеку як захист від цифрового втручання: хакерських атак, вірусів, програм-вимагачів.

Війна в Україні актуалізувала принципово новий тип загрози - кінетично-кібернетичну конвергенцію (Kinetic-Cyber Convergence), яка не описана в стандартах МАГАТЕ. Традиційна модель (NSS No. 17) передбачає, що фізичний захист серверних приміщень та центрів обробки даних (ЦОД) гарантується загальною системою охорони периметра. Однак, коли периметр прорвано або об'єкт знаходиться під артилерійським вогнем, фізичне знищення серверів стає найпростішим способом виведення з ладу систем управління та фізичного захисту [10]. Крім того, документ NSS No. 33-T фокусується на конфіденційності та цілісності даних [17]. В умовах окупації на перший план

виходить проблема інформаційної ізоляції. Захоплення російськими військами телекомунікаційних вузлів та перемикання трафіку на підконтрольні агресору мережі створило прецедент, коли український оператор та регулятор втратили можливість отримувати дані автоматизованих систем радіаційного контролю (АСКРО) в режимі реального часу [6; 18]. Чинні міжнародні стандарти не містять протоколів розгортання резервних, незалежних від наземної інфраструктури каналів супутникового зв'язку (типу Starlink) в умовах бойових дій.

1.1.7 Методологічна криза формування проектної загрози (Аналіз NSS No. 10)

Фундаментальною проблемою, що унеможливлює ефективне застосування міжнародних стандартів в умовах війни, є застаріла методологія оцінки загроз. Ключовим документом у цій сфері є IAEA Nuclear Security Series No. 10 «Розробка, використання та підтримання проектної загрози» (Development, Use and Maintenance of the Design Basis Threat) [19]. Цей документ регламентує процес створення державного документа «Проектна загроза» (DBT), який є основою для проектування будь-якої системи фізичного захисту. Детальний аналіз положень NSS No. 10 крізь призму воєнних дій в Україні виявляє критичні вади методології.

Документ NSS No. 10 визначає DBT як опис атрибутів та характеристик потенційних внутрішніх та/або зовнішніх порушників. Однак, у пункті 2.3 документа чітко окреслено коло цих порушників: «терористи, злочинці, протестувальники або інші недержавні суб'єкти» [19, с. 4]. Методологія МАГАТЕ не містить інструментарію для опису загрози, джерелом якої є суверенна держава (State Actor). Це створює парадоксальну ситуацію: система фізичного захисту АЕС проектується для протидії групі з 5–10 диверсантів з легкою зброєю, тоді як реальна загроза походить від батальйонно-тактичних груп чисельністю в сотні осіб за підтримки бронетехніки [6]. В результаті,

оператор АЕС витрачає колосальні ресурси на захист від «нижчою» загрози, яка стає нерелевантною в момент початку бойових дій.

Поряд з цим, методологія NSS No. 10 також базується на припущенні, що держава контролює територію навколо ядерного об'єкта («зона безпеки»). Це дозволяє розраховувати час прибуття зовнішніх сил реагування [19]. У документі відсутні рекомендації щодо формування DBT для сценарію «оточення» або «наближення лінії фронту», коли зовнішній периметр безпеки перестає існувати.

Процес перегляду DBT, згідно з рекомендаціями МАГАТЕ, також є недосконалим і займає місяці або роки. Сучасна війна характеризується динамічною зміною тактики (наприклад, поява FPV-дронів змінила поле бою за лічені тижні) [10]. Методологія NSS No. 10 є занадто інертною: вона не передбачає механізмів оперативної адаптації проектної загрози в режимі реального часу (наприклад, щодобового оновлення профілю загроз залежно від тактичної обстановки на фронті).

1.1.8 Ілюзорність «конфліктних» рекомендацій (Аналіз TECDOC-1867)

Особливої уваги в контексті дослідження заслуговує документ IAEA TECDOC-1867 «Питання щодо вибухонебезпечних залишків війни та інших конфліктних ситуацій на ядерних установках» (Considerations for Explosive Remnants of War and Other Conflict Situations at Nuclear Facilities) [20]. Назва документа може створити хибне враження, що МАГАТЕ має готові рецепти для воєнного часу. Проте змістовний аналіз тексту спростовує це припущення.

Документ фокусується на концепції ERW (Explosive Remnants of War - вибухонебезпечні залишки війни). Він детально описує процедури виявлення мін, снарядів, що не розірвалися, та покинутих боєприпасів [20, с. 15]. Фактично, TECDOC-1867 є інструкцією для постконфліктного відновлення (post-conflict recovery). У документі наявний критичний пробіл: він не описує дії персоналу та систем захисту під час активної фази кінетичного впливу.

Що робити зміні фізичного захисту під час артилерійського обстрілу прохідної? Як забезпечити фізичний захист периметра, якщо огорожу зруйновано танковим проривом, а бій триває? Яким є протокол дій у разі захоплення центрального пульту фізичного захисту озброєним противником?

Відповіді на ці питання в TECDOC-1867 відсутні. Документ рекомендує «призупинити діяльність, що загрожує безпеці», що є абсурдним для ядерного реактора, який неможливо «вимкнути» під час бою [20]. Таким чином, цей документ створює небезпечну ілюзію наявності регулювання, тоді як де-факто оператор залишається сам на сам із проблемою виживання під вогнем [6; 11].

1.1.9 Розрив між фізичним захистом та аварійною готовністю (Аналіз GSR Part 7)

В умовах війни фізичний захист (Security) та ядерна безпека (Safety) стають нерозривними. Атака на систему фізичного захисту (наприклад, підрив трансформатора) миттєво перетворюється на аварійну ситуацію. Тут виникає колізія з документом IAEA General Safety Requirements Part 7 «Готовність та реагування на ядерну чи радіаційну аварійну ситуацію» (Preparedness and Response for a Nuclear or Radiological Emergency) [21].

Цей документ встановлює вимоги до планів аварійного реагування. Однак він виходить із «мирної» логіки:

- Доступність шляхів евакуації. GSR Part 7 передбачає евакуацію персоналу та населення у безпечні зони [21, с. 42]. В умовах окупації або активних бойових дій евакуаційні шляхи можуть бути перерізані, замінновані або знаходитися під вогнем. Поняття «безпечної зони» на окупованій території не існує.
- Захист аварійних бригад. Документ вимагає забезпечення радіаційного захисту аварійних бригад. Проте він не розглядає питання фізичного захисту цих бригад від снайперського вогню чи дронів під час ліквідації наслідків обстрілу. Досвід ЗАЕС показав, що ремонтні бригади часто не могли вийти на об’єкт для відновлення ліній живлення через заборону

окупантів або продовження обстрілів, що прямо суперечить вимогам GSR Part 7 щодо оперативності реагування [6; 21].

- Автономність кризових центрів. Вимоги до кризових центрів не передбачають їх фортифікаційного укріплення (бункеризації) від проникаючих боєприпасів, що робить центри прийняття рішень вразливими для точкових ракетних ударів.

Таким чином, аналіз GSR Part 7 у комплексі з документами з фізичного захисту демонструє відсутність інтегрованого підходу «Safety-Security» для умов війни. Фізичний захист не готовий відбивати військові атаки, а система аварійної готовності не здатна функціонувати в умовах вогневого ураження та блокади.

Підсумовуючи викладене, можна стверджувати, що чинна глобальна архітектура фізичної ядерної безпеки є продуктом історичного консенсусу мирного часу. Вона базується на аксіомах стабільності державних інституцій, непорушності кордонів та дії міжнародного гуманітарного права. Ці аксіоми були спростовані практикою гібридної та повномасштабної агресії РФ проти України, що призвело до девальвації існуючих гарантій безпеки.

Має місце критична невідповідність між проектними загрозами, закладеними в стандарти (INFCIRC/225/Rev.5) [9], та реальними засобами ураження, що застосовуються у сучасній війні. Концепція «глибокого ешелонування», ефективна проти терористів, втрачає свою функціональність при зіткненні з регулярною армією, оснащеною важким озброєнням.

Рекомендації щодо державного режиму (NSS No. 20) [3] та оцінки ризиків (NSS No. 30-G) [8] не містять алгоритмів дій в умовах втрати державою контролю над територією, окупації об’єкта та неспроможності сил реагування.

Сліпе копіювання та імплементація міжнародних стандартів без їх адаптації до воєнних реалій створює лише ілюзію захищеності ядерних об’єктів України. Це формує об’єктивну наукову проблему, яка полягає у необхідності розроблення нової методології фізичного захисту, що інтегрувала б традиційні підходи МАГАТЕ з вимогами військової оборони та протидії гібридним

загрозам. Вирішення цієї проблеми вимагає переходу від статичної моделі «охорони» до динамічної моделі «живучості» ядерної установки в умовах ворожого середовища, що і є метою даного дисертаційного дослідження.

Рекомендації МАГАТЕ з фізичного захисту розроблені під модель, у якій ядерна установка функціонує в мирній державі, з повним контролем над територією, стабільною інфраструктурою, доступними силами реагування та відсутністю військових загроз. Ця модель повністю зруйнувалася під час війни проти України, що створює об’єктивну наукову та практичну потребу в розробленні нових принципів фізичного захисту, адаптованих до умов війни.

Варто зазначити, що міжнародні документи, які є фундаментом для національних систем фізичного захисту, не забезпечують необхідного рівня безпеки в умовах повномасштабної війни та не можуть бути застосовані. Український досвід, що включає ураження ядерних об’єктів ракетами, застосування дронів, довготривалі відключення від мережі, окупацію атомної станції, психологічний і фізичний тиск на персонал, довів необхідність переходу від мирної концепції фізичного захисту до концепції фізичного захисту в умовах гібридних і відкритих військових конфліктів.

Таблиця 1.2 – Критичний аналіз застосовності вимог аварійного реагування (GSR Part 7) в умовах активних бойових дій

Вимога стандарту IAEA GSR Part 7	**Базове припущення мирного часу**	**Реальна ситуація під час бойових дій (Gap Analysis)**
Евакуація персоналу та населення	Наявність безпечних маршрутів та транспорту. Можливість вивезення людей у «чисту зону»	Евакуаційні шляхи заблоковані, замінновані або знаходяться під прямим вогнем. Поняття «безпечної зони» на окупованій території відсутнє
Доступ аварійних бригад	Безперешкодний допуск ремонтних служб до пошкодженого обладнання	Ремонтні бригади не можуть вийти на об'єкт через снайперський вогонь, артилерійські обстріли або заборону адміністрації

Продовження таблиці 1.2

Вимога стандарту IAEA GSR Part 7	**Базове припущення мирного часу**	**Реальна ситуація під час бойових дій (Gap Analysis)**
Функціонування кризових центрів	Робота в штатному режимі, захист від радіації	Кризові центри стають пріоритетними цілями для ракетних ударів. Відсутні вимоги щодо їх фортифікаційного захисту (бункеризації)
Зовнішня підтримка	Гарантоване прибуття пожежних та медичних служб з-за меж майданчика	Зовнішня допомога відрізана лінією фронту. Логістика заблокована. Об'єкт має розраховувати виключно на власні сили

1.2 Аналіз законодавства України: Системна відповідність міжнародним «мирним» стандартам та нормативно-правовий колапс в умовах військової агресії

Українська національна нормативно-правова база, що регулює фізичний захист ядерних установок та ядерних матеріалів, формувалася як логічне та обов’язкове продовження глобальних стандартів, рекомендованих Міжнародним агентством з атомної енергії (МАГАТЕ) [1; 3; 9]. Впродовж десятиліть ця база була прикладом успішної імплементації міжнародних конвенцій та керівництв. Однак, її філософська та методологічна основа була вибудувана на аксіоматичному припущенні про непорушність державного суверенітету, цілісність території та стабільність соціально-політичного середовища. Усі національні нормативно-правові акти, без жодного винятку, зокрема базовий Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [22], були розроблені в умовах миру, передбачуваності та відсутності збройних загроз із використанням важкого озброєння, ракетних систем чи військової авіації.

Саме ця фундаментальна концептуальна «сліпа зона» призвела до того, що українська нормативна база сьогодні демонструє критичну невідповідність реальним загрозам. Національна система фізичного захисту, що будувалася на принципах логіки мирного часу та закріплена у відповідних нормах Закону України «Про використання ядерної енергії та радіаційну безпеку» [23], виявилася нормативно непідготовленою до сценаріїв повномасштабного вторгнення. Це обґрунтовує необхідність її суттєвого перегляду та адаптації, що є ключовою науковою проблемою цього дисертаційного дослідження.

1.2.1 Правовий вакуум у сфері державного контролю (Закон № 2064-III та № 39/95-ВР)

Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів та інших джерел іонізуючого випромінювання» № 2064-III [23] є основним структуроутворюючим нормативним актом. Він визначає терміни, принципи побудови та загальні вимоги до системи фізичного захисту. У статті 1 подається визначення фізичного захисту як діяльності, спрямованої на запобігання неправомірним діям (крадіжці, диверсії, несанкціонованому доступу). У статтях 5-6 встановлюються вимоги до запобігання диверсіям та крадіжці, проте ключовою рисою закону є те, що його норми повністю віддзеркалюють мирну модель порушника, успадковану з INFCIRC/225/Rev.4 [2].

Закон не містить жодних згадок про збройні конфлікти, воєнні дії, ракетні удари, застосування безпілотних систем або, що є найбільш критичним, втрату контролю над територією розташування ядерної установки. Механізми реагування (статті 13-16) та взаємодії між суб’єктами фізичного захисту (стаття 18) ґрунтуються на аксіомі інституційної дієздатності: передбачається, що державні органи - Служба безпеки України (СБУ), Національна поліція України (НПУ), Національна гвардія України (НГУ) - завжди мають фізичний доступ до об’єкта та можуть виконувати свої функції в повному обсязі.

Події, пов’язані із Запорізькою атомною електростанцією (ЗАЕС) у 2022-2023 роках, стали емпіричним доказом системного юридичного колапсу, який виникає у разі військової окупації. Жодний механізм, передбачений Законом № 2064-III [23], не може бути реалізований:

- держава-оператор (Україна) втрачає можливість контролювати пропускний режим;
- унеможливлюється здійснення нагляду через Державний регулюючий орган (ДІЯРУ) внаслідок фізичної блокади;
- блокується можливість оперативного реагування силами НГУ та НПУ;
- ускладнюється або унеможливлюється підтримка комунікації з персоналом та отримання інформації про стан об’єкта.

Таким чином, Закон № 2064-III, хоча й залишається ключовим документом національної системи, фактично не охоплює реальні загрози, пов’язані із застосуванням військової сили, перетворюючись на «мертву норму» для об’єктів, що знаходяться в зоні бойових дій або окупації [11; 21].
Закон України «Про використання ядерної енергії та радіаційну безпеку» № 39/95-ВР [22] також містить низку норм, що формують правові засади державного управління у сфері атомної енергетики. У ньому визначено поняття безпеки, встановлено обов’язки оператора та регулятора та механізми ліцензування.

Аналіз тексту демонструє, що всі процедури, визначені у законі, імперативно передбачають наявність стабільного державного апарату. Зокрема, механізм ліцензування та регуляторного контролю базується на двох аксіомах, які були зруйновані війною.

По-перше, це наявність постійного каналу комунікації. Передбачається безперервний обмін інформацією між оператором та регулятором. В умовах окупації ЗАЕС цей канал був порушений, і регулятор втратив можливість отримувати дані автоматизованих систем контролю (АСКРО) в режимі реального часу, що унеможливлює виконання його функцій [18].

По-друге, це доступність інспекторського контролю. Закон передбачає право регулятора на проведення інспекційних перевірок ядерних установок. Фізичне блокування доступу інспекторів на майданчик ЗАЕС російськими військовими формуваннями повністю паралізувало цей ключовий механізм державного контролю [6; 13].

Закон не містить положень щодо:

- ерозії суверенітету над об’єктом (втрата контролю над територією);
- насильницького захоплення та примусу персоналу до дій;
- перешкоджання функціонуванню регуляторного органу збройними силами іноземної держави;
- протоколів дій у разі системного та тривалого знеструмлення критичної інфраструктури, спричиненого бойовими діями.

Недостатність національної законодавчої бази в цих питаннях призвела до правової колізії на міжнародному рівні: наприклад, Україна де-юре залишається відповідальною за ядерну безпеку та фізичний захист ЗАЕС (як ліцензіат), але де-факто позбавлена можливості реалізовувати свої законні повноваження через дії окупанта. Закон № 39/95-ВР [22] не містить механізму «призупинення» або «передачі» відповідальності в умовах Force Majeure (непереборної сили), спричиненої військовою агресією.

1.2.2 Аналіз організаційно-процедурного паралічу (Правила та Вимоги ДІЯРУ)

Правила фізичного захисту ядерних установок та ядерних матеріалів, затверджені наказом ДІЯРУ від 04.08.2006 № 116 [24], є ключовим нормативним документом, що переводить загальні вимоги Закону в конкретні технічні та організаційні дії. Аналіз тексту Правил демонструє їхню майже повну ідентичність із методологічною логікою INFCIRC/225/Rev.4-5 [2; 9]. Документ детально регламентує: визначення зон обмеження доступу (захищена зона, життєво важлива зона); обов’язки охорони та її озброєння; порядок

пропускного та внутрішньооб'єктового режиму; алгоритми реагування підрозділів охорони на сигнали тривоги.

Ці Правила [24] не містять жодних положень, які враховують можливість систематичного руйнування периметра внаслідок артилерійських обстрілів, виведення з ладу центрального пульта охорони, блокування внутрішнього пересування персоналу військовими або дискредитації пропускного режиму силами агресора.

В умовах окупації Запорізької АЕС усі припущення, закладені в основу Правил, були зруйновані.

Доступ на об'єкт став контролюватися не оператором, а окупаційними військовими, що повністю нівелювало юридичну силу пропускних документів, виданих українським оператором [6; 21]. Алгоритми реагування охорони (розділ 4 Правил [24]) передбачають взаємодію з підрозділами НГУ та МВС, що було фізично неможливим, коли ці підрозділи були або виведені з ладу, або заблоковані на території, що перебуває під контролем ворога.

Система, що передбачає підпорядкування персоналу виключно оператору, виявилася неспроможною у ситуації, коли лояльний персонал перебуває під загрозою насильства або примусу з боку окупаційної адміністрації.

Вимоги до комплексу інженерно-технічних засобів фізичного захисту, затверджені наказом ДІЯРУ від 05.12.2011 № 176 [25], максимально деталізують національне законодавство. Вони детально описують вимоги до огороджень різних типів, сенсорів виявлення проникнення, систем відеоспостереження (ВН) та контролю і управління доступом (СКУД).

Аналіз змісту документа доводить, що ці вимоги сформульовані на припущенні абсолютної технічної стабільності, яка характерна виключно для мирного часу. Вимоги передбачають безперервне та гарантоване електропостачання, включаючи резервні джерела, але не розглядають сценарій системного зовнішнього блекауту, спричиненого масовим знищенням

критичної інфраструктури (трансформатори, лінії електропередач) ракетними ударами [18; 20].

Вимоги до систем виявлення [25] проникнення розраховані на протидію фізичному перерізанню чи перелазанню огородження. Вони не містять жодних вимог щодо бронювання або фортифікаційного захисту елементів периметра від мінометного вогню, артилерії чи ударних дронів. Це означає, що, хоча система фізичного захисту технічно існує, вона функціонально знищується до моменту прямого контакту з військовим порушником.

Вимоги передбачають також безперервне та гарантоване електропостачання, включаючи наявність резервних джерел. Однак вони не розглядають сценарій системного, тривалого зовнішнього блекауту (Station Blackout), спричиненого масовим кінетичним знищенням ключових елементів критичної інфраструктури (трансформаторні підстанції, відкриті розподільчі пристрої, високовольтні лінії електропередач) ракетними ударами або атаками БпЛА. Втрата зовнішнього електропостачання, що неодноразово фіксувалася на ЗАЕС, неминуче призводить до деградації систем ФЗ, виходу з ладу периметрових сенсорів та СКУД, що нівелює всі інженерні вимоги, закладені у Наказі № 176.

Вимоги до інженерних загороджень також розраховані на протидію спробам фізичного перерізання, перелазання чи злому з використанням ручного інструменту. Вони не містять жодних вимог щодо бункеризації, бронювання або фортифікаційного захисту елементів периметра від мінометного чи артилерійського вогню, або кумулятивного ураження, що здійснюється ударними дронами. Це означає, що, хоча система фізичного захисту технічно існує відповідно до національних стандартів, вона функціонально знищується до моменту прямого контакту з військовим порушником, оскільки атаки на інженерно-технічні засоби є масованими та системними.

Вимоги до систем відеоспостереження передбачають їхню цілодобову функціональність у штатному режимі, проте не містять протоколів дій та вимог до стійкості в умовах масованого застосування засобів радіоелектронної

боротьби (РЕБ). Використання РЕБ агресором призводить до блокування каналів передачі сигналів тривоги, порушення роботи сенсорів та "осліплення" операторів, що повністю паралізує функцію виявлення.

У реальних умовах війни жодна з цих умов не може бути гарантована. Нормативні вимоги до системи фізичного захисту, хоч і відповідають міжнародним стандартам мирного часу, виявилися концептуально непридатними для забезпечення безпеки під час військових дій.

НП 306.5.02/3.068-2001 «Вимоги до систем фізичного захисту ядерних установок та ядерних матеріалів» [26] визначає мінімальні критерії до побудови системи фізичного захисту, включно з вимогами до зон обмеженого доступу, характеристик периметра, а також категоризації ядерних матеріалів.

Проте ключовою вадою цього національного документа є те, що вся його логіка побудована на моделі проектної загрози, яка повністю повторює мирний, обмежений підхід INFCIRC/225/Rev.4-5. У документі встановлено, що противник - це група або окрема фізична особа, озброєна стрілецькою зброєю, вибуховими пристроями та здатна діяти приховано. Це, фактично, на початковому етапі розробки проекту фізичного захисту полегшує задачу адміністрації атомної електростанції, оскільки обмежує вимоги до стійкості. Однак, такий підхід цілком виключає з моделі проектної загрози такі елементи, як:

- застосування важкої військової техніки (танки, БМП);
- несанкціоноване використання повітряного простору ударними та розвідувальними БпЛА;
- масоване вогневе ураження з використанням артилерійських систем великої дальності.

Як наслідок, національна система фізичного захисту апріорі не проектувалася на забезпечення стійкості до військового втручання, що є прямим наслідком сліпого наслідування міжнародних «мирних» стандартів (рисунок 1.2).

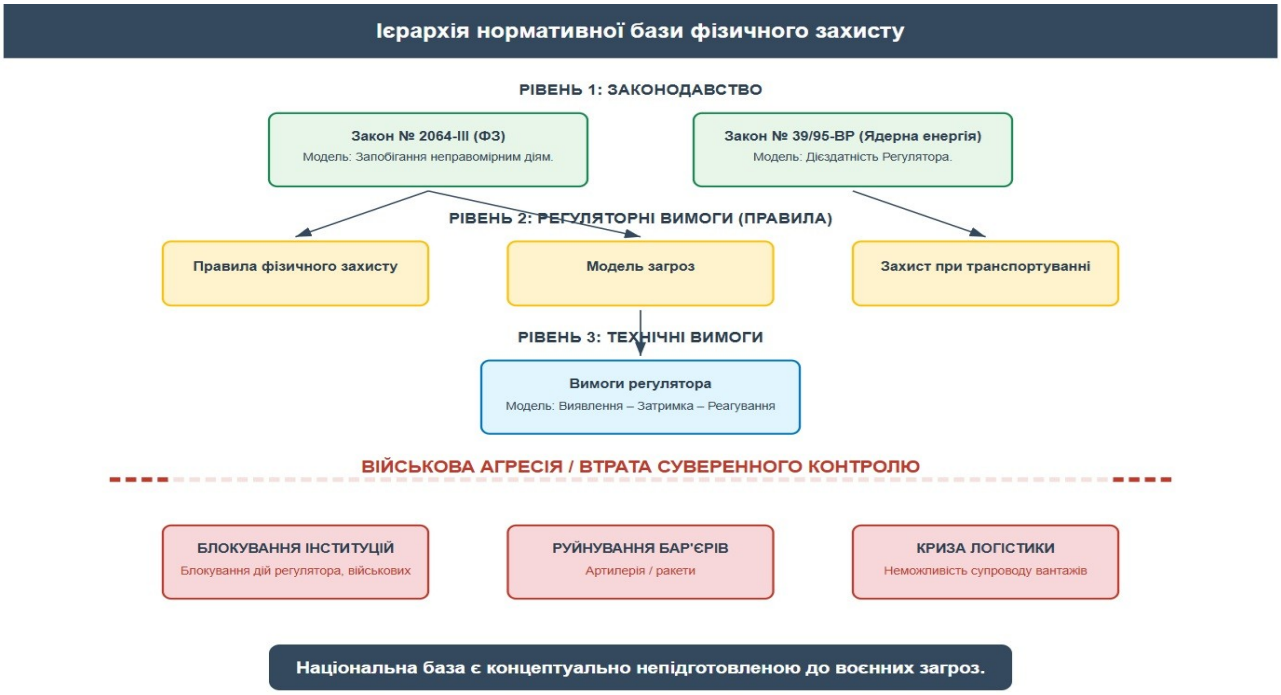

Рисунок 1.2 – Ієрархія нормативної бази фізичного захисту

1.2.3 Колапс транспортної безпеки (Аналіз НП 306.5.02/3.069-2002)

Особливої деталізації потребує сфера безпеки транспортування ядерних матеріалів, оскільки вона становить підвищений ризик для цивільного населення у випадку аварії під час перевезення. НП 306.5.02/3.069-2002 «Вимоги до фізичного захисту під час перевезення ядерних матеріалів» [27] визначає деталізовані вимоги до:

- супроводу вантажів;
- маршрутизації перевезень;
- прогнозування ризиків на маршруті;
- взаємодії з правоохоронними органами;
- забезпечення безперервного зв'язку між транспортними колоннами та службами безпеки.

Проте, як і всі попередні нормативні акти, цей документ є повністю орієнтованим на мирні умови, що у воєнний час створює низку критичних загроз: НП 306.02/3.069-2002 [27] передбачає доступність автомобільних шляхів, можливість патрулювання маршрутів та стабільність зв'язку. Утім, після початку повномасштабної війни частина територій України опинилася під

окупацією, транспортні шляхи зруйновані або заблоковані, а використання відкритих маршрутів становить надзвичайний ризик. Жоден норматив не описує, як діяти у разі, коли маршрут транспортування перетинає зону бойових дій або перебуває під загрозою ракетного обстрілу, що робить існуючу систему транспортної безпеки непридатною в умовах сучасної війни [14; 16].

Цей документ також не містить жодних вимог до додаткового фізичного захисту транспортних засобів від дронових або ракетних атак. Транспортні засоби з ядерними матеріалами стають потенційними мішенями для сучасних засобів ураження, а НП 306.02/3.069-2002 не передбачає ні тактичних протоколів уникнення небезпеки (наприклад, маскування, застосування антидронових засобів), ні вимог до конструктивної стійкості контейнерів до кінетичного впливу [15; 19].

Українська нормативно-правова база у сфері безпеки перевезень повністю дублює міжнародну мирну логіку, що призводить до глибокої нормативної прогалини та нездатності гарантувати безпеку ядерних матеріалів у воєнних умовах.

1.2.4 Проблема інтеграції фізичного захисту та ядерної безпеки (Security-Safety Interface)

В умовах мирного часу фізичний захист (запобігання несанкціонованим діям) та ядерна безпека (запобігання аваріям) розглядаються національним законодавством як окремі, хоча й взаємопов’язані, функції. Проте в умовах збройного конфлікту атака на систему фізичного захисту (Security) миттєво перетворюється на загрозу ядерній безпеці (Safety), що вимагає негайного комплексного реагування. Українське законодавство виявилося непідготовленим до такої конвергенції загроз.

Наприклад, Закон України «Про використання ядерної енергії та радіаційну безпеку» № 39/95-ВР [21] та відповідні норми щодо аварійної готовності, як і міжнародний документ IAEA General Safety Requirements Part 7

«Готовність та реагування на ядерну чи радіаційну аварійну ситуацію» [20], виходять із «мирної» логіки.

Національні плани аварійного реагування передбачають доступність шляхів евакуації персоналу та населення, а також гарантоване прибуття зовнішніх аварійних бригад, пожежних та медичних служб. В умовах окупації чи активних бойових дій ці припущення є хибними. Евакуаційні шляхи можуть бути перерізані, замінновані або знаходитися під прямим вогнем ворожих підрозділів [6; 13]. Відсутність у національних нормах протоколів, які б регламентували дії аварійних бригад під час снайперського вогню чи обстрілів, створює реальну загрозу не лише для безпеки об’єкта, але й для життя ліквідаторів. Таким чином, система аварійної готовності, що існує в Україні, є функціонально паралізованою в умовах воєнного стану через відсутність інтеграції з військовими протоколами фізичного захисту.

Національні вимоги до фізичного захисту (зокрема, Наказ Державної інспекції ядерного регулювання України № 176 [24]) зосереджені на захисті периметра та внутрішніх життєво важливих зон (реактор, сховища). Проте вони не передбачають вимог до фізичного захисту об’єктів, які життєво необхідні для підтримки ядерної безпеки, але знаходяться поза периметром: зовнішні трансформаторні підстанції, відкриті розподільчі пристрої та лінії електропередач. Саме ці об’єкти стали основними цілями ракетних та дронових атак, оскільки їх знищення призводить до системного знеструмлення, що, у свою чергу, ставить під загрозу роботу насосів охолодження реакторів [17; 18]. Національне законодавство не містить норм, які б зобов'язували оператора забезпечувати посилений фізичний захист або фортифікаційне укріплення зовнішніх енергетичних вузлів.

1.2.5 Системна відповідність та її наслідки: узагальнення національної неготовності

Загальним недоліком усіх без винятку українських нормативних документів є те, що вони не містять жодних легітимних механізмів забезпечення фізичного захисту в умовах, коли правова влада держави-оператора є тимчасово обмеженою або відсутньою.

Закон України № 2064-III [22] формує основні принципи фізичного захисту, встановлюючи обов’язок оператора взаємодіяти з підрозділами охорони та правоохоронними органами у разі виявлення неправомірних дій. Проте у реальних умовах військової окупації оператор фактично втрачає можливість взаємодіяти з національними силовими структурами (Національною гвардією, Національною поліцією, Службою безпеки України), що робить ці норми беззмістовними та нездійсненними. Аналогічно, вимоги до пропускного режиму, встановлені Правилами фізичного захисту [23], передбачають, що доступ до всіх критичних систем здійснюється персоналом, який перебуває у правовому полі та підпорядковується виключно оператору. Така система виявилася повністю неспроможною у випадку Запорізької атомної електростанції, де частина персоналу була під психологічним та фізичним примусом окупаційних військ, а оператор втратив адміністративний та фізичний контроль над територією об’єкта [13; 21].

Вимоги до перевезення ядерних матеріалів, установлені нормативним документом НП 306.5.02/3.069-2002 [26], базуються на наявності доступних, підконтрольних державі маршрутів та гарантованого супроводу. Утім, після початку повномасштабної війни транспортні шляхи виявилися зруйнованими або заблокованими, а використання відкритих маршрутів становить надзвичайний ризик для безпеки не лише ядерного матеріалу, але й цивільного населення. Жоден нормативний акт не описує, як діяти у разі, коли маршрут транспортування перетинає зону активних бойових дій або перебуває під

загрозою ракетного обстрілу чи використання дронів, що робить існуючу систему транспортної безпеки непридатною в умовах сучасної війни [14; 15].

Вимоги до інженерно-технічних засобів фізичного захисту (Наказ Державної інспекції ядерного регулювання України № 176 [24]) передбачають функціонування складних систем, розрахованих на сценарії, де противник діє приховано або намагається подолати периметр за допомогою ручних засобів. У реальних умовах війни периметри можуть бути знищені артилерійськими ударами або вибухами, які не передбачені жодним національним документом. Технічні засоби охорони, як показав досвід Запорізької атомної електростанції, можуть бути виведені з ладу точковими ударами безпілотних літальних апаратів або високоточними снарядами, тоді як нормативи вимагають, щоб вони забезпечували безперервне виявлення порушника [10; 19].

Аналіз національної нормативної бази свідчить про її системну відповідність міжнародним підходам МАГАТЕ [2; 4; 9], але водночас і про її концептуальну невідповідність воєнним загрозам, які стали реальною загрозою для України. Закони, підзаконні акти та нормативні документи Державної інспекції ядерного регулювання відображають виключно парадигму мирного часу, у межах якої ядерна установка функціонує у стабільному середовищі, під повним контролем держави, із передбачуваною поведінкою потенційних порушників, обмежених у доступі до важкого озброєння. Внаслідок цього українська система фізичного захисту виявилася незахищеною від кардинально нових типів загроз, характерних для повномасштабної війни: ракетних ударів, масованих атак дронів, артилерійського ураження, блокади, окупації, примусу персоналу та інформаційної ізоляції [6; 11].

Наразі можна стверджувати, що українська нормативна база з фізичного захисту потребує докорінного перегляду з урахуванням нових типів загроз, які не охоплені жодним чинним документом.

Це вимагає не просто внесення косметичних змін, а створення цілісної концепції фізичного захисту в умовах воєнного стану, яка повинна передбачати:

- Розширення моделі проектної загрози шляхом включення до неї сценаріїв застосування військової сили, важкої бронетехніки та безпілотних літальних апаратів [18]. Це дозволить перейти від захисту від «диверсанта з вибухівкою» до захисту від «військового підрозділу з ракетним озброєнням».
- Розроблення вимог до стійкості інженерно-технічних засобів фізичного захисту (периметрів, систем відеоспостереження, комунікаційних вузлів) у разі масованих ракетних і дронових атак, а також вимог до їхньої автономності в умовах тривалого знеструмлення [17; 20].
- Визначення юридичного порядку функціонування ядерних установок у випадку часткової або повної втрати державного контролю над територією, що є ключовим для вирішення проблеми відповідальності та зв'язку з персоналом.
- Створення процедур взаємодії оператора з регулятором в умовах часткової або повної інформаційної ізоляції, включаючи вимоги до захищених, автономних каналів супутникового зв’язку [16].
- Розроблення протоколів забезпечення фізичного захисту під час окупації або тимчасового захоплення об’єкта, що охоплюють питання поведінки персоналу та запобігання виконанню злочинних наказів агресора.

Такий докорінний перегляд є не лише технічною необхідністю, що випливає з досвіду експлуатації ядерних об’єктів у війні, але й критично важливим фактором забезпечення національної безпеки України та підвищення стійкості глобального режиму ядерної безпеки перед викликами воєнних загроз XXI століття.

Результати детального нормативно-правового аналізу відповідності міжнародних рекомендацій МАГАТЕ та законодавства України узагальнено у додатку А (табл. А.1-А.2).

1.3 Аналіз наукових досліджень та методологій фізичного захисту: деконструкція «Мирної Парадигми»

Міжнародні наукові дослідження, технічні методології та математичні моделі у сфері фізичного захисту ядерних установок формувалися протягом останніх п’ятдесяти років під впливом глобального розвитку ядерної енергетики, що був тісно пов’язаний із парадигмою «Атом для миру», а також у відповідь на загрози незаконного обігу ядерних матеріалів [1; 3]. Основний пласт цих досліджень та розробок походить зі Сполучених Штатів Америки - зокрема, від провідних установ, таких як Лос-Аламоська національна лабораторія, Національна лабораторія Сандія (Sandia National Laboratories, SNL), Міністерство енергетики США (DOE), Комісія з ядерного регулювання (NRC), а також від міжнародних платформ, таких як World Institute for Nuclear Security (WINS) та низки технічних серій документів МАГАТЕ, включно з TECDOC [19; 20].

Проте спільною та визначальною рисою всіх цих наукових підходів є їхня розробка в умовах ідеалізованого мирного часу, з виключною орієнтацією на диверсійні, кримінальні або терористичні загрози, а не на великомасштабні воєнні конфлікти. Міжнародна наукова література, незважаючи на її глибину, інженерну точність та математичну логічність, не передбачала і не прогнозувала появи ситуацій, коли ядерний об’єкт може стати полем бойових дій або бути цілеспрямовано атакований регулярною армією іноземної держави з використанням важкого озброєння та високих технологій [6; 11]. Ця фундаментальна наукова прогалина створила методологічний вакуум, що став критичним в умовах військової агресії проти України.

1.3.1 Деконструкція фундаментальної моделі SNL PPS: колапс тріади D-D-R

Одним із ключових наукових внесків у формування сучасної моделі фізичного захисту стала методологія побудови Систем фізичного захисту (Physical Protection Systems - PPS), створена в Національній лабораторії Сандія (SNL) ще у 1970-1980-х роках. Ця методологія була пізніше розвинена у серії фундаментальних праць, таких як «Довідник систем фізичної безпеки» (Physical Security Systems Handbook) та «Проектування та оцінка систем фізичного захисту» (Design and Evaluation of Physical Protection Systems), авторства Родріго Гарсіа (Rodrigo Garcia) та інших [27].

Модель SNL PPS є основою для всіх міжнародних стандартів, включно з INFCIRC/225/Rev.5 [2] та IAEA Nuclear Security Series No. 27-G. Вона побудована на трьох базових, послідовних компонентах - Виявлення (Detection), Затримка (Delay) та Реагування (Response) (методологія D-D-R) - які вважаються універсальними та взаємозамінними для будь-якої системи захисту. Проте сама по собі ця тріада є ефективною виключно в мирних умовах, де противник має обмежені можливості у вогневих засобах і не може знищити периметр за межами розрахункового часу.

Аналіз наукової літератури SNL виразно показує, що вся система PPS моделюється під противника з кардинально обмеженими ресурсами. У класичній моделі, що лягла в основу міжнародного регулювання, противники:

- діють приховано або малими групами;
- не володіють бронетехнікою;
- не мають доступу до важкого озброєння та ракетних систем;
- не застосовують засоби радіоелектронної боротьби для придушення зв’язку;
- не здатні вести загальновійськові бойові дії у відкритому наступі.

Це підкреслює, що модель SNL PPS від самого початку була побудована для боротьби з терористичними та кримінальними загрозами (non-state actors), а не для ситуацій військового втручання.

У воєнний час усі три компоненти класичної моделі втрачають свою функціональність, що призводить до системного колапсу фізичного захисту:

Наукові моделі виявлення SNL розраховані на ймовірність виявлення (PD) порушника, який намагається приховано подолати інженерні бар'єри. Водночас, засоби виявлення (камери, сенсори, радіохвильові датчики), регламентовані міжнародними вимогами, виводяться з ладу ще до моменту прориву. Масове застосування радіоелектронної боротьби [9] «осліплює» системи відеоспостереження, а артилерійський обстріл периметра знищує фізичні датчики та освітлення. Наукова література не містить методик розрахунку ймовірності виявлення в умовах активного придушення систем.

Методології SNL не включають моделювання БпЛА. Дрони-камікадзе долають периметр «повітрям», не активуючи наземні сенсори, що створює 100% гарантію прориву системи виявлення по цьому вектору.

Функція затримки є математично найважливішою, оскільки час затримки (T_D) повинен бути більшим, ніж час реагування (T_R) (тобто $T_D > T_R$). Наукові розрахунки T_D ґрунтуються на часі, необхідному для подолання бар'єра (паркана, стіни, дверей) з використанням ручного інструменту, різаків або легкої вибухівки.

В умовах військової агресії функція затримки стає ілюзорною. Фізичні бар'єри, розраховані на затримку в 5–10 хвилин проти терориста, знищуються одним танковим пострілом або влучанням ракети за мілісекунди. T_D в цих умовах математично прямує до нуля. Наукові методології не передбачають вимог до протитанкової оборони периметра (протитанкові рови, тетраедри), що могло б збільшити T_D проти бронетехніки.

Функція реагування передбачає прибуття та дії сил охорони, які мають перервати (Interruption) дії порушника. Ймовірність переривання (P_I)

розраховується на основі часу реакції та часу затримки. В умовах військового конфлікту час реагування (T_R) стає нескінченним або невизначеним.

Документи SNL та МАГАТЕ не розглядають сценарій, коли зовнішні сили реагування (НГУ, поліція) фізично блокуються лінією фронту або окупантом [6; 11]. T_R стає часом, необхідним для деокупації території. Навіть якщо сили охорони перебувають на об'єкті, їхнє штатне озброєння (легка стрілецька зброя) не відповідає озброєнню військового противника (бронетехніка, артилерія). Це призводить до того, що ймовірність успішного переривання (P_I) дій військового противника фактично прямує до нуля.

1.3.2 Обмеженість інструментів кількісного моделювання: EASI та SAVI

Обмеженість класичної моделі простежується і в наукових інструментах кількісного моделювання загроз, розроблених у SNL - EASI (Estimate of Adversary Sequence Interruption) та SAVI (Systematic Analysis of Vulnerability to Intrusion) [2; 27].

Обидва інструменти створені для моделювання ймовірності того, що система фізичного захисту зможе виявити, затримати або перервати дії порушника. Проте вони є алгоритмічно обмеженими концепцією мирного часу. Усі їхні вхідні змінні мають сенс лише за умови стабільності. Моделі EASI та SAVI виходять з того, що інженерні бар'єри зберігають свою структуру протягом атаки, а сили виявлення не вимикаються зовнішнім впливом (обстрілами) [19; 20].

Жодна модель не передбачає сценарію «катастрофічної деструкції», де час затримки (T_D) дорівнює нулю, а час реагування (T_R) є невизначеним.

Це означає, що спроба застосувати моделі EASI чи SAVI для оцінки загроз із використанням артилерії або дронів [9; 10] призводить до математичного абсурду: результати моделювання завжди показуватимуть нульову ймовірність успішного переривання атаки ($P_I = 0$), що вимагає або виведення ядерної установки з експлуатації, або повної зміни вхідних даних, що є науково неправомірним.

1.3.3 Регуляторні виключення в американській методології: свідоме ігнорування військових загроз

Обмеженість науково-методологічної бази фізичного захисту посилюється регуляторною політикою ключових ядерних держав. Аналіз американських методологій Міністерства енергетики (DOE) та Комісії з ядерного регулювання (NRC) підтверджує, що існуюча система не лише не здатна, але й свідомо не призначена для моделювання загроз військового походження.

Обмеження, характерні для наукових розробок Сандія Нешнл Лабораторіз [27], також відображаються у методологіях Департаменту енергетики США, зокрема у документах серії Nuclear Security Program та DOE Orders 470.3B і 473.3A. У цих документах визначено проектну загрозу, процедури оцінки вразливості, вимоги до охоронних підрозділів та інженерно-технічних бар'єрів. Проте жоден документ не розглядає сценарій руйнування об'єкта важким озброєнням, яке може бути застосоване регулярною армією, чи окупації території військами противника. Навіть у більш деталізованих документах DOE йдеться про «перевірку сил-на-силу» (force-on-force test), що передбачає моделювання збройного нападу у межах можливостей невеликої, добре підготовленої диверсійної групи. Цей підхід є ефективним для оцінки здатності системи протистояти терористам-комбатантам, але є повністю нерелевантним для протидії кінетичній силі та тактиці армійської операції [10; 11].

Найбільш показовою є позиція Комісії з ядерного регулювання США (Nuclear Regulatory Commission, NRC), яка встановлює вимоги до фізичного захисту атомних електростанцій у Сполучених Штатах. У федеральному регламенті 10 CFR 73 «Physical Protection of Plants and Materials» чітко визначено, що проектна загроза включає: сухопутну атаку, використання легкої стрілецької зброї, сценарії внутрішнього порушника та спроби проникнення.

Однак, NRC прямо, законодавчо виключає зі сфери проектних загроз великомасштабні військові операції або атаки, здійснені іноземною державою. Це юридичне обмеження, яке існує в найрозвиненішій системі ядерного регулювання світу, є прямим доказом того, що наукова і регуляторна спільноти не моделюють і не готують цивільні ядерні об'єкти до війни.

Причина цього виключення є подвійною. Атаки, здійснені іноземною державою, є актами війни, а не злочинними діяннями. Захист від них є функцією військових і зовнішньополітичних відомств (Міністерство оборони, Держдепартамент), а не цивільного регулятора (NRC). При цьому вважається, що рівень захисту, необхідний для протистояння регулярній армії з важким озброєнням, є нереалістичним і економічно недоцільним для цивільної інфраструктури.

Це регуляторне рішення, хоча і є логічним у контексті американського розподілу повноважень, призводить до того, що основні наукові моделі фізичного захисту залишаються концептуально «сліпими» до найвищого рівня загрози, що сьогодні є реальністю для України [6; 20].

1.3.4 Обмеження діяльності World Institute for Nuclear Security (WINS) та технічних документів МАГАТЕ

Обмеженість методології D-D-R та регуляторні виключення посилюються фокусом діяльності інших міжнародних наукових та прикладних організацій. World Institute for Nuclear Security (WINS) здійснює важливу діяльність, спрямовану на підвищення культури безпеки та поширення найкращих практик. Інститут випустив низку керівних документів, зокрема WINS Best Practice Guide 1 - Nuclear Security Governance, WINS Guide on Insider Threat Mitigation [12] та WINS Guide on Transport Security [14] .

Документи WINS, які є значущими з точки зору операційної безпеки, містять детальні описи моделей внутрішнього порушника, сценаріїв диверсії або крадіжки ядерних матеріалів. Однак усі ці моделі, знову ж таки, орієнтовані

на мирні загрози, що стосуються терористичних або злочинних груп, а не сценаріїв державної агресії. У наукових та прикладних документах WINS немає рекомендацій щодо того, як має діяти оператор або держава у разі:

- окупації ядерного об’єкта або встановлення зовнішнього військового контролю [6];
- блокади транспортних шляхів та неможливості безпечного перевезення матеріалів [15];
- цілеспрямованого знищення зовнішньої інфраструктури, що підтримує життєдіяльність об’єкта [18].

Таким чином, WINS, як і інші міжнародні наукові центри, не має концептуального інструментарію для надання практичних рекомендацій в умовах військового конфлікту.

Навіть технічні документи МАГАТЕ серії TECDOC (Technical Document), які, на відміну від NSS, містять більш інженерні та прикладні розробки, обмежені мирною парадигмою. Наприклад, IAEA TECDOC-575 “Protection of Nuclear Facilities Against Sabotage” та IAEA TECDOC-1801 “Development of an Incident Response System for Nuclear Security Events” детально описують лише сценарії диверсій, незаконного проникнення та інших неправомірних дій, які відбуваються у контрольованому, мирному середовищі. Вони не враховують сценарії повного руйнування об’єкта важкою зброєю або застосування проти нього регулярних збройних сил. Це підтверджує, що існуючий TECDOC-1867 [20], хоча і є кроком до усвідомлення проблеми, поки що залишається винятком, а не частиною системної інженерної методології.

1.3.5 Фундаментальний науковий висновок та обґрунтування нової методології

Аналіз міжнародної наукової літератури, регуляторних документів та прикладних методологій свідчить про повну домінацію мирної парадигми у світовій науковій думці щодо фізичного захисту. Ця домінація привела до того,

що наукова модель (SNL, EASI, SAVI) є нечутливою до змін у вогневій силі противника [2; 27]. Регуляторна база (NRC, DOE) свідомо виводить військові загрози зі сфери цивільної відповідальності. Ні Сандія Нешнл Лабораторіз, ні Міністерство енергетики США, ні WINS, ні академічні дослідження не передбачали можливості військових атак на цивільні ядерні об'єкти, а тому не містять концептуального інструментарію, який дозволив би забезпечити захист в реальних умовах, з якими зіткнулася Україна [6; 11].

Це формує об'єктивну наукову необхідність розроблення нової методологічної рамки, яка повинна здійснити перехід від концепції «захисту від проектної загрози» до концепції «забезпечення живучості (Resilience) та стійкості до воєнних загроз» на рис. 1.3. Ця нова модель має стати основою для інтеграції військових факторів у цивільне ядерне регулювання [18; 20].

Рисунок 1.3 – Трансформація системи фізичного захисту

Аналіз досвіду бойових дій на території України виявив низку критичних вразливостей існуючих систем захисту, які раніше не розглядалися в

міжнародних стандартах. Практичні кейси, що ілюструють реальні сценарії атак на енергетичну інфраструктуру та порушення режимів безпеки АЕС, наведено у Додатку Д.

1.4 Огляд української наукової літератури у сфері фізичного захисту: Концептуальний розвиток та методологічна обмеженість

Українська наукова література з питань фізичного захисту ядерних установок формувалася у взаємодії з національною нормативною базою [22; 23], міжнародними стандартами Міжнародного агентства з атомної енергії (МАГАТЕ) [2; 4] та накопиченим практичним досвідом експлуатації українських атомних електростанцій. Домінуючим напрямом розвитку української наукової школи стало поєднання інженерно-технічного аналізу з процедурними та організаційними аспектами забезпечення безпеки. В більшості наукових публікацій українських авторів фізичний захист розглядається як інтегрована система технічних, організаційних і режимних заходів, яка має забезпечувати запобігання неправомірним діям, їх виявлення та стримування [7; 25].

Систематизація наукових досягнень української наукової школи у сфері фізичного захисту дозволяє виокремити три ключові напрями, які є найбільш досліджені та визначені, проте водночас найбільш вразливі до критики в контексті воєнних загроз: інституційний та регуляторний аналіз, інженерно-технічне моделювання та соціотехнічна проблематика.

1.4.1 Внесок ключових науково-технічних центрів та інституційна критика

Значну роль у формуванні української наукової літератури відіграли дослідження, підготовлені Державним науково-технічним центром ядерної та радіаційної безпеки (ДНТЦ ЯРБ). Як ключовий експертний та аналітичний центр у системі ядерного регулювання, ДНТЦ ЯРБ сфокусувався на детальному

розробленні методичних і аналітичних матеріалів, що слугували основою для національних норм і правил [7; 18].

У працях фахівців Центру детально розглядаються питання оцінки вразливості систем фізичного захисту, включаючи аналіз можливих шляхів проникнення, характеристик засобів виявлення та факторів, що впливають на надійність фізичних бар'єрів. У цих дослідженнях закладено фундаментальні підходи до системного моделювання загроз, які стали основою для численних наукових публікацій у сфері проектування та модернізації елементів охорони [25]. Проте, оскільки діяльність ДНТЦ ЯРБ була безпосередньо обмежена чинними національними нормами, які повторюють логіку INFCIRC/225/Rev.4/5 [2; 9], науковий аналіз Центру апріорі базувався на моделі мирного часу. Відсутність у сфері їхніх досліджень сценаріїв застосування військової сили, артилерійських обстрілів чи окупації території є не їхньою недоробкою, а наслідком виконання мандату, який не передбачав таких катастрофічних загроз.

У публікаціях Інституту проблем безпеки АЕС НАН України особлива увага приділяється дослідженню технічних характеристик систем виявлення, контролю доступу та реагування. У науково-технічних збірниках Інституту наведені результати експериментальних досліджень ефективності сенсорів та датчиків, аналізу роботи засобів відеонагляду, випробувань фізичних бар'єрів та оцінювання надійності технічних рішень в умовах тривалої експлуатації. У цих роботах системи фізичного захисту аналізуються як складні технічні комплекси, які повинні відповідати вимогам режимності, адаптивності та безвідмовності.

Водночас, фокус цих досліджень на міцності бетону чи швидкості спрацювання датчиків у штатному режимі не давав відповіді на питання стійкості цих систем перед кінетичною енергією сучасних засобів ураження, що стало критичним фактором під час захоплення ЧАЕС та обстрілів ЗАЕС [6; 20].

1.4.2 Аналіз інженерно-технічного моделювання та його обмежень

Значний внесок у розвиток української наукової школи зробили технічні університети, зокрема Київський політехнічний інститут імені Ігоря Сікорського. У дисертаційних роботах і наукових статтях дослідників цього університету системи фізичного захисту розглядаються крізь призму математичного моделювання неправомірних дій, оптимізації розміщення технічних засобів та аналізу структурної конфігурації охоронних зон.

Українські дослідники часто застосовують методи теорії ймовірностей, оптимізаційні алгоритми та процедури формалізації критеріїв ризику. Однак, критичний аналіз цих праць свідчить, що всі математичні моделі та алгоритми оптимізації ґрунтувалися на вхідних даних мирного часу [7; 25].

Моделювання часу затримки фізичних бар'єрів (T_D) передбачало вплив лише ручного інструменту або легкої вибухівки. У наукових працях відсутні моделі, які б враховували ймовірність руйнування бар’єрів важкою бронетехнікою або артилерійськими ударами, що є ключовим фактором зведення до нулю часу затримки [19].

Математичні моделі, що аналізують ймовірність переривання порушника, оперували з гарантованим часом прибуття сил реагування (T_R). Жодне дослідження не враховувало сценарій блокади підкріплення чи інституційного колапсу, коли час реагування є невизначеним або дорівнює часу, необхідному для деокупації території [6; 11].

Оптимізація розміщення технічних засобів охорони (сенсорів, камер) була спрямована на підвищення ймовірності виявлення (P_D) прихованого проникнення, але не на забезпечення їхньої фізичної стійкості (Hardening) до осколкового ураження або точкових ударів безпілотних літальних апаратів [9; 10].

1.4.3 Огляд проблематики внутрішнього порушника та інтеграції систем

У низці українських досліджень простежується увага до проблематики внутрішнього порушника (insider threat). У роботах фахівців, що працюють у сфері ядерної безпеки та фізичного захисту, розглядаються моделі потенційного внутрішнього порушника, аналізуються типові сценарії дій персоналу, досліджуються психологічні та організаційні фактори, які можуть призвести до порушення режиму доступу або несанкціонованого доступу до критичних елементів об’єкта. В українській літературі також наголошується на важливості процедурної регламентації поведінки персоналу, багаторівневого контролю доступу та структуризації повноважень [7; 12].

Проте, як і у випадку міжнародних підходів WINS, усі ці моделі є ефективними проти інсайдера, який діє за власною мотивацією (ідеологічною, фінансовою, помстою). Українська наукова література не розглядала феномен «примусового інсайдера» (coerced insider), де лояльний персонал змушений діяти проти інтересів держави під загрозою насильства окупаційних військ. Відсутність протоколів та наукового аналізу цього явища свідчить про глибоку соціотехнічну прогалину, яка не була актуальною у мирний час [6; 13].

Важливим напрямом українських наукових досліджень є питання взаємодії елементів системи фізичного захисту з іншими системами безпеки на ядерних установках. У роботах цього напряму досліджуються питання інтеграції технічних засобів охорони у загальну систему управління безпекою та взаємозв’язки між фізичним захистом і радіаційним контролем [4; 18]. Ці дослідження демонструють прагнення української наукової школи до системного підходу, який виходить за межі окремих технічних аспектів. Однак, інтеграція «Security» та «Safety» розглядалася лише у контексті запобігання аварії, спричиненій диверсією, і не включала механізмів виживання цих систем під час воєнного впливу.

Важливим напрямом українських наукових досліджень є питання взаємодії елементів системи фізичного захисту з іншими системами безпеки на

ядерних установках. У роботах цього напряму досліджуються питання інтеграції технічних засобів охорони у загальну систему управління безпекою, взаємозв'язки між фізичним захистом і радіаційним контролем, технічна сумісність систем та можливості оптимізації процедур. Такі дослідження демонструють прагнення української наукової школи до системного підходу, який виходить за межі окремих технічних або процедурних аспектів.

Таким чином, українська наукова література характеризується комплексним підходом до аналізу фізичного захисту ядерних установок, що включає технічні, організаційні, процедурні та соціотехнічні аспекти. Роботи українських дослідників суттєво доповнюють міжнародні підходи, поєднуючи їх із практичними реаліями експлуатації українських ядерних об'єктів. Узагальнення цих досліджень є важливим для формування повного уявлення про еволюцію науки про фізичний захист в Україні та створює основу для переходу до аналізу методологічних засад проектування систем фізичного захисту, що становитиме зміст наступного підрозділу.

Водночас узагальнення української наукової літератури дає підстави стверджувати, що всі зазначені дослідження - як технічні, так і аналітичні - формувалися в умовах, коли функціонування ядерних установок України відбувалося у стабільному середовищі, а фізичний захист розглядався виключно в контексті мирного часу.

У нормативних матеріалах, методичних рекомендаціях, дисертаційних роботах та аналітичних дослідженнях не розглядається можливість зовнішнього силового втручання, застосування засобів ураження військового типу, деструктивних дій регулярних армій чи обстрілів критичної інфраструктури [10; 11].

Моделі загроз, критерії оцінювання, підходи до визначення уразливостей і варіанти реагування ґрунтувалися на припущенні про відсутність масштабних воєнних ризиків і відмежовувалися від сценаріїв, які згодом стали реальністю для українських ядерних об'єктів [19].

Таким чином, національна наукова школа фізичного захисту, попри її значну глибину й розвиток, потребує фундаментального переосмислення у напрямі врахування воєнних загроз, що виходить за межі класичних підходів і створює науково-практичне підґрунтя для переходу до наступного етапу дослідження - аналізу методологічних засад побудови системи фізичного захисту в нових умовах.

1.5 Еволюція концепції фізичного захисту ядерних установок: міжнародний та національний контекст

Еволюція підходів до побудови систем фізичного захисту ядерних установок у світовій та українській науковій традиції характеризується послідовним формуванням концепцій, що відображають соціально-політичні умови, технологічний рівень та безпекові уявлення певного історичного періоду.

Аналіз джерел свідчить, що фундаментальні принципи фізичного захисту, які сьогодні лежать в основі міжнародних та національних підходів, були сформовані у другій половині XX століття та не передбачали можливості масштабних воєнних дій або збройної агресії проти ядерних об’єктів. Саме ця вихідна парадигма мирного часу стала визначальною для подальшого розвитку нормативних рекомендацій, наукових концепцій та практичних рішень, які упродовж десятиліть сприймалися як універсальні та достатні [1; 27].

Одним із ключових етапів становлення концепції фізичного захисту стало формування перших рекомендацій МАГАТЕ щодо захисту ядерних матеріалів і установок у 1970-1980-х роках, що пізніше були кодифіковані у документі INFCIRC/225 у редакціях Rev.1-Rev.3.

У цих документах описувалася модель порушника як групи злочинців з обмеженими ресурсами, які діють приховано, прагнуть викрадення матеріалу або саботажу, але не ведуть відкритих бойових дій, не застосовують важке озброєння, не мають доступу до військової техніки, не обстрілюють об’єкти та

не здійснюють операцій штурмового типу. Концепція фізичного захисту в цей період формувалася на припущеннях стабільності, дипломатичної рівноваги та глобальної системи контролю озброєнь (Риснок 1.4).

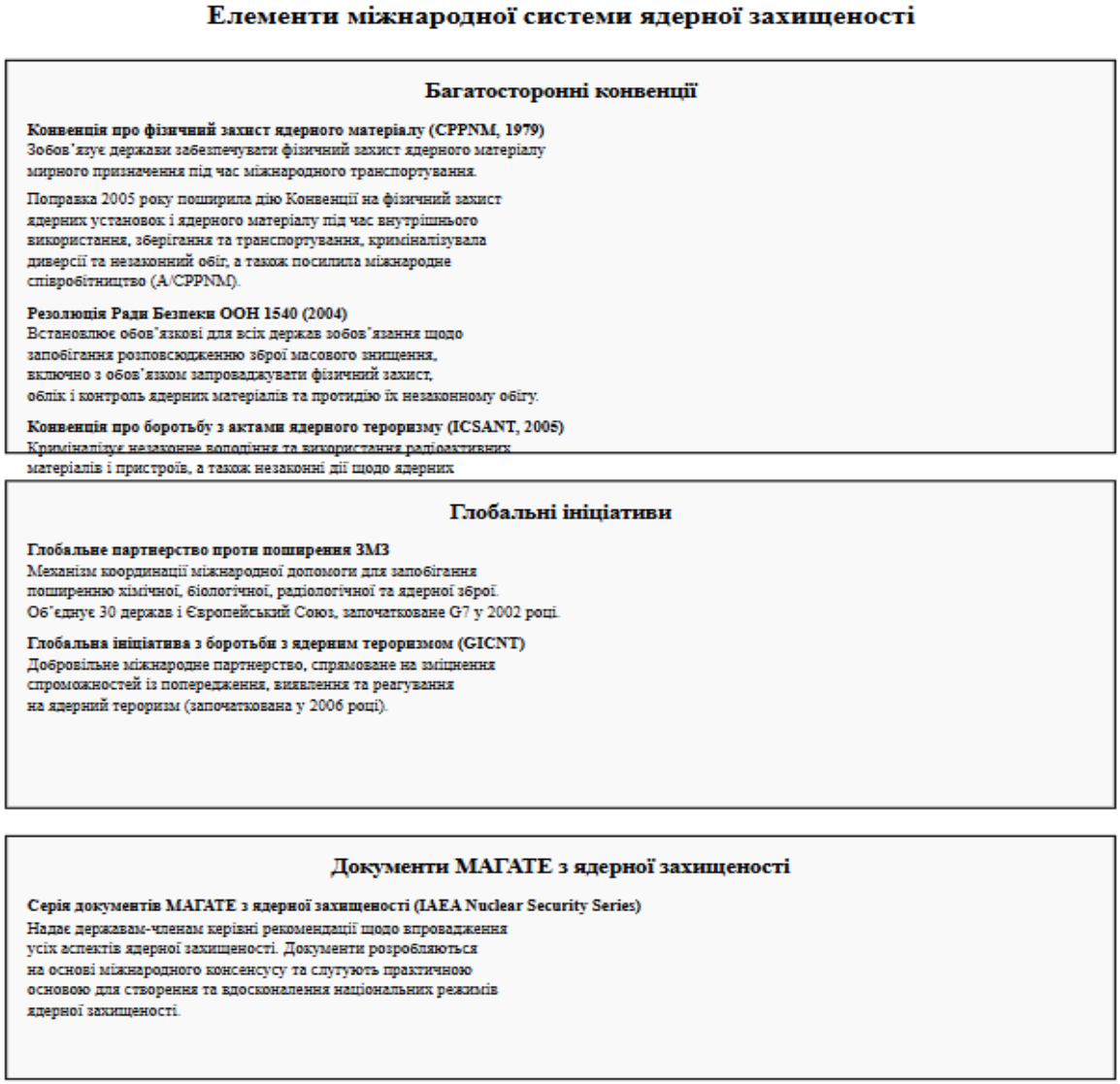

Рисунок 1.4 – Елементи міжнародної системи ядерної захищеності

Подальший розвиток міжнародних рекомендацій, що призвів до появи INFCIRC/225/Rev.4 та Rev.5 [2; 9], відбувся вже в умовах після холодної війни та зростання загроз, пов’язаних із діяльністю терористичних організацій. Проте попри розширення спектра сценаріїв неправомірних дій, у літературі та нормативних документах цього періоду продовжує зберігатися базове припущення про мирний характер середовища, у якому функціонують ядерні об’єкти.

Порушник розглядається як нелегальний суб’єкт, а не як збройні сили держави. Документи МАГАТЕ передбачають застосування лише стрілецької зброї, вибухівки, транспортних засобів, але не включають сценарії артилерійських обстрілів, ракетних ударів, окупації, блокади об’єкта або навмисного руйнування зовнішніх інженерних систем за допомогою військових засобів [4; 19].

Аналіз міжнародної наукової літератури другої половини XX - початку XXI століття підтверджує, що дослідники зосереджували увагу на розвитку технічних засобів охорони, оптимізації периметральних систем, удосконаленні методів оцінювання вразливостей, але в межах парадигми, де ядерна установка є захищеним режимним об’єктом у стабільній державі, що має контроль над власною територією та правоохоронною інфраструктурою.

Концепції «виявлення–затримка–реагування», математичні моделі затримки порушника, алгоритми прогнозування шляхів проникнення - усі ці підходи формувалися як інструментарій для боротьби з диверсійно-терористичними групами, але не з військовими атаками, що мають іншу шкалу, динаміку та рівень руйнівного потенціалу [27].

У цьому контексті аналіз літератури чітко демонструє, що військові загрози знаходились поза межами компетенції систем фізичного захисту. Класичний підхід МАГАТЕ, який домінує і сьогодні, чітко розмежовує фізичний захист (physical protection), ядерну безпеку (nuclear safety) та ядерну захищеність (nuclear security), при цьому будь-які питання військових дій відносяться до сфери національної оборони, а не до сфери цивільної ядерної безпеки.

Це означає, що міжнародна наукова спільнота не розглядала сценарії, подібні до подій на ЗАЕС, як можливі в реальному житті; вони вважалися такими, що виходять за межі «раціональної моделі загроз».

Схожа динаміка простежується і в українській науковій традиції. Українські публікації 1990-2010-х років здебільшого орієнтуються на

міжнародні документи та адаптують їх до національного законодавства й технічної інфраструктури [22; 23].

У працях ДНТЦ ЯРБ, ІПБ АЕС та технічних університетів значна увага приділяється технічним аспектам захисту периметра, функціональним характеристикам систем виявлення, моделюванню дій внутрішнього порушника, оптимізації охоронних процедур, але всі ці дослідження виконані із припущенням, що ядерні установки функціонують у неконфліктному середовищі, де зовнішня загроза обмежується кримінальними або терористичними актами невеликого масштабу [7; 25].

Методики аналізу уразливостей, що були розроблені в Україні у 2000-2010-х роках, також побудовані на концепції мирного часу. У них передбачено нормальне функціонування комунікацій, відсутність бойових дій, доступність сил реагування, можливість своєчасного прибуття підрозділів охорони, а також відсутність загрози руйнування критичної інфраструктури засобами військового ураження. Жодна з методик не містить аналізу сценаріїв артилерійського обстрілу, збройного штурму, окупації або захоплення персоналу [11; 18].

Таким чином, аналіз розвитку концепції фізичного захисту як у міжнародній, так і в українській літературі, свідчить про домінування стабільної, мирної моделі безпекового середовища, яка була покладена в основу майже всіх теоретичних конструкцій, нормативних документів та методів оцінювання. Еволюція системи фізичного захисту відбувалася в умовах, де війна, цілеспрямовані удари по критичній інфраструктурі та застосування засобів військового ураження не розглядалися як предмет наукового аналізу. Така парадигма, що була цілком логічною для свого часу, виявилася неспроможною пояснити та охопити реалії, з якими зіткнулася Україна після 2014 року, а особливо після 2022 року [5; 6].

Підсумовуючи, можна стверджувати, що історичний розвиток фізичного захисту ядерних установок сформував сильну, але однобічну модель, у якій захист орієнтовано на порушника, а не на повномасштабні загрози державного

рівня. Саме ця невідповідність між історично сформованими підходами та сучасними викликами створює основу для формулювання наукової проблеми дисертації та переходу до наступного підрозділу - аналізу порівняльних підходів і виявлення концептуальних розривів між міжнародними, українськими та воєнними умовами.

1.6 Порівняльний аналіз міжнародних і національних підходів до фізичного захисту ядерних установок

Порівняння міжнародних і національних підходів до фізичного захисту ядерних установок дозволяє виявити спільні концептуальні засади, структурні подібності та системні відмінності, що визначають специфіку реалізації фізичного захисту в Україні. Аналіз літератури свідчить, що українська нормативна та наукова база формувалася на основі міжнародних рекомендацій МАГАТЕ, насамперед INFCIRC/225 [2] та супутніх документів серії Nuclear Security Series [4; 19], які впродовж кількох десятиліть залишаються фундаментальною основою у сфері фізичного захисту.

Попри це, національні документи увібрали в себе як міжнародні принципи, так і специфічні особливості української ядерної інфраструктури, що визначає особливості їх співвідношення [22; 23].

Однією з ключових спільних рис між міжнародними та українськими підходами є домінування функціональної принципу побудови системи фізичного захисту - «виявлення - затримка - реагування». У міжнародних документах цей принцип подається як універсальний [27], а нормативно-правові акти України та наукові праці вітчизняних дослідників, зокрема В. В. Сухоручкіна [28], практично повністю відтворюють цю концепцію, пристосовуючи її до особливостей територіальної організації охорони українських АЕС.

Нормативно-правові акти України практично повністю відтворюють цю концепцію, пристосовуючи її до українських АЕС, особливостей територіальної

організації охорони та взаємодії між експлуатуючою організацією та правоохоронними структурами.

У міжнародній літературі основна увага приділяється визначенню проектної загрози (DBT) [19]. Українська модель загроз деталізує дії порушників, їх можливості та мотиви, проте порівняльний аналіз показує, що обидві моделі історично формувалися під впливом припущення: порушник не є регулярною армією. Як зазначає С. І. Кондратов [29], стратегії захисту критичної інфраструктури в Україні тривалий час розроблялися в межах антитерористичної парадигми, що робить їх концептуально мирними та обмежує можливості аналізу сценаріїв воєнної агресії [10, 11; 20].

Особливістю міжнародних документів МАГАТЕ є їх універсальний характер. В Україні, навпаки, вимоги адаптовані до структури національних об’єктів та розподілу обов’язків між підрозділами НГУ та експлуатуючою організацією [7; 24]. Крім того, українська нормативна база значно детальніша у технічному плані. Дослідження, що публікуються у фахових виданнях, як-от «Ядерна та радіаційна безпека» [30], містять конкретні результати випробувань фізичних бар’єрів та алгоритми оптимізації систем виявлення, що виступає важливою складовою регуляторного нагляду.

Попри структурні відмінності, міжнародні та українські документи мають спільний концептуальний недолік: обидва рівні нормативного забезпечення виходять з припущення щодо мирного функціонування ядерних об’єктів. У міжнародній літературі практично відсутні згадки про можливість військової агресії проти ядерних установок, тоді як українські документи успадкували ці припущення, не передбачаючи сценаріїв, які стали реальністю під час воєнних дій.

Це обмеження проявляється у всіх компонентах системи фізичного захисту - від моделі порушника до критеріїв затримки та оцінювання часу реагування.

Аналіз українських досліджень також показує, що хоча в науковій літературі систематично вивчаються технічні засоби охорони, методи

оптимізації та управління режимом доступу, ні міжнародні, ні українські наукові роботи не містять моделей фізичного захисту, розрахованих на умови повномасштабної війни. У публікаціях не розглядаються сценарії руйнування інфраструктури внаслідок обстрілів, відсутність сил реагування, блокада об'єкта, обмеженість персоналу, порушення зв'язку або тимчасова окупація території. Таким чином, обидві системи підходів - міжнародна і національна - мають спільний історично обумовлений обмежувальний фактор.

Попри це, міжнародні та українські документи мають спільний концептуальний недолік: припущення про мирне функціонування об'єктів. Аналіз українських дисертаційних робіт та статей свідчить, що хоча в них систематично вивчаються технічні засоби охорони та методи оптимізації [12; 16], вони не містять моделей, розрахованих на умови повномасштабної війни. У публікаціях не розглядаються:

- сценарії руйнування інфраструктури артилерією [6; 11];
- повна блокада сил реагування та втрата зв'язку з регулятором [17; 18];
- феномен «примусового інсайдера» в умовах окупації [13].

Порівняльний аналіз дозволяє зробити висновок, що українські нормативні та наукові документи є більш деталізованими й адаптованими до місцевих умов, але концептуально спираються на міжнародну традицію, яка була сформована за умов глобальної стабільності та відсутності уявлення про можливість воєнного втручання в роботу ядерних установок. Це створює методологічну прогалину, яка виразно проявилася у сучасних умовах, та підкреслює необхідність переосмислення базових підходів до фізичного захисту в умовах військових загроз.

Цей аналіз показує, що міжнародні та українські підходи значною мірою збігаються у своїх принципах, структурі та вихідних припущеннях, однак обидві системи є концептуально мирними, що зумовлює їхню обмежену ефективність у контексті сучасних викликів. Цей висновок стає передумовою для переходу до розгляду наступного підрозділу, присвяченого критичному

аналізу мирної орієнтації глобальних стандартів фізичного захисту та її впливу на безпеку ядерних об’єктів у період збройних конфліктів.

1.7 Проблематика мирної орієнтації міжнародних стандартів фізичного захисту ядерних установок

Аналіз міжнародних нормативних документів та наукової літератури засвідчує, що всі ключові концепції, на яких базується сучасна система фізичного захисту ядерних установок, формувалися в умовах тривалої глобальної стабільності та були орієнтовані виключно на контекст мирного часу. Рекомендації МАГАТЕ [2], документи серії INFCIRC, стандарти Nuclear Security Series [4; 19], керівні матеріали WINS [31] та відповідні технічні публікації, що заклали фундамент для підходів побудови систем фізичного захисту ядерних установок, виходять із припущення, що ядерні об’єкти функціонують у середовищі, вільному від активних бойових дій, артилерійських обстрілів, окупації чи захоплення військовими формуваннями.

Ця парадигма мирного часу не є випадковою - вона відображає історичні, політичні та правові обставини, у яких формувалася міжнародна система ядерної безпеки. Після завершення Другої світової війни і створення МАГАТЕ у 1957 році, основна увага міжнародної спільноти була спрямована на запобігання розповсюдженню ядерної зброї, контроль над ядерними матеріалами та забезпечення їх мирного використання. Відповідно, перші рекомендації керівних документів з фізичного захисту були сконцентровані на запобіганні крадіжкам ядерних матеріалів та окремим диверсійним діям, а не на протидії військовим загрозам.

У фундаментальному документі INFCIRC/225 у редакціях Rev.1-Rev.4 не передбачено жодних сценаріїв воєнного ураження об’єкта. Поняття проектної загрози формулюється через діяльність недержавного суб’єкта: злочинної чи терористичної групи з обмеженою кількістю осіб та засобів. Відсутність у моделі загроз озброєних сил держави є системною ознакою. Навіть у

найсучаснішій версії INFCIRC/225/Rev.5 (2011) порушник розглядається виключно як нелегальна група, що діє приховано або з обмеженою силою. У документі немає жодних положень, що стосувалися б захисту ядерних установок від ракетних ударів, артилерії, безпілотних літальних апаратів військового типу, радіоелектронної боротьби або окупації території [10; 11; 20].

У міжнародних документах також не передбачено можливості руйнування інженерно-технічних засобів фізичного захисту внаслідок обстрілів або ударів високоточної зброї. Сенсорні системи, бар'єри, відеоспостереження, системи електроживлення та зв'язку описуються як такі, що функціонують у нормальних умовах, а механізми резервування спрямовані на відмовостійкість у технічному, а не у бойовому розумінні [18; 25].

У наявних керівних документах МАГАТЕ не міститься положень щодо захисту зовнішніх ліній електропостачання від навмисних руйнувань, тоді як у практиці України після 2022 року саме такі атаки неодноразово створювали критичні ризики для ядерної безпеки.

Ще одним свідченням мирної орієнтації міжнародних стандартів є підхід до класифікації зон доступу та визначення рівнів охорони. Їхня логіка ґрунтується на припущенні про стабільність державних інститутів, працездатність правоохоронної системи та наявність централізованого контролю над територією. Ці вимоги не враховують реальних ризиків, що виникають у зоні активних бойових дій, де доступ до ядерного об'єкта може бути втрачений, а персонал може опинитися під фізичним чи психологічним тиском з боку збройних формувань.

Мирний характер підходів підтверджується і в науковій літературі. Як зазначають С. І. Кондратов [29] та міжнародні дослідники (наприклад, у працях щодо концептуальних розривів безпеки [32]), сучасні математичні моделі затримки порушника розраховані на умови, де держава зберігає повний контроль над територією. У наукових працях практично відсутні концепції «примусового інсайдера» в умовах окупації, коли персонал опиняється під фізичним тиском збройних формувань [13].

Таким чином, міжнародні стандарти фізичного захисту та відповідна наукова література мають низку структурних характеристик, які свідчать про їхню чітку прив’язку до мирної моделі середовища. Вони не враховують загроз повномасштабної війни, не розглядають можливості прямого воєнного впливу на ядерні об’єкти, не включають сценарії застосування важких озброєнь та не передбачають механізмів протидії військовим формуванням. Ця концептуальна обмеженість має фундаментальне значення для аналізу ефективності фізичного захисту у сучасних умовах.

З огляду на це, можна зробити висновок, що мирна парадигма, на якій базуються міжнародні стандарти фізичного захисту, є одним із ключових чинників їхньої обмеженості в умовах воєнних загроз. Огляд літератури підтверджує, що ані інституційні, ані науково-методичні підходи не враховують специфіку ризиків, що виникають у ході збройної агресії. Саме ця невідповідність між історично сформованими принципами та сучасними викликами стає центральною науковою проблемою, що обґрунтовує необхідність розроблення нових підходів до фізичного захисту ядерних об’єктів. Цим питанням присвячено наступний підрозділ, який міститиме узагальнений аналіз наукових прогалин та формування проблемного поля дослідження.

1.8 Узагальнення наукових підходів та виявлення концептуальних прогалин у сфері фізичного захисту ядерних установок

Узагальнення міжнародної та національної нормативної бази, наукових публікацій і спеціалізованих досліджень свідчить, що сучасна система фізичного захисту ядерних установок сформувалася як комплексний міждисциплінарний напрям, що поєднує технічні, організаційні, режимні та аналітичні аспекти.

Упродовж кількох десятиліть підходи до фізичного захисту розвивалися послідовно та логічно, створюючи цілісну структуру моделей загроз, функціональних принципів, технічних вимог і процедурних регламентів.

Міжнародні стандарти МАГАТЕ [2; 4], національні нормативні документи України [7; 24] та наукові дослідження різних країн формують фундамент, який забезпечив високий рівень уніфікації та узгодженості підходів до захисту ядерних об’єктів у період глобальної стабільності.

Проте всебічний аналіз літератури дозволяє виявити одну системну й концептуально важливу обставину: усі сучасні підходи до фізичного захисту ядерних установок - як міжнародні, так і в Україні - побудовані винятково на умовах мирного часу.

Це вихідне припущення, що тривалий час залишалося непорушним, визначило структуру моделей загроз, логіку функціональних елементів системи, методи оцінювання ефективності, характеристики інженерно-технічних засобів та вимоги до організаційних процедур. Його домінування виявляється як у нормативних документах (INFCIRC/225, Nuclear Security Series, Закон України «Про фізичний захист» та відповідні підзаконні акти [28; 29]), так і у наукових публікаціях, присвячених аналізу уразливостей, проєктуванню систем та оцінюванню ризиків.

Основні прогалини, які виявляються при порівнянні отриманих результатів, мають системний характер. Передусім, модель порушника у всіх міжнародних та національних документах [12; 19] ґрунтується на припущенні, що неправомірні дії здійснює група злочинців або терористів, а не регулярні збройні сили держави. Це обмеження виключає можливість аналізу сценаріїв, пов’язаних з артилерійськими ударами, ракетними обстрілами, штурмом об’єкта, застосуванням бронетехніки чи захопленням території, що стало критично важливим у сучасних умовах.

Другою важливою прогалиною є функціональна неспроможність принципу «виявлення - затримка - реагування» у воєнних умовах. Міжнародні та національні документи [27] виходять із того, що сили реагування здатні

прибути на об’єкт у визначений час, а також що інфраструктура довкола нього є доступною, а система зв’язку - стабільною. У реальності збройних конфліктів ці припущення порушуються: маршрути реагування можуть бути зруйновані, підрозділи - відсутні, а сам об’єкт - перебувати в зоні бойових дій, що повністю змінює функціональну логіку системи фізичного захисту [32].

Третьою прогалиною є відсутність методологій оцінювання вразливостей у контексті воєнних загроз. Міжнародні рекомендації МАГАТЕ та українські методики ДНТЦ ЯРБ [30] охоплюють широкий спектр технічних і організаційних ризиків, але не включають моделі руйнування інженерних мереж внаслідок бойових дій, втрату доступу до зовнішнього електроживлення, окупацію території або загрозу захоплення персоналу [6; 13; 18].

У наукових публікаціях також відсутні моделі оцінювання наслідків цілеспрямованих атак військового характеру, зокрема ударів дронами-камікадзе, застосування високоточної зброї чи деструкції критичних елементів об’єкта.

Четвертою прогалиною є недостатня інтеграція фізичного захисту в ширший контекст національної оборони, що є прямим наслідком розмежування між «nuclear security» та «national security».

Міжнародні стандарти свідомо не включають військові аспекти з огляду на їх суверенний характер, тоді як національні документи України успадкували цю модель без внесення змін, які б відображали реальні загрози, що стали актуальними після 2014 року. Це призвело до відсутності комплексних, інтегрованих підходів до захисту ядерних об’єктів у воєнний період.

Узагальнюючи огляд, можна стверджувати, що сучасна міжнародна та українська література забезпечує глибоке розуміння фізичного захисту у нормальних, неконфліктних умовах, але водночас демонструє критичну нестачу досліджень, що стосуються функціонування ядерних установок у період активних бойових дій.

Саме ця сукупність концептуальних прогалин і невідповідностей визначає наукову проблему, яка потребує вирішення. Вона пов’язана з

необхідністю переосмислення базових засад фізичного захисту в умовах воєнних загроз, а також розроблення нових моделей ризику, альтернативних підходів до оцінювання уразливостей та нових принципів інтеграції фізичного захисту в систему національної безпеки.

Це формує теоретичне підґрунтя для переходу до наступних розділів дисертації, у яких буде розглянуто методологічні підходи до побудови фізичного захисту ядерних об’єктів, аналіз ефективності існуючих систем та обґрунтування потреби у розробленні нових рішень, здатних забезпечити захист у сучасних воєнних умовах.

1.9 Методологічні наслідки деградації нормативної моделі фізичного захисту ядерних установок

Проведений аналіз міжнародних і національних нормативно-правових документів у сфері фізичного захисту ядерних установок [1; 7; 23] засвідчив, що чинна модель забезпечення фізичної безпеки ґрунтується на припущеннях, характерних для умов мирного часу та обмежених загроз некримінального характеру. Центральним елементом цієї моделі є якісна оцінка відповідності систем фізичного захисту встановленим вимогам, що формалізується через виконання нормативних процедур, організаційних заходів та технічних стандартів [24; 26].

В умовах збройного конфлікту, появи асиметричних загроз та широкого застосування безпілотних літальних апаратів як засобів розвідки й ураження, зазначений підхід виявляє свою принципову обмеженість [10; 11]. Деградація інституційного контролю, примус персоналу, руйнування або обходження інженерних бар’єрів, а також можливість дистанційного впливу без фізичного проникнення порушника на об’єкт призводять до втрати практичного сенсу традиційних категорій «відповідності», «достатності» та «нормативної адекватності» систем фізичного захисту [13; 32].

За таких умов фізичний захист перестає бути дискретною характеристикою типу «відповідає / не відповідає вимогам» і набуває імовірнісної природи. Будь-який елемент системи - засоби виявлення, канали зв’язку, людський фактор, сили реагування або технічні засоби нейтралізації - не гарантує абсолютного результату, а характеризується лише певною ймовірністю виконання своєї функції в реальних умовах загрози [27; 28].

Особливо наочно ця трансформація проявляється у випадку загроз повітряного характеру, реалізованих із застосуванням безпілотних літальних апаратів. На відміну від класичних сценаріїв наземного проникнення, для яких ключовими є часові затримки бар’єрами та фізичне реагування охорони, протидія БпЛА визначається ланцюгом імовірнісних подій: виявлення повітряної цілі, її коректна ідентифікація, своєчасне ухвалення рішення та ефективна нейтралізація [10; 30]. Порушення або відмова будь-якої з цих ланок призводить до реалізації загрози незалежно від формальної відповідності системи фізичного захисту нормативним вимогам.

У такій ситуації єдиним універсальним інструментом порівняльного аналізу альтернативних варіантів захисту та обґрунтування управлінських рішень стає кількісний ризик-орієнтований підхід [8]. На відміну від якісних експертних оцінок, він дозволяє формалізувати невизначеність, інтегрувати різнорідні фактори та оцінювати ефективність системи фізичного захисту через числові показники ймовірності успішної протидії загрозі.

У загальному вигляді ризик у сфері фізичного захисту може бути інтерпретований як функція імовірності успішної реалізації загрози та величини можливих наслідків. Такий підхід не суперечить чинним міжнародним рекомендаціям [4; 8] , проте виходить за межі їх традиційного якісного трактування та потребує розроблення спеціалізованих методик кількісного оцінювання. Саме кількісна модель дозволяє перейти від декларативного твердження про «високий рівень захищеності» до обґрунтованого визначення ймовірності виявлення загрози, ймовірності її нейтралізації та інтегрального показника ризику [27; 29].

Таким чином, деградація нормативної моделі фізичного захисту в умовах сучасних воєнних загроз об’єктивно зумовлює необхідність переходу від переважно якісного, нормативно-процедурного підходу до кількісного ризик-орієнтованого аналізу. Такий перехід не заперечує значення чинних нормативних вимог, але доповнює їх універсальним інструментарієм, який дозволяє оцінювати реальну результативність систем фізичного захисту в умовах невизначеності, асиметрії та високої динаміки загроз.

Саме в цьому контексті постає необхідність розроблення кількісної методики оцінки ймовірності виявлення та нейтралізації безпілотних літальних апаратів як складової інтегральної оцінки ризику для ядерних установок, що і становить предмет подальшого дослідження.

1.10 Висновки до Розділу 1

Проведений аналіз міжнародної нормативно-правової бази у сфері фізичного захисту ядерних установок засвідчив, що її формування відбувалося в умовах стабільного мирного середовища та ґрунтувалося на припущенні повного державного контролю над територією розміщення ядерних об’єктів.

Встановлено, що Конвенція про фізичний захист ядерного матеріалу та Поправка до неї містять принципові юридичні обмеження, які фактично виводять дії регулярних збройних сил держав зі сфери спеціального режиму фізичного захисту, що створює нормативний вакуум у разі збройної агресії або військової окупації ядерних установок.

Показано, що документи серії IAEA Nuclear Security Series (зокрема NSS No. 20, NSS No. 10, NSS No. 30-G) базуються на припущеннях інституційної стабільності, безперервності регуляторного нагляду та протидії виключно недержавним суб’єктам, що обмежує їх методологічну придатність для аналізу загроз воєнного часу.

Детальний розгляд рекомендацій INFCIRC/225/Rev.5 засвідчив, що класична концепція фізичного захисту, побудована на принципах стримування,

виявлення, затримки та реагування, втрачає концептуальну адекватність за умов застосування важкого озброєння, засобів радіоелектронної боротьби та асиметрії сил реагування.

Виявлено системну невідповідність між вимогами фізичного захисту та аварійної готовності, зумовлену відсутністю інтегрованого підходу «Security-Safety» для сценаріїв активних бойових дій, деградації інфраструктури та блокування доступу аварійних і ремонтних підрозділів.

Узагальнення результатів аналізу дозволяє дійти висновку, що чинна міжнародна архітектура фізичного захисту не забезпечує концептуальної адекватності оцінювання захищеності ядерних установок у сценаріях «держава проти держави», що формує самостійну наукову проблему.

Отримані у розділі результати створюють теоретичне та методологічне підґрунтя для подальшої систематизації воєнних загроз, формування розширеної матриці загроз і розроблення формалізованих підходів до оцінки вразливості ядерних установок, що реалізується у наступних розділах дисертаційної роботи.

2 ФІЗИЧНА ЯДЕРНА БЕЗПЕКА У ВІЙСЬКОВИЙ ЧАС

2.1 Історія нападів на ядерні об’єкти

Аналіз задокументованих випадків силового впливу на ядерні об’єкти є важливою складовою сучасних досліджень у сфері фізичного захисту, оскільки дозволяє простежити еволюцію загроз та виявити закономірності їх реалізації у різні історичні періоди [33; 34].

На відміну від нормативних і концептуальних документів, у яких традиційно переважає припущення про малоймовірність умисних нападів на ядерні установки, фактичні дані свідчать про наявність значної кількості інцидентів, у межах яких здійснювався цілеспрямований силовий вплив на інфраструктуру ядерних або радіаційно небезпечних об’єктів із використанням диверсійних, військових або гібридних засобів [11; 35]. Дослідження таких подій дозволяє сформувати комплексне уявлення про реальні механізми виникнення загроз та чинники, що сприяли матеріалізації відповідних ризиків.

Перші задокументовані випадки нападів на інфраструктуру, пов’язану з ядерними програмами, належать до періоду Другої світової війни. Найбільш показовим прикладом є диверсійна операція на заводі з виробництва важкої води в Р’юкані (Норвегія, 1943 р.), яка в науковій літературі розглядається як один із перших цілеспрямованих нападів на об’єкт, критично важливий для розвитку ядерних технологій. Знищення ключового обладнання в межах цієї операції продемонструвало, що навіть обмежені людські та матеріальні ресурси можуть завдати суттєвої шкоди ядерній програмі держави-противника.

До ранніх інцидентів також належать спроби несанкціонованого проникнення на американські дослідницькі ядерні центри «Oak Ridge» та «Brookhaven» у 1950–1960-х роках, здійснені окремими радикальними угрупованнями як форма протесту проти ядерних досліджень [33]. Незважаючи на мінімальні прямі пошкодження обладнання, ці події сприяли

переосмисленню підходів до фізичного захисту, який у той період базувався переважно на обмежених режимних та адміністративних заходах.

У наукових джерелах також згадуються випадки диверсійного впливу на об’єкти ядерної програми Південної Африки у 1980-х роках. Хоча такі інциденти мали локальний характер, вони засвідчили здатність політично мотивованих груп цілеспрямовано впливати на критичну інфраструктуру без суттєвого протидіяння з боку силових структур держави.

Період 1980-2000-х років характеризується появою найбільш резонансних випадків цілеспрямованого ураження ядерних об’єктів у світовій практиці. Найбільш відомим є авіаудар по ядерному реактору «Озирак» у 1981 році, внаслідок якого об’єкт було повністю знищено ще на стадії формування ядерної програми Іраку [36]. Даний інцидент продемонстрував, що ядерний реактор може розглядатися іншими державами як стратегічна загроза навіть до введення його в експлуатацію.

Під час операції «Буря в пустелі» у 1991 році удари було завдано по низці об’єктів ядерної інфраструктури Іраку, включно з дослідницькими реакторами та будівлями зі збагачувальним обладнанням. У цьому випадку силовий вплив здійснювався в межах широкомасштабної військової кампанії, що принципово відрізняє ці події від попередніх точкових атак.

У 2007 році було зафіксовано ураження об’єкта в районі Дейр-ез-Зор (Сирія), який розглядався як реактор, що перебував на стадії будівництва. Цей випадок став прикладом реалізації концепції випереджувальної атаки, яка, згідно з позиціями окремих держав, вважається допустимою за наявності ризику створення військового ядерного потенціалу.

Упродовж 2010-2021 років об’єкти ядерної інфраструктури Ірану, зокрема комплекс у Натанзі, зазнали серії диверсійних впливів і вибухів, що призвели до пошкодження центрифуг та допоміжних систем [37]. Характерною особливістю цих інцидентів стало поєднання фізичних та кібератак, що дало підстави говорити про формування нової категорії гібридних загроз у сфері ядерної безпеки [17; 35].

Окрему групу становлять інциденти силового впливу на об’єкти, які не є ядерними установками у класичному розумінні, але містять радіоактивні матеріали у значних кількостях. До таких подій належать вибухи на складах радіаційно небезпечних матеріалів у Сирії під час громадянської війни, а також обстріли промислових об’єктів в Іраку та Ірані, де використовувалися джерела іонізуючого випромінювання у технологічних процесах.

Окремо слід виділити напади на сховища відпрацьованого ядерного палива. У низці країн, зокрема в Ірані, фіксувалися вибухи на територіях зберігання контейнерів із високоактивними відходами, що створювало ризики порушення їх герметичності. Такі інциденти засвідчують, що навіть об’єкти, які не належать до активного ядерно-паливного циклу, можуть становити інтерес для диверсійних або військових операцій.

Сучасний етап розвитку загроз характеризується появою принципово нових форм силового впливу, які раніше не розглядалися в нормативних моделях фізичного захисту. Особливої уваги потребують випадки, коли напади на ядерні об’єкти відбуваються не як одноразові або обмежені у часі інциденти, а як елемент повномасштабного збройного протистояння [6; 32].

На основі аналізу відкритих джерел можна виокремити такі типові прояви силового впливу на ядерні об’єкти:

- систематичний вогневий вплив на енергетичну інфраструктуру, включно з лініями електропередач, підстанціями та трансформаторами, що забезпечують електропостачання систем тепловідведення;
- ведення бойових дій у безпосередній близькості до ядерних установок, що супроводжується руйнуванням промислової інфраструктури, логістичних маршрутів і засобів зв’язку;
- окупація територій розташування ядерних об’єктів, яка створює небезпечні умови для персоналу та порушує регламентовані процедури фізичного захисту, доступу і контролю за ядерними матеріалами;
- застосування безпілотних літальних апаратів для ураження окремих елементів критичної інфраструктури ядерного паливно-енергетичного

комплексу з високою точністю та обмеженими можливостями їх своєчасного виявлення традиційними засобами.

Більшість досліджень підкреслює, що силові дії щодо ядерних об’єктів мають комплексний характер, оскільки спричиняють не лише прямі фізичні пошкодження, а й суттєво ускладнюють забезпечення експлуатаційної надійності. До основних наслідків належать:

- зниження надійності систем тепловідведення внаслідок пошкодження енергопостачання;
- виснаження резервних джерел живлення через тривалі аварійні режими роботи;
- порушення технологічних регламентів через обмеження можливостей технічного обслуговування;
- зростання ймовірності людської помилки, зумовленої стресовими умовами та дефіцитом ресурсів персоналу [38].

Аналіз історичних і сучасних даних щодо силового впливу на ядерні та радіаційно небезпечні об’єкти дає підстави стверджувати, що характер загроз суттєво змінився порівняно з тими сценаріями, які закладалися у традиційні нормативні та концептуальні моделі фізичного захисту [19; 32]. Якщо у другій половині XX століття напади мали переважно диверсійний або точковий превентивний характер, то починаючи з XXI століття фіксуються випадки комплексного та тривалого силового впливу із використанням широкого спектра військових засобів.

У контексті сучасних збройних конфліктів ядерні об’єкти перестали бути виключно теоретичною ціллю. Наявні дані свідчать про можливість систематичного вогневого впливу, окупації територій, втрати зовнішнього електропостачання, а також функціонування в умовах деградації систем радіаційного контролю та аварійного реагування. Це зумовлює необхідність перегляду уявлень про природу загроз та розроблення методологічних підходів, здатних забезпечити стійкість ядерних установок до широкого спектра силових

дій, включно з тими, що раніше вважалися малоймовірними або нереалістичними.

2.2 Хорологія нападів на ядерні об’єкти України

О 6:41 за центральноєвропейським часом 24 лютого 2022 року Державна інспекція ядерного регулювання України (ДІЯРУ), виконуючи функції національного компетентного органу відповідно до Конвенції про оперативне оповіщення про ядерну аварію 1986 року, звернулася до керівника реагування на надзвичайні ситуації Інцидентно-аварійного центру МАГАТЕ (IEC). Вона поінформувала IEC про перебування російських військ на території Чорнобильської атомної електростанції (АЕС), а також про запровадження воєнного стану на всій території України [5; 6].

Увечері того ж дня ДІЯРУ повідомила, що внаслідок військового нападу всі об’єкти Чорнобильської АЕС були захоплені російськими військовими формуваннями [18; 31].

Цей перший напад став лише початком подальших атак. МАГАТЕ здійснило ґрунтовне документування подій, засвідчивши, що в період з лютого 2022 року по лютий 2023 року численні ядерні об’єкти України зазнавали різних форм ворожого військового впливу (Таблиця 3.1) [6; 39].

Таблиця 2.1 – Характеристики та фрми військового впливу впливу на ядерні установки

Об’єкт	**Характеристика об’єкта**	**Характер та форма впливу**
ДСП «Чорнобильська АЕС»	- Шість енергоблоків (енергоблоки №1-3 зупинені; енергоблок №4 частково зруйнований унаслідок аварії 26 квітня 1986 р.; енергоблоки №5-6 не введені в експлуатацію) • Два сховища відпрацьованого ядерного палива (СВЯП-1, СВЯП-2) - Об’єкти поводження з радіоактивними відходами на промисловому майданчику АЕС та в зоні відчуження	Окупація об’єкта: 24 лютого - 31 березня 2022 р.

Продовження таблиці 2.1

Об’єкт	**Характеристика об’єкта**	**Характер та форма впливу**
Філія «ВП «Хмельницька АЕС»	- Два діючі енергоблоки - Два енергоблоки на стадії будівництва	Пошкодження ліній електропередач та інші порушення зовнішнього електропостачання
Філія «ВП Рівненська АЕС»	Чотири діючі енергоблоки	Пошкодження ліній електропередач та інші порушення зовнішнього електропостачання
Філія «ВП Південноукраїнська АЕС»	Три діючі енергоблоки	Обстріли Пошкодження ліній електропередач та інші порушення зовнішнього електропостачання
Філія «ВП Запорізька АЕС»	Шість енергоблоків (експлуатувалися станом на 23 лютого 2022 р.; усі зупинені до 10 вересня 2022 р.)	Обстріли Пошкодження ліній електропередач та інші порушення зовнішнього електропостачання Окупація: з 4 березня 2022 р. Незаконна анексія: з 4 жовтня 2022 р.
Харківський фізико-технічний інститут	Підкритична нейтронна установка	Обстріли
Харківська міжоблосна філія ДСП «Об’єднання «Радон»	Об’єкт поводження з радіоактивними відходами	Пошкодження внаслідок бойових дій
Київська міжоблосна філія ДСП «Об’єднання «Радон»	Об’єкт поводження з радіоактивними відходами	Ракетний удар

Проте, низка істотних відмінностей вирізняє події в Україні серед попередніх випадків нападів на ядерні об’єкти. Насамперед, жоден із попередніх військових нападів не був спрямований безпосередньо на велику діючу атомну електростанцію, таку як Запорізька АЕС, що має значні обсяги опроміненого ядерного палива як у активних зонах реакторів, так і в сховищах, розміщених безпосередньо на майданчику. Це становить принципову відмінність порівняно з усіма попередніми атаками [32; 40].

Майданчики Запорізької та Чорнобильської АЕС включають такі об’єкти, як діючі ядерні енергоблоки та сховища відпрацьованого (опроміненого) ядерного палива, що означає, що сукупна кількість радіоактивних матеріалів, наявних на цих об’єктах, є істотно більшою, ніж на будь-яких ядерних установках, які зазнавали нападів у попередні періоди.

Варто відзначити, що напади на ядерні установки, що мали місце до 2022 року, носили цілеспрямований характер і були безпосередньо спрямовані саме на ці об’єкти. Натомість у 2022 році збройні сили рф здійснювали масовані атаки на широкий спектр промислових об’єктів України, включно з об’єктами енергетичної інфраструктури та електроенергетичною мережею загалом [11; 41].

Поза майданчикові лінії електропостачання є необхідними не лише для передачі електроенергії, виробленої атомними електростанціями, до об’єднаної енергосистеми України, але й для забезпечення самих АЕС електроенергією, потрібною для реалізації їхніх функцій безпеки. Навіть у разі зупинення атомної електростанції вона протягом тривалого часу потребує зовнішнього електропостачання та водопостачання для відведення тепла і охолодження ядерного палива в активній зоні реактора.

Так, безпосередньо після зупинення реактора ядерне паливо в енергоблоці потужності, співставної з енергоблоками Запорізької АЕС, продовжує виділяти приблизно 200 мегаватів (МВт) теплової енергії внаслідок залишкового тепловиділення продуктів поділу. Втрата зовнішнього електропостачання або кінцевого поглинача тепла установки (наприклад, води з річки або моря) потенційно може призвести до наслідків, подібних до аварії на атомній електростанції «Фукусіма-Даїчі» у 2011 році [42].

Упродовж 2022 року підключення українських атомних електростанцій до поза майданчикових джерел електропостачання неодноразово переривалося (див. Табл. 2.1). Зокрема, 23 листопада 2022 року ракетні удари Російської Федерації спричинили зниження частоти в об’єднаній енергосистемі України, що, своєю чергою, призвело до автоматичного відключення від електромережі Рівненської, Південноукраїнської та Хмельницької атомних електростанцій [18; 43].

2.3 Правове регулювання питання атак на ядерні об’єкти

Під час збройного конфлікту ризик пошкодження ядерних установок є надзвичайно високим, особливо у випадках, коли бойові дії відбуваються безпосередньо на майданчику ядерної установки або в його безпосередній близькості, що створює значну загрозу викиду радіоактивних речовин. Пошкодження таких об’єктів може бути спричинене як прямим силовим впливом, так і опосередковано - через порушення вимог ядерної безпеки або фізичного захисту [21; 44]. Усвідомлення масштабності цих ризиків зумовило їх визнання в рамках міжнародного гуманітарного права (МГП), яке передбачає декілька рівнів правового захисту ядерних установок.

По-перше, у разі міжнародного (міждержавного) збройного конфлікту норми звичаєвого міжнародного гуманітарного права, а також Додатковий протокол I 1977 року до Женевських конвенцій 1949 року, визначають атомні електростанції та інші пов’язані з ними ядерні об’єкти, зокрема сховища відпрацьованого ядерного палива, як цивільні об’єкти [45; 46]. Відповідно, вони не повинні бути об’єктами спрямованих військових дій.

У разі виникнення сумнівів щодо того, чи призначена конкретна ядерна установка для цивільних або військових цілей, вона має презюмуватися як цивільний об’єкт. З огляду на потенційні наслідки радіаційного викиду, зобов’язання міжнародного гуманітарного права вживати всіх можливих заходів для збереження цивільних об’єктів набуває у цьому контексті особливої ваги [47].

По-друге, окрім загального захисту, який міжнародне гуманітарне право надає всім цивільним ядерним установкам, атомні електростанції користуються спеціальним захистом від нападу у випадках, коли такий напад може спричинити вивільнення небезпечних сил і, як наслідок, завдати значних втрат серед цивільного населення [45, ст. 56]. Цей захист зберігається навіть у разі, якщо атомна електростанція буде визнана військовим об’єктом.

У ході неміжнародного (внутрішньодержавного) збройного конфлікту, на який поширюється дія Додаткового протоколу II 1977 року до Женевських конвенцій, заборона нападу застосовується навіть у випадку розміщення військового об’єкта в безпосередній близькості до атомної електростанції [48].

У разі міжнародного збройного конфлікту спеціальний захист, передбачений Додатковим протоколом I для атомних електростанцій або військових об’єктів, розташованих поблизу них, може бути втрачений, якщо атомна електростанція забезпечує електропостачання, яке здійснюється на регулярній, суттєвій і безпосередній основі з метою підтримки військових операцій, і якщо напад на станцію є єдиним можливим способом припинення такої підтримки [46; 49].

Додатковий протокол I також покладає на обидві сторони міжнародного збройного конфлікту обов’язок уживати заходів для захисту цивільного населення. Відповідно до одного з правових тлумачень відповідних положень, запропонованого фахівцями Міжнародного комітету Червоного Хреста (МКЧХ), Женевські конвенції та норми звичаєвого міжнародного права вимагають від сторони конфлікту, яка здійснює контроль над атомною електростанцією, забезпечувати ядерну безпеку та фізичний захист на такому об’єкті як першочергове завдання [50].

Згідно з цим тлумаченням, відповідні заходи мають включати:

- забезпечення функціонального технічного обслуговування критично важливих компонентів, зокрема резервних джерел електроживлення;
- гарантування доступу оперативного персоналу до майданчика електростанції та/або її критичних елементів і можливості виконання службових обов’язків без необґрунтованих обмежень, фізичного чи психологічного примусу або будь-яких інших форм незаконного поводження, а також забезпечення належних умов харчування та гігієни;
- у разі неможливості гарантування безпечної та захищеної експлуатації установки - часткову або повну зупинку атомної електростанції.

Разом із тим договірне міжнародне гуманітарне право не вважає передбачені ним механізми захисту атомних електростанцій і, зокрема, інших ядерних установок достатніми. У Додатковому протоколі І державам пропонується «укладати між собою додаткові угоди з метою забезпечення посиленого захисту об'єктів, що містять небезпечні сили». У правовій доктрині та практиці держав обговорювалися, а в окремих випадках і реалізовувалися, різні формати такого додаткового захисту, зокрема наведені нижче.

2.3.1 Демілітаризовані зони та угоди про ненапад

Під час збройних конфліктів або у мирний час держави можуть розглядати можливість укладення між собою двосторонніх або багатосторонніх угод з метою створення демілітаризованих зон, які сторони конфлікту зобов'язуються не окуповувати, не використовувати у військових цілях та не піддавати нападам. Додатковий протокол І до Женевських конвенцій пропонує загальну правову рамку для формування таких зон, яка передбачає їх адаптацію сторонами конфлікту відповідно до конкретних потреб і обставин [45; 46].

Унікальним прикладом реалізації подібного підходу є Угода між Індією та Пакистаном про ненапад 1988 року [51]. Відповідно до цієї угоди, обидві держави не лише зобов'язуються утримуватися від будь-яких форм нападу на ядерні установки одна одної, незалежно від їх типу, але й щорічно обмінюватися географічними координатами таких об'єктів [34].

У цьому ж напрямі у 1993 році один із американських правознавців запропонував наділити Міжнародне агентство з атомної енергії (МАГАТЕ) так званим «правом ініціативи» для укладення ad hoc угод, спрямованих на захист конкретних об'єктів, що перебувають під гарантіями МАГАТЕ, під час збройного конфлікту [52; 53]. Запропонований механізм передбачав надання Генеральному директору МАГАТЕ повноважень на ведення прямих переговорів зі сторонами збройного конфлікту з метою забезпечення тимчасового, але дієвого правового захисту таких об'єктів.

2.3.2 Досвід Договору Пеліндаба

Африканський договір про зону, вільну від ядерної зброї 1996 року (Договір Пеліндаба) є унікальним серед міжнародних договорів, що встановлюють зони, вільні від ядерної зброї (NWFZ), оскільки він прямо забороняє напади на ядерні установки [54]. Зокрема, у договорі зазначено: «Кожна Сторона зобов'язується не вчиняти, не сприяти та не заохочувати будь-які дії, спрямовані на здійснення збройного нападу - із застосуванням звичайних або інших засобів - проти ядерних установок у межах Африканської зони, вільної від ядерної зброї» [54, ст. 11].

Договір Пеліндаба містить низку положень, які мають істотне значення для загального обговорення правових механізмів заборони нападів на ядерні установки. У ході переговорів сторони розглядали питання щодо можливості обмеження сфери дії такого захисту. Один із варіантів передбачав поширення заборони на напади лише на ядерні установки, розташовані в державах - учасницях договору, і лише на ті об'єкти, що перебувають під гарантіями МАГАТЕ та, відповідно, «сертифіковані» як такі, що використовуються виключно в мирних цілях [55].

Згідно з позицією спостерігачів від Сполучених Штатів Америки, такі обмеження могли б усунути ризик зловживань, за яких держава могла б використовувати положення договору з метою прикриття військових об'єктів, розміщуючи на них радіоактивні матеріали та заявляючи про їхній захищений статус. Проте в підсумку учасники переговорів відхилили цю пропозицію, дійшовши висновку, що захист від нападу має поширюватися на всі ядерні установки в усіх державах, розташованих у межах зони, вільної від ядерної зброї [56].

2.3.3 Багатосторонні конвенції

Пропозиції щодо укладення багатосторонніх конвенцій, які б прямо забороняли напади на ядерні установки, неодноразово висувалися в різних формах. Такі ініціативи відображають усвідомлення того, що рівень захисту, передбачений Женевськими конвенціями та їхніми Додатковими протоколами, є недостатнім для ефективного запобігання ризикам, пов'язаним із воєнними діями проти ядерних об'єктів [49; 57].

У 1979 році Сполучені Штати Америки та Радянський Союз спільно подали на розгляд Комітету з роззброєння в Женеві (перейменованого у 1984 році на Конференцію з роззброєння) текст конвенції про заборону радіологічної зброї, яка, серед іншого, була спрямована на обмеження дій, що могли б призвести до умисного радіологічного ураження, включно з потенційними атаками на ядерні та радіаційно небезпечні об'єкти [58] .

Швеція, за підтримки інших нейтральних і неприєднаних держав, висунула пропозицію внести зміни до проєкту конвенції шляхом включення до нього прямої заборони на напади на ядерні установки, зокрема на реактори, заводи з переробки ядерного палива, а також сховища відпрацьованого ядерного палива і радіоактивних відходів, що перевищують визначений розмір. Однак Сполучені Штати Америки відмовилися прийняти цю поправку, тоді як Швеція та держави, що її підтримували, відмовилися зняти свою пропозицію. Унаслідок цього переговорний процес щодо відповідної конвенції так і не був розпочатий [34; 59].

У 1992 році один із американських науковців у галузі міжнародного права запропонував конвенцію про захист ядерних установок, що перебувають під гарантіями МАГАТЕ, від будь-яких нападів, спрямованих на їх знищення як потенційних джерел ядерного матеріалу, придатного для створення зброї [53].

У 2003 році колишній президент Асоціації ядерного права (Nuclear Law Association) висунув не менш радикальну ініціативу, яка передбачала

запровадження «повномасштабного захисту за будь-яких обставин усіх цивільних ядерних установок» [60].

2.4 Ядерна захищеність і ядерна безпека в надзвичайних обставинах: сім стовпів Генерального директора МАГАТЕ

Ядерна захищеність охоплює «запобігання, виявлення та реагування на кримінальні або навмисні несанкціоновані дії, пов'язані з ядерним матеріалом, іншими радіоактивними матеріалами, відповідними установками або пов'язаною діяльністю» [4]. Окрема галузь - ядерна безпека - спрямована на досягнення та підтримання «належних умов експлуатації, запобігання аваріям і пом'якшення їхніх наслідків, що забезпечує захист персоналу, населення та навколишнього середовища від надмірних радіаційних ризиків» [21].

Різницю між ядерною безпекою та ядерною захищеністю часто узагальнюють таким чином: «безпека полягає в утриманні джерел іонізуючого випромінювання подалі від людей, тоді як захищеність - в утриманні людей подалі від джерел випромінювання» [61]. На ядерній установці, як у режимі нормальної експлуатації, так і в умовах надзвичайних подій, ядерна захищеність створює умови для досягнення цілей ядерної безпеки, затримуючи (через виявлення та реагування) або стримуючи осіб зі зловмисними намірами.

Це має особливе значення для атомних електростанцій. Серед об'єктів ядерно-паливного циклу саме ядерні реактори та сховища відпрацьованого палива містять найбільші запаси високоактивних радіоактивних матеріалів. У випадку АЕС ці матеріали зосереджені в порівняно невеликому, але надзвичайно енергоємному об'ємі активної зони реактора. Поєднання високої енергії та значної радіоактивності в обмеженому просторі означає, що у разі порушення герметичності оболонки та інших бар'єрів потенціал радіоактивного викиду є надзвичайно високим [42]. Це особливо актуально у ситуаціях, коли інші системи ядерної безпеки виводяться з ладу, як це сталося, зокрема, під час аварії на АЕС «Фукусіма-Даїчі».

2 березня 2022 року, через кілька днів після першого нападу на ядерну установку в Україні, Рада керуючих МАГАТЕ провела засідання, присвячене обговоренню «наслідків для ядерної безпеки, ядерної захищеності та гарантій у зв'язку з конфліктом в Україні внаслідок військової операції Російської Федерації, що розпочалася 24 лютого» [62]. У вступному слові Генеральний директор МАГАТЕ Рафаель Маріано Гроссі підсумував інформацію про атаки російських військ на українську ядерну інфраструктуру, відомі на той момент. Він також зазначив, що, попри надзвичайні обставини, ядерні установки продовжують працювати «нормально» з технічної точки зору, однак наголосив, що «немає нічого нормального в тих умовах, за яких фахівці на чотирьох атомних електростанціях України змушені підтримувати роботу реакторів, які виробляють половину електроенергії країни» [63].

У цьому ж виступі Гроссі представив концепцію, яка згодом отримала назву «сім незамінних стовпів ядерної безпеки та ядерної захищеності» (див. рис. 2.1) [39].

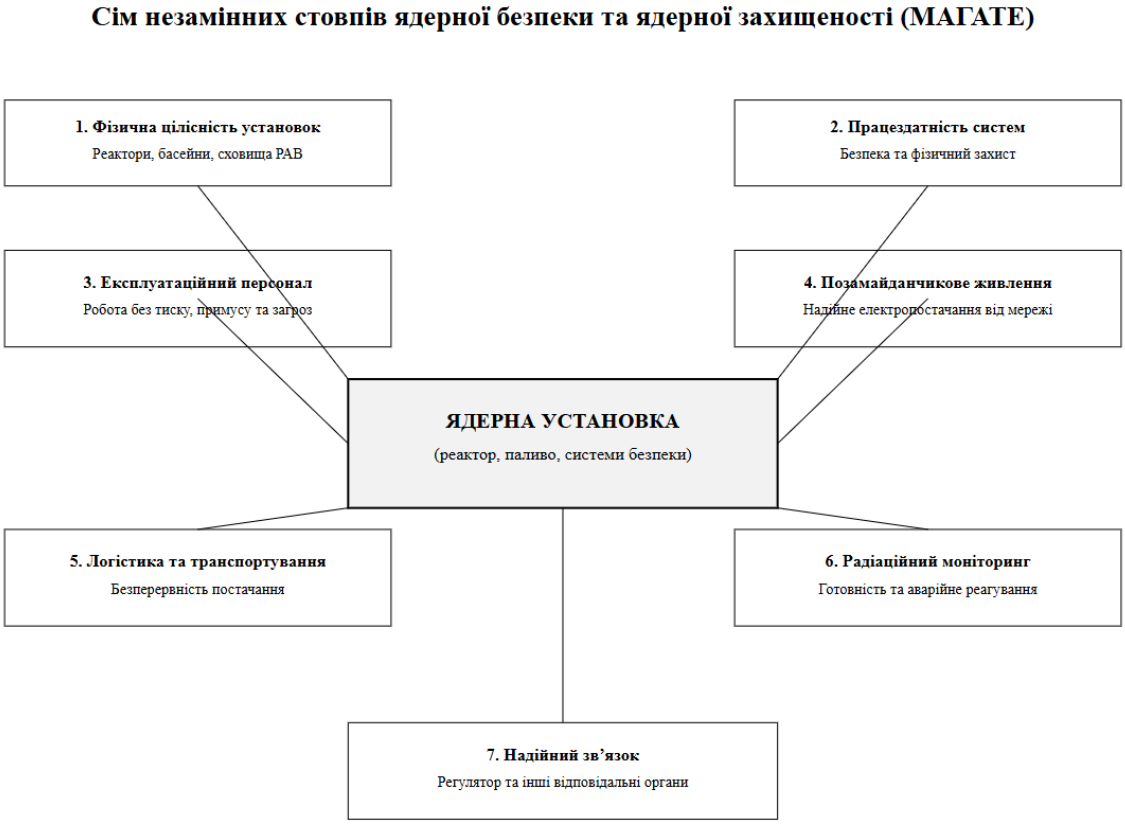

Рисунок 2.1 – Сім незамінних стовпів ядерної безпеки та ядерної захищеності (МАГАТЕ)

Ці стовпи ґрунтуються на чинних стандартах МАГАТЕ з ядерної безпеки та керівних документах з ядерної захищеності і частково перегукуються з рекомендаціями Міжнародного комітету Червоного Хреста, згаданими вище. Зокрема, Гроссі зазначив, що «в основі ядерної безпеки лежать три ключові функції: утримання (containment), керування (control) та охолодження (cooling)», підтримання яких і потребує реалізації семи запропонованих принципів або «стовпів».

Концепція семи стовпів отримала широке схвалення міжнародної спільноти. Запропонована менш ніж через тиждень після першого нападу на ядерну установку в Україні - Чорнобильську АЕС - і за два дні до атаки на Запорізьку АЕС, вона стала оперативно сформованою концептуальною основою для подальших дій як МАГАТЕ, так і окремих держав [6; 64]. Водночас цю концепцію не слід розглядати як вичерпний перелік принципів, принаймні без подальшої деталізації з боку МАГАТЕ.

Так, наприклад, функція охолодження, на яку вказує Гроссі, передбачає, серед іншого, наявність кінцевого поглинача тепла - такого як велика маса води або атмосфера. Такий поглинач може використовуватися як для охолодження конденсаторів турбін під час нормальної експлуатації АЕС, так і для відведення тепла після зупинки реактора. Деякі експерти зазначають, що забезпечення доступності кінцевого поглинача тепла може заслуговувати на окремий «стовп» поряд із вимогою щодо надійного позамайданчикового електропостачання [43].

З операційної точки зору сім стовпів відіграли ключову роль для МАГАТЕ та держав-донорів під час структурування допомоги та реагування на атаки на ядерні установки в Україні. З стратегічної точки зору ця концепція може розглядатися як передвісник адаптації міжнародної системи ядерної захищеності до принципово нового, раніше майже не охопленого сценарію - функціонування національних режимів ядерної захищеності в умовах атак і дестабілізації, здійснюваних державами, а не недержавними акторами.

Варто підкреслити, що навіть у разі міжнародного збройного конфлікту ядерна захищеність за своєю суттю зосереджена на протидії зловмисним діям

окремих осіб і недержавних груп, а не збройним силам держави. Проте в умовах міжнародного збройного конфлікту або інших надзвичайних обставин система ядерної захищеності має продовжувати функціонувати, що неминуче потребує її адаптації.

З метою реагування на такі сценарії концепція семи стовпів прямо об'єднує ядерну безпеку, ядерну захищеність та готовність до аварійного реагування в межах єдиного концептуального підходу (див. рамку 1). Такий підхід є логічним, необхідним і узгоджується з чинною політикою МАГАТЕ. Зокрема, протягом низки років МАГАТЕ розвиває концепцію інтерфейсу між ядерною безпекою та ядерною захищеністю, який визначається як «аспекти вимог і заходів у сфері безпеки та захищеності, що можуть взаємно доповнювати або, навпаки, нейтралізувати один одного» [65].

Два провідні консультативні органи МАГАТЕ - Консультативний комітет з ядерної захищеності (AdSec) та Міжнародна група з ядерної безпеки (IAEA) - розпочали спільну роботу над цим питанням ще у 2017 році. У 2018 році Генеральна конференція та Рада керуючих МАГАТЕ офіційно доручили Секретаріату МАГАТЕ продовжити розвиток цієї концепції у співпраці з державами-членами [66].

Концепція семи стовпів, з огляду на обставини, була впроваджена у прискореному режимі. На відміну від інших документів МАГАТЕ з ядерної безпеки та ядерної захищеності, які розробляються в межах ретельно регламентованого процесу за участю та за згодою держав-членів, сім стовпів були представлені безпосередньо Генеральним директором у його зверненні до Ради керуючих. Очевидно, що ця концепція потребуватиме подальшого опрацювання та деталізації МАГАТЕ за участю держав-членів.

Наступні етапи її розвитку можуть вимагати відповіді, зокрема, на такі питання:

- який статус має концепція семи стовпів щодо чинних керівних документів МАГАТЕ з ядерної безпеки, ядерної захищеності та аварійного реагування;

- який вплив вона повинна мати на національні закони та нормативно-правові акти держав-членів МАГАТЕ;
- як забезпечити, щоб елементи систем ядерної безпеки та ядерної захищеності, не згадані безпосередньо в концепції семи стовпів, не були відсунуті на другий план;
- хто несе відповідальність за реалізацію семи стовпів у випадках, коли de jure та de facto контроль над ядерною установкою належить різним суб'єктам (наприклад, у разі окупації або анексії).

2.5 Національні режими ядерної захищеності та розподіл відповідальності за реагування на загрози

Ключовим принципом міжнародної системи ядерної захищеності є твердження про те, що «відповідальність за ядерну захищеність у межах держави повністю покладається на державу» [4]. Зміст такої відповідальності полягає в тому, що кожна держава має вживати заходів для забезпечення захищеності ядерного матеріалу, інших радіоактивних матеріалів, пов'язаних установок і пов'язаної діяльності в межах своєї юрисдикції. Реалізація цього обов'язку здійснюється шляхом створення та підтримання національного режиму ядерної захищеності. У найзагальнішому вигляді національний режим ядерної захищеності включає: (а) законодавство та нормативно-правові акти; (б) інституції та організації, відповідальні за їх виконання; і (в) заходи, спрямовані на запобігання несанкціонованим діям або на їх виявлення та реагування (повне визначення наведено в таблиці 2.2).

Із цього випливає, що в межах національного режиму ядерної захищеності можна виокремити три типи національних суб'єктів, кожен з яких має відмінні види відповідальності щодо його реалізації. Перший тип - це «держава» в широкому розумінні, тобто найвищий рівень виконавчої влади, законодавча та судова гілки, які несуть відповідальність за управління національною безпекою, міжнародними відносинами та збройними силами,

особливо в критичних ситуаціях, таких як збройний конфлікт або інші надзвичайні події. Другий тип становлять «компетентні органи», тобто державні організації, які держава офіційно визначає для виконання функцій у сфері ядерної захищеності. До таких органів можуть належати, зокрема, регуляторні органи, правоохоронні структури, митні та прикордонні органи, розвідувальні й безпекові служби, а також органи охорони здоров'я. Конкретна інституційна конфігурація перших двох типів суб'єктів - держави та компетентних органів - є унікальною для кожної країни, однак, принаймні в принципі, у межах кожної держави завжди існує суб'єкт, який виконує відповідні функції. Третій тип - оператор будь-якої установки або діяльності, пов'язаної з ядерними чи іншими радіоактивними матеріалами, наприклад компанія, що володіє та експлуатує атомну електростанцію [4; 7].

Для визначення того, що вважається нормальними умовами з позицій ядерної захищеності, МАГАТЕ та багато національних органів застосовують поняття «проєктна загроза» (design basis threat, DBT). Воно описує потенційну «загрозу» (тобто противника/порушника), проти якої системи та заходи ядерної захищеності, включно з фізичним захистом об'єкта, проєктуються як ефективні (таблиця 2.2) [19].

Таблиця 2.2 – Потенційні «загрози» для протидії яким створюється система фізичного захисту

Суб'єкт	**Нормальні умови**	**Надзвичайні обставини**
Держава	Управління діяльністю компетентних органів у процесі розроблення національної оцінки загроз ядерній захищеності та визначення проєктної загрози (DBT)	Реагування на загрози ядерній захищеності, що виходять за межі проєктної загрози (Beyond DBT)
Компетентні органи	Участь у розробленні національної оцінки загроз у сфері ядерної захищеності	

Продовження таблиці 2.2

Суб'єкт	**Нормальні умови**	**Надзвичайні обставини**
Встановлення вимог до систем і заходів ядерної захищеності для операторів ядерних установок	Функції та обсяг відповідальності чітко не визначені в документі *IAEA Nuclear Security Series No. 10-G (Rev. 1)*	
Оператор	Виконання вимог щодо систем і заходів ядерної захищеності для протидії загрозам, визначеним у межах DBT	Виконання вимог щодо систем і заходів ядерної захищеності для загроз у межах DBT
Сприяння державі у реагуванні на загрози, що виходять за межі DBT		
Сприяння державі в пом'якшенні наслідків надзвичайних подій		

Якщо загроза перебуває в межах параметрів DBT - наприклад, коли особу затримано під час спроби викрасти паливні таблетки з місця роботи, - ситуація, хоча й є серйозною, все ще може вважатися «нормальною» у тому сенсі, що вона була передбачена під час планування.

Держава здійснює управління компетентними органами в процесі проведення національної оцінки загроз у сфері ядерної захищеності та розроблення DBT. За нормальних умов оператор установки несе відповідальність за ядерну захищеність об'єкта та ядерного (або іншого радіоактивного) матеріалу на ньому (або під час транспортування), а також за ядерну безпеку і радіаційний захист [67]. Оператор має впровадити системи та заходи ядерної захищеності для протидії спектру сценаріїв нападу, передбачених у DBT. Проєктування і конфігурація таких систем та заходів повинні відповідати конкретним вимогам, що формуються регуляторними органами на підставі їхнього розуміння параметрів DBT.

Розподіл відповідальності у сфері ядерної захищеності закономірно змінюється в надзвичайних обставинах (див. табл. 2.2). Під час надзвичайних

подій держава бере на себе відповідальність за реагування на загрози, які не охоплюються DBT, і, відповідно, не можуть бути віднесені виключно до сфери відповідальності оператора. Водночас відповідальність оператора в надзвичайних умовах не припиняється. По-перше, очікується, що оператор сприятиме державі в протидії загрозам «поза DBT», а також у подальшому пом'якшенні наслідків [12; 68]. По-друге, провідні експерти у сфері ядерної захищеності, опитані SIPRI, погоджуються, що - наскільки це є можливим - оператор має залишатися відповідальним за протидію загрозам у межах DBT навіть за надзвичайних обставин, включно зі збройним конфліктом [69].

Публічно доступної інформації щодо того, наскільки в окремих країнах здійснено підготовку до надзвичайних обставин, небагато. Водночас опитані експерти вказують, що питання дій і розподілу відповідальності між різними національними (та міжнародними) суб'єктами ядерної захищеності в умовах надзвичайних подій - на національному, регіональному чи глобальному рівнях, включно зі збройними конфліктами - залишається недостатньо розробленим. Як пояснив один із провідних експертів із країни з розвинутими спроможностями у сфері ядерної захищеності, «хоча оператор має первинну відповідальність за захист від загроз у межах DBT, а держава - від загроз поза DBT, у більшості країн (включно з моєю) держава насправді не здійснила серйозної підготовки до реального реагування на загрози поза DBT» [69]. Попри те, що держави мають активніше вирішувати цю проблему, керівні матеріали МАГАТЕ також потребують подальшого розвитку, аби доповнювати національні зусилля. У цьому контексті корисним може бути використання досвіду підходів до захисту ядерних установок від потенційних зовнішніх подій (наприклад, вулканічної активності, зовнішніх пожеж та вибухів, радіологічних небезпек від інших установок і, зокрема, ударів повітряних суден) на етапах проєктування, будівництва та експлуатації об'єкта [70].

2.6 Планування реагування у сфері ядерної захищеності на надзвичайні події

Існує об’єктивна потреба у структурованому підході до планування дій суб’єктів ядерної захищеності в умовах надзвичайних подій або у відповідь на загрози ядерній захищеності, що виходять за межі проєктної загрози (DBT). Такий підхід має ґрунтуватися на чотирьох ключових елементах.

По-перше, підхід до планування має враховувати, що надзвичайні події, які суттєво впливають на ядерну захищеність, не обов’язково супроводжуються власне загрозами ядерній захищеності. Відповідно до визначення МАГАТЕ, загроза ядерній захищеності - це:

особа або група осіб, які мають мотивацію, намір і спроможність вчинити кримінальні або навмисні несанкціоновані дії, пов’язані з ядерним матеріалом, іншими радіоактивними матеріалами, відповідними установками або пов’язаною діяльністю, або інші дії, які держава визначає як такі, що негативно впливають на ядерну захищеність [4; 19].

По суті, «загроза - це гіпотетичний противник, проти якого проєктуються заходи захищеності». Надзвичайні події, такі як пандемія COVID-19 або масштабні природні катастрофи (наприклад, землетрус із подальшим цунамі), мають специфічні наслідки для ядерної захищеності, але не створюють нових противників, окрім тих, що вже враховані в межах DBT [71]. У післяпандемічних дослідженнях почали аналізуватися уроки функціонування режимів ядерної захищеності в умовах надзвичайних подій, які змінюють операційне середовище, але не змінюють набір загроз або противників, на які ці режими мають реагувати [72].

Подібним чином, у разі збройного конфлікту атака, не спрямована безпосередньо на ядерну установку, все одно може мати суттєвий вплив на ядерну захищеність. Наприклад, пошкодження національної енергетичної інфраструктури може призвести до втрати електроживлення систем

відеоспостереження та інших елементів системи фізичного захисту на ядерному об’єкті.

По-друге, хоча це дослідження зумовлене необхідністю розуміння впливу військового вторгнення та війни на національні режими ядерної захищеності, слід визнати, що загрози ядерній захищеності поза межами DBT існують і в інших сценаріях. Окрім міждержавних воєн, до таких сценаріїв належать колапс держави (failed state) та масштабні прояви громадянських заворушень. Інциденти, пов’язані із загрозами поза DBT, доцільно класифікувати за масштабом, оскільки саме масштаб визначає коло задіяних суб’єктів і, відповідно, розподіл відповідальності.

Одним із можливих підходів є використання логіки міжнародного гуманітарного права та поділ інцидентів, що впливають на ядерну захищеність, на міжнародні та національні. До міжнародних інцидентів, зокрема, належать міжнародні збройні конфлікти, тобто воєнні дії між двома або більше державами. Національні інциденти можуть включати неміжнародні збройні конфлікти - воєнні дії між державою та недержавними збройними формуваннями або виключно між такими формуваннями, зокрема в умовах масових заворушень або державного колапсу [46]. Остання категорія частково перетинається із загрозами в межах DBT, яка зазвичай охоплює збройні групи до певного розміру.

По-третє, головними пріоритетами національних режимів ядерної захищеності під час збройних конфліктів мають бути:

- запобігання радіоактивному викиду з ядерних установок;
- недопущення виходу ядерних та інших радіоактивних матеріалів з-під регуляторного контролю.

Національне планування на випадок збройних конфліктів - як міжнародних, так і неміжнародних - має враховувати сценарії як навмисних, так і ненавмисних інцидентів. Наприклад, нападник може свідомо прагнути спричинити радіоактивний викид з атомної електростанції, тоді як війна може призвести до загальних порушень у ланцюгах постачання або в

енергозабезпеченні, що матиме ненавмисні наслідки для ядерної установки. На етапі планування держава має визначити, чи повинні оператори ядерних установок нести певну відповідальність за зменшення вразливості, принаймні щодо ненавмисних впливів у ході воєнних дій (наприклад, випадкових артилерійських уражень або тривалих втрат позамайданчикового електропостачання) [69]. Керівні документи МАГАТЕ з цього питання є лаконічними, однак допускають можливість покладення на оператора такої ролі.

По-четверте, має бути створена стійка система планування та національних спроможностей реагування для трьох ключових сценаріїв, визначених вище:

- надзвичайні події, що впливають на ядерну захищеність, але не створюють загроз поза DBT (наприклад, пандемія або природна катастрофа);
- міжнародні збройні конфлікти;
- неміжнародні (внутрішньодержавні) збройні конфлікти.

Певні елементи такого планування можуть існувати в окремих державах для окремих сценаріїв, однак у цілому це радше виняток, ніж правило. Планування у сфері ядерної захищеності для кожного з трьох сценаріїв має, в ідеалі, відповідати таким вимогам:

Всеосяжність - планування повинно охоплювати всі релевантні функції, суб’єкти та максимально можливу кількість потенційних сценаріїв.

Формалізація - планування має бути належним чином оформлене, а його елементи розподілені між відповідними державними органами. Дослідження показують, що навіть у державах із розвинутими режимами ядерної захищеності не всі органи усвідомлюють власні повноваження та обов’язки [69; 73].

Юридична обов’язковість - відповідний план має бути ухвалений на належному рівні з відповідною юридичною силою, а визначені в ньому повноваження та обов’язки органів влади повинні бути обов’язковими до виконання [73].

Регулярне тестування - план має систематично перевірятися в межах спеціалізованих навчань і тренувань, а результати таких заходів повинні використовуватися для його оновлення та вдосконалення.

2.7 Міжнародний режим фізичної ядерної безпеки в умовах збройних конфліктів: концептуальні засади адаптації та напрями вдосконалення

2.7.1 Проектна загроза у військовий час

У сучасній літературі пропонується формальна класифікація сценаріїв, що виходять за межі проектної загрози, але можуть бути формалізовані у національних режим безпеки країни, а саме:

- сценарії надзвичайних ситуацій невійськового характеру, які потребують залучення додаткових сил та засобів (стихійні лиха тощо);
- сценарії міжнародного збройного конфлікту, у яких територія ядерного об’єкта зазнає вогневого впливу, обмеження доступу або окупації;
- сценарії неміжнародних конфліктів (масштабних заворушень), що створюють ризик втрати контролю або доступу на об’єкт [31; 69].

Розширення проектної загрози таким чином створює багаторівневу систему планування, у якій традиційна модель проектної загрози залишається основою мирного режиму, а спеціальні сценарії – інструментом адаптації до умов особливого періоду.

Варто підкреслити, що на відміну від багатьох інших держав, Україна вже інституційно оформлює перегляд підходів до формування проектної загрози з урахуванням досвіду збройної агресії.

На законодавчому рівні це закріплено, зокрема, через внесення до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» окремої статті, яка б визначала проектну загрозу як результат спеціальної оцінки ризику диверсій, крадіжки або іншого неправомірного вилучення матеріалів і

встановлює, що організація роботи з її визначення здійснюється уповноваженим органом державної влади [23, ст. 4-1].

Наразі Кабінет Міністрів України постановою від 27.08.2022 № 956 визначив Державну інспекцію ядерного регулювання України відповідальним органом за організацію роботи з визначення проектної загрози для ядерних установок, ядерних матеріалів, радіоактивних відходів та інших джерел іонізуючого випромінювання в Україні, а також передбачив створення міжвідомчої робочої групи з цією метою [74].

Регуляторна практика останніх років демонструє, що йдеться не лише про формальне закріплення повноважень, а про реальний процес оновлення підходів до оцінювання загроз і формування нової об'єктової проектної загрози. ДІЯРУ спільно з ДНТЦ ЯРБ та за підтримки іноземних партнерів (зокрема норвезького регулюючого органу) розробило загальні положення щодо ядерної захищеності, що прямо спрямовані на врегулювання питань ядерної безпеки та фізичного захисту в умовах підвищеного ризику, включаючи воєнний час [18; 30].

У відкритих джерелах також відзначається, що український регулятор перейшов до систематичного оцінювання ядерно-безпекових загроз на державному рівні та підготовки оновленої проектної загрози з урахуванням досвіду широкомасштабної агресії, що фактично означає перегляд вихідних припущень, закладених у довоєнні моделі [11; 32].

Міжнародні аналітики підкреслюють, що запуск Україною процесу перегляду проектної загрози після прямих воєнних нападів на ядерні об'єкти має потенційно трансформаційний характер для всієї національної системи ядерної безпеки [69].

Зазначається, що перегляд проектної загрози в українських реаліях означає зміщення акценту від класичної терористичної моделі до комплексної моделі, яка включає сценарії артилерійських та ракетних обстрілів, загрози окупації, руйнування зовнішнього електропостачання, застосування безпілотних літальних апаратів та інші форми воєнного впливу на ядерну

інфраструктуру. Деталізована класифікація ідентифікованих загроз воєнного характеру, а також розроблені сценарії силового впливу на ядерні установки, які формують базис для оновленої проектної загрози, наведені у Додатку Б.

У межах дослідження доцільно розглядати цей процес як емпіричне підтвердження можливості адаптації національного режиму фізичного захисту до умов війни, причому Україна виступає в цьому процесі першопроходьцем, який вимушено поєднує практичний досвід функціонування АЕС у зоні бойових дій з формальним переглядом моделі проектної загрози, що в подальшому може вплинути й на еволюцію міжнародних підходів [47; 75].

Одним із ключових рішень питання забезпечення фізичного захисту у військовий час, визначених у сучасних дослідженнях, є розроблення спеціального національного плану ядерної безпеки на воєнний час, який інтегрує фізичний захист, ядерну безпеку, радіаційний контроль, аварійну готовність, логістичне забезпечення персоналу й інженерний захист критичної інфраструктури.

Такий план має розглядатися як окрема форма організації роботи ядерного об’єкта під час збройного конфлікту, що встановлює правила взаємодії між державними органами, оператором, регулятором та силовими структурами [73].

Ключовими тезами такого плану можуть бути:

- наявність чітко визначеної ієрархії прийняття рішень, яка не допускає дублювання повноважень між регулятором, оператором і військовим командуванням;
- юридично закріплена обов’язковість виконання, яка унеможливлює ситуації, коли безпекові процедури залежать від політичних домовленостей або ситуативних рішень;
- комплексність змісту, що включає питання електроживлення, евакуації, логістики паливних запасів, резервних центрів управління, комунікацій та дій у разі втрати контролю над окремими системами;

- періодичне тестування, яке проводиться у формі спеціальних навчань, спрямованих на моделювання дій під час обстрілів, втрати зовнішнього електроживлення чи тривалого блокування об’єкта.

Створення такого плану дозволить компенсувати інституційну фрагментацію, яка характерна для мирного режиму, і створює правову основу для функціонування ядерного об’єкта у складних безпекових умовах.

Традиційна модель розподілу відповідальності між державою, експлуатуючою організацією та збройними силами передбачає, що держава несе загальну відповідальність за ядерну безпеку, оператор - за безпечну експлуатацію та фізичний захист, а силові структури виконують допоміжні функції. У воєнний час таке співвідношення зазнає суттєвих змін, оскільки саме військове командування має можливості забезпечити оборону периметра, протиповітряну оборону, супровід персоналу та захист транспортної інфраструктури.

Для чіткого розмежування повноважень доцільно виконати наступне:

- визначити перелік функцій фізичного захисту, які у разі введення воєнного стану переходять до військових формувань (охорона під’їзних шляхів, відбиття нападів, протидія повітряним загрозам);
- закріпити обов’язки оператора підтримувати додаткову військову інфраструктуру навколо ядерних об’єктів, яка в подальшому буде використовуватись військовими формуваннями під час збройного нападу;
- посилити роль регулятора як органу, що відповідає за ядерну безпеку і як найточніше може прогнозувати наслідки атаки того чи іншого засобу ураження на ядерний об’єкт та надавати методичні рекомендації для адаптації системи фізичного захисту.

Таким чином буде створено чітку інституційно стійку структуру управління, яка здатна діяти в умовах непередбачуваності та високої інтенсивності бойових дій.

2.7.2 Роль Міжнародного гуманітарного права

Неостанню роль у процесі захисту ядерних об’єктів може відігравати Міжнародне гуманітарне право (МГП), яке визначає окремі категорії об’єктів як такі, що містять «небезпечні сили», і забороняє здійснювати на них напад або використовувати їх для прикриття військових операцій. У цьому контексті ядерні об’єкти мають особливий статус, оскільки їх пошкодження може призвести до значних транскордонних наслідків [45; 46].

На сьогодні у літературі згадуються наступні практичні механізми застосування МГП:

- укладання двосторонніх або багатосторонніх угод про демілітаризацію території довкола ядерних об’єктів, що встановлюють зобов’язання сторін не використовувати їх у військових цілях;
- створення «зон під міжнародним спостереженням», у межах яких забезпечується постійна присутність інспекторів МАГАТЕ або інших уповноважених організацій [50; 56].
- запровадження спеціального режиму зв’язку між сторонами конфлікту з питань забезпечення доступу персоналу, аварійних служб та доставки матеріалів, необхідних для безпечної експлуатації об’єкта.

Ці механізми є гнучкими й не потребують внесення змін до фундаментальних міжнародних конвенцій, водночас істотно підвищуючи рівень захищеності ядерних об’єктів у зоні бойових дій.

Однак, такий механізм не завжди є дієвим. Україна послідовно ініціювала створення міжнародної безпекової демілітаризованої зони довкола Запорізької атомної електростанції, виходячи з того, що унікальний характер небезпеки, пов’язаної з розташуванням військових підрозділів на території найбільшої АЕС у Європі, не може бути належним чином врегульований наявними інструментами міжнародного режиму ядерної безпеки [41; 49].

Починаючи з серпня 2022 року, Україна неодноразово зверталася до Ради Безпеки ООН, Генеральної конференції МАГАТЕ та партнерських держав із

закликом створити спеціальний режим, який передбачав би повне відведення військ та озброєння з території станції та прилеглих районів [6; 62].

Такі пропозиції були сформульовані як відповідь на систематичні обстріли, порушення роботи зовнішніх ліній електропередач та фактичну неможливість забезпечення належного доступу українського персоналу до критично важливих систем ЗАЕС.

Важливим елементом української ініціативи стало напрацювання концепції, у якій демілітаризована зона розглядається не як політичний компроміс, а як спеціальний міжнародний захисний режим, заснований на положеннях міжнародного гуманітарного права щодо об'єктів, які містять «небезпечні сили», а також на повноваженнях МАГАТЕ щодо забезпечення безпечної експлуатації ядерних установок [47].

Україна запропонувала, щоб демілітаризована зона включала фізичне відведення військових підрозділів, заборону на використання території станції для військових цілей, а також гарантії безперешкодного доступу інспекторів МАГАТЕ для постійного моніторингу ситуації. Ця концепція була підтримана низкою держав, оскільки її реалізація розглядається як єдиний на сьогодні механізм стабілізації безпекової ситуації довкола ЗАЕС у короткостроковій перспективі [5].

Позиція України була спрямована на те, щоб створення демілітаризованої зони увійшло до ширшого контексту міжнародних практик із забезпечення ядерної безпеки в умовах збройних конфліктів. У межах консультацій з МАГАТЕ у 2022-2023 роках Україна наполягала на тому, що безпекову зону необхідно закріпити як прецедент міжнародного рівня, який у майбутньому має бути інтегрований до рекомендаційних документів щодо фізичного захисту та аварійної готовності [39].

Це, на думку української сторони, дозволило б заповнити суттєву прогалину міжнародного режиму ядерної безпеки: відсутність інструментів реагування у випадках, коли ядерний об'єкт стає безпосереднім середовищем ведення бойових дій.

Ініціатива України щодо демілітаризації ЗАЕС має не лише практичне, але й концептуальне значення, оскільки ставить питання про формування нових норм і механізмів міжнародного регулювання у сфері ядерної безпеки під час війни, хоча й досі залишається нереалізованою.

Варто підкреслити, що питання ефективного функціонування системи фізичного захисту у воєнний період потребує не лише організаційних змін, але й комплексної модернізації технічних підходів. Дослідження показують, що ключовими напрямами технічної модернізації систем фізичного захисту під військові загрози є:

- підвищення стійкості систем електроживлення за рахунок дублювання ліній передачі, створення незалежних резервних джерел та збільшення запасів палива для автономних генераторів [43];
- розгортання додаткових резервних центрів керування з автономними каналами зв’язку та локалізованими системами контролю;
- захист систем виявлення й відеоспостереження шляхом створення броньованих або заглиблених каналів їх розміщення;
- забезпечення фізичного укріплення будівель, що містять елементи ІТЗ ФЗ, засоби зв’язку тощо [25; 27].

Особливої уваги потребує питання інтеграції фізичного захисту, ядерної безпеки та аварійної готовності

У мирний час фізичний захист, ядерна безпека та аварійне реагування переважно функціонують у відносно автономних регуляторних та організаційних площинах. У воєнний час така автономність створює загрозу виникнення прогалин під час управління у атомною генерацією у кризових ситуаціях [66]. Тому важливим рішенням є створення єдиного інтегрованого підходу до управління всіма системами безпеки, який передбачатиме спільні алгоритми прийняття рішень у разі відключення електропостачання, обстрілів або загроз втрати контролю; централізовану координацію інформаційного обміну між оператором, регулятором, військовими структурами та аварійними службами; проведення спільних навчань і симуляцій воєнних сценаріїв.

Така інтеграція дозволяє мінімізувати час реагування на події, знизити ризик дублювання або конфлікту рішень і забезпечити узгодженість дій у режимі обмеженого часу.

Адаптація міжнародного режиму фізичної ядерної безпеки до умов збройних конфліктів може бути досягнута через сукупність взаємопов'язаних заходів, які не суперечать базовим принципам ядерної безпеки, але забезпечують можливість функціонування системи в умовах масштабних бойових дій. Основні напрями такого вдосконалення включають:

- розширення спектра загроз у проектній загрозі, включаючи збройні напади;
- формування національного плану забезпечення безпеки ядерних об'єктів на воєнний час [73];
- перерозподіл відповідальності між органами влади виходячи із загроз;
- використання юридичних механізмів МГП;
- модернізація систем фізичного захисту;
- інтеграцію всіх систем безпеки в єдиний систему реагування.

Таким чином, міжнародний режим фізичного захисту та безпеки ядерних об'єктів в цілому у його сучасному вигляді не потребує повного перегляду, однак потребує суттєвого доповнення, яке визнає реальність війни як окремого режиму функціонування ядерної інфраструктури.

2.8 Загрози нанесення повітряних ударів по ядерних об'єктах і використанням БпЛА

Збройна агресія проти України створила унікальну, безпрецедентну у світовій практиці експлуатації ядерної енергетики ситуацію, коли об'єкти мирного атома опинилися в епіцентрі високоінтенсивного військового конфлікту із застосуванням повного спектру засобів повітряного нападу. Ядерні енергоблоки, об'єкти зберігання відпрацьованого ядерного палива (СВЯП), системи зовнішнього електроживлення атомних станцій та критичні елементи

допоміжної інженерної інфраструктури зазнали системного впливу масованих ракетних та безпілотних атак [6; 39]. Характер цих ударів, їхня регулярність, тактична спрямованість на енергетичні вузли та критичні технологічні елементи засвідчили фундаментальний розрив між традиційною моделлю фізичного захисту, розробленою міжнародною спільнотою для мирного часу, та реальними воєнними загрозами, що вимагає перегляду базових постулатів ядерної безпеки (рисунок 2.2).

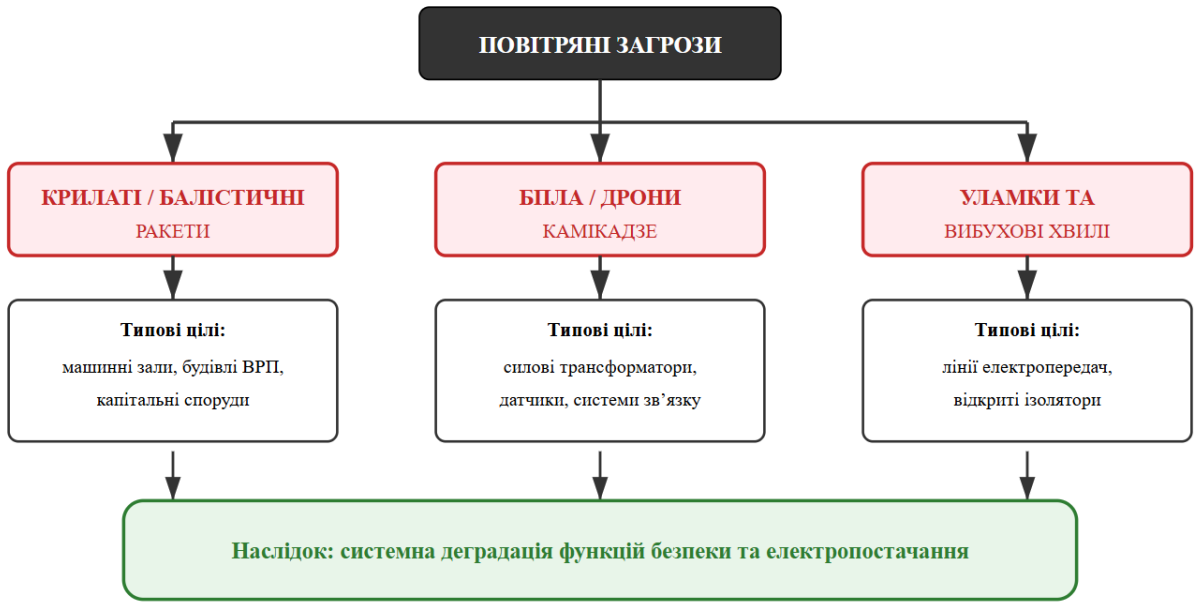

Рисунок 2.2 – Схематичне представлення характер ударів повітряного нападу, їхня регулярність, тактична спрямованість на енергетичні вузли та критичні технологічні елементи

Функціонування ядерних об'єктів в Україні у період після лютого 2022 року надало унікальну можливість емпірично дослідити механізми впливу сучасних засобів повітряного нападу на системи, що забезпечують фізичний захист, ядерну та радіаційну безпеку. Аналіз подій війни дозволяє виявити закономірності деструктивного впливу, які раніше не були достатньо опрацьовані ні в науковій літературі, ні в міжнародному праві, оскільки вони виходили за межі так званої «проектної загрози» (Design Basis Threat) [19; 32].

Ключовим висновком, який випливає із системного аналізу подій війни, є доведення факту, що сучасні засоби повітряного нападу дозволяють агресору

повністю ігнорувати класичну архітектуру фізичного захисту. Випадки, зафіксовані на енергетичних об’єктах України, зокрема на вузлах електропостачання, що забезпечують роботу АЕС, продемонстрували здатність ракетного озброєння та ударних безпілотних літальних апаратів (БпЛА) обходити інженерні бар’єри (огородження, стіни, шлюзи) шляхом вертикального охоплення. Завдавання ураження з відстані у сотні або тисячі кілометрів фактично нівелює функції «виявлення» та «затримки» порушника, які є базовими у структурі фізичного захисту відповідно до рекомендацій МАГАТЕ INFCIRC/225/Rev.5 [2; 9].

Традиційна парадигма фізичного захисту, збудована на підходах мирного часу, базувалася на сценарії наземного проникнення, де порушник має фізично подолати периметр, що дає силам охорони час на реакцію. Повітряна війна скасовує цей часовий лаг. Ракета або дрон долають зону безпеки миттєво, не вступаючи в контакт із силами охорони, що робить класичні засоби (відеоспостереження, сигналізація, стрілецька зброя охорони) неефективними. Це означає, що система фізичного захисту в її нинішньому вигляді не має інструментів для протидії загрозам, що реалізуються в повітряному просторі, не передбачають фізичної присутності диверсанта в зоні об’єкта та характеризуються надвисокою швидкістю реалізації деструктивного впливу.

Одним із найбільш критичних аспектів повітряної загрози, виявленим у ході бойових дій, стала вразливість систем зовнішнього електроживлення АЕС. Український досвід показав, що навіть без прямого кінетичного ураження реакторних будівель або гермооболонок, повітряні удари здатні спричиняти довготривалі та системні порушення функцій безпеки через руйнування зовнішньої інфраструктури [42; 43].

Особливої уваги заслуговує проблема системного ураження високовольтних ліній електропередач та відкритих розподільчих пристроїв (ВРП), що живлять українські атомні електростанції. Повітряні удари продемонстрували здатність агресора одночасно знищувати декілька паралельних ліній електропередач, що вважалося малоймовірним у мирних

ймовірнісних моделях безпеки (PSA). Таке синхронізоване руйнування позбавляє енергоблоки всіх незалежних джерел зовнішнього живлення, примусово переводячи їх у режим повного знеструмлення (Station Blackout - SBO).

Сценарії повного знеструмлення неодноразово фіксувалися під час масованих російських ракетних ударів, коли цілі групи підстанцій та трансформаторного обладнання зазнавали ураження протягом короткого проміжку часу (декількох хвилин). Така ситуація підтверджує, що ураження енергетичної інфраструктури перестало бути побічним ефектом бойових дій і трансформувалося у цілеспрямовану тактику створення вторинних ризиків для ядерної безпеки. Втрата зовнішнього живлення є критичною подією, оскільки саме воно забезпечує роботу головних циркуляційних насосів, систем підживлення першого контуру та систем тепловідведення, необхідних для розхолоджування активної зони реактора.

Негативний досвід масованих атак на об’єднану енергетичну систему (ОЕС) України виявив системну закономірність: противник застосовував різні типи високоточних боєприпасів не стільки для фізичного знищення конкретних будівель, скільки для створення довготривалих функціональних розривів у мережі [11; 18]. Ураження вузлових розподільчих підстанцій, яке повторювалося з інтервалом у кілька днів або тижнів, унеможливлювало швидке відновлення схеми живлення АЕС. Це призводило до виникнення станів, коли енергоблоки вимушено переходили у режим аварійного живлення від дизель-генераторів на непрогнозовано тривалий час. З огляду на те, що стабільність зовнішньої мережі є першим рівнем у концепції «глибокого ешелонування», її руйнування повітряними ударами означає фактичну ліквідацію першого бар’єра безпеки, що значно підвищує навантаження на наступні ешелони захисту та збільшує ймовірність важкої аварії.

Важливим науковим висновком є те, що вплив повітряних ударів на ядерну інфраструктуру не можна оцінювати як набір ізольованих інцидентів.

Йдеться про сукупність взаємопов’язаних подій, що створюють тривалу загрозу через кумулятивний характер пошкоджень.

У мирний час аварійне відключення зовнішньої лінії є одиничною подією, яка усувається ремонтними бригадами в штатному режимі. В умовах повітряної війни відбувається часткове ураження допоміжних елементів (кабельні траси, системи релейного захисту, трансформатори власних потреб) знижує надійність системи навіть після формального відновлення живлення. Пошкодження енергосистеми на значній відстані від АЕС створює «ефект хвилі» - коливання частоти та напруги, аварійні відключення споживачів, розбалансування енергосистеми. Це автоматично призводить до відключення турбогенераторів АЕС дією автоматики, навіть якщо сама станція не була атакована. Обмежений доступ ремонтного персоналу до пошкоджених об’єктів через загрозу повторних ударів або мінування території суттєво розтягує часові рамки відновлення.

Таким чином, повітряна загроза має розподілений характер: атака, спрямована на інфраструктуру за десятки або сотні кілометрів від атомної станції, може мати прямий і миттєвий вплив на її здатність функціонувати у безпечному режимі. Таке розширення зони потенційних ризиків є принциповою зміною парадигми безпеки, оскільки вимагає переходу від локальних методів захисту периметра до регіонально орієнтованих моделей, які враховують взаємозв’язок критичних об’єктів у масштабах великих енергетичних систем.

Аналіз подій воєнного періоду показує, що вплив на ядерну установку дедалі частіше реалізується не у формі прямого проникнення на об’єкт, а через ураження зовнішніх елементів критичної інфраструктури, насамперед енергетичної. За таких умов «об’єктом атаки» стає не тільки майданчик АЕС, а і ширший контур забезпечення її стійкої експлуатації: підстанції магістральних мереж, відкриті розподільчі пристрої, лінії електропередач, системи зв’язку та логістичні маршрути постачання ресурсів. Це якісно змінює підходи до оцінювання уразливості, адже традиційна модель фізичного захисту,

орієнтована на периметр і локальні бар'єри, перестає охоплювати ключові ланки причинно-наслідкового ланцюга.

На рисунку 2.3 відображено механізм формування каскадної аварійної ситуації типу повного знеструмлення (SBO) як результату повітряних ударів по зовнішній інфраструктурі. Критично важливим є те, що навіть за відсутності безпосереднього ураження корпусів реакторних установок або внутрішніх систем безпеки, деградація зовнішнього електропостачання створює умови, за яких безпека переходить у режим залежності від резервних джерел енергії (передусім дизель-генераторів). Отже, подія «поза периметром» фактично ініціює ланцюг внутрішніх експлуатаційних обмежень і ризиків, зростання яких має не лінійний, а накопичувальний характер .

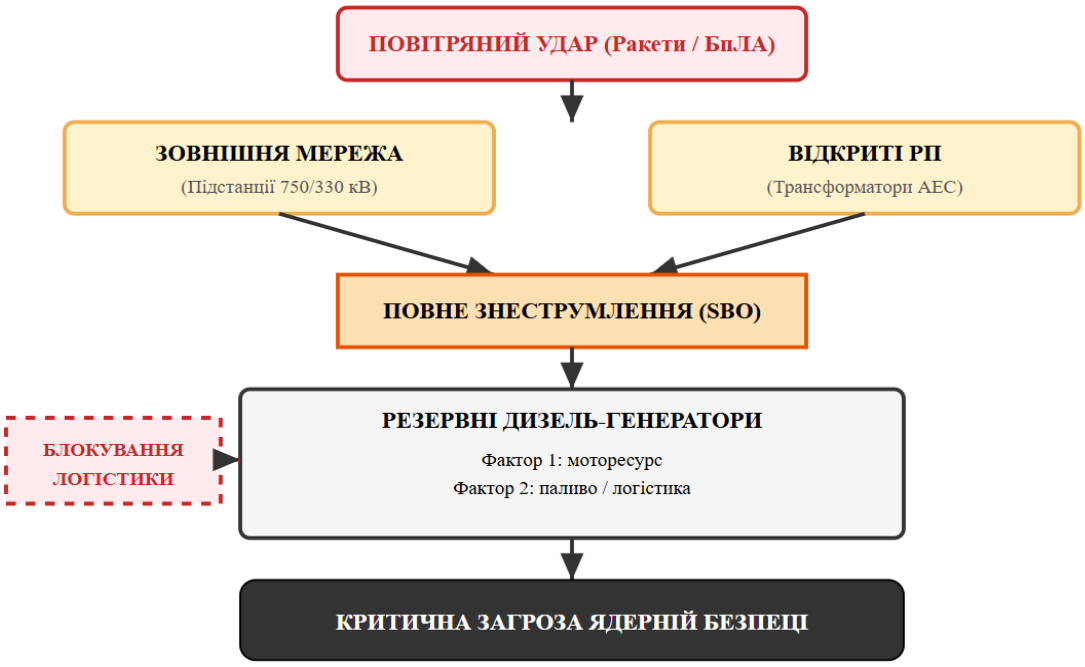

Рисунок 2.3 – Схематичне представлення механізму формування каскадної аварійної ситуації типу повного знеструмлення (SBO) як результату повітряних ударів

Окремо слід підкреслити, що режим роботи резервних дизель-генераторів у ситуації SBO є часово та ресурсно обмеженим. Вичерпання моторесурсу, нестача палива, проблеми із технічним обслуговуванням, затримки у доставці витратних матеріалів та обмежений доступ персоналу формують сукупність

факторів, які можуть трансформувати «керовану» ситуацію втрати зовнішнього електропостачання у небезпечний сценарій із дефіцитом енергії для підтримання функцій безпеки. Таким чином, логістика й доступність ресурсів (паливо, ремонтні комплекти, персонал, зв'язок) стають елементами, які прямо впливають на стійкість бар'єрів безпеки, хоча формально можуть виходити за межі класичних переліків елементів системи фізичного захисту.

Критичним наслідком системного руйнування зовнішньої енергетичної інфраструктури стало виникнення загрози, яка раніше розглядалася лише теоретично у межах стрес-тестів після аварії на АЕС «Фукусіма-1» - це проблема тривалої роботи на аварійних джерелах живлення. У технічних звітах українського оператора АЕС зафіксовано численні випадки вимушеного переходу енергоблоків у стан «холодного зупину» або роботи на потужності, що забезпечується виключно резервними дизель-генераторами (РДЕС).

Досвід війни виявив фундаментальну невідповідність між проектним призначенням РДЕС та реальними умовами їх експлуатації під час повітряних кампаній. Традиційно резервні системи проектувалися як тимчасовий інструмент стабілізації (на період до 72 годин), необхідний для безпечної зупинки реактора та очікування відновлення зовнішньої мережі. Проте в умовах масованих ракетних атак на національну енергосистему періоди знеструмлення ставали непрогнозованими та повторюваними. Це призвело до експлуатації дизель-генераторів у режимі, наближеному до базового навантаження, що створює низку критичних ризиків:

Тривала безперервна робота аварійних генераторів призводить до прискореного трибологічного зношення механічних вузлів, перегріву систем та підвищення ймовірності відмови під час запуску (Failure to Start) або під час роботи (Failure to Run). Науковий аналіз показує, що зі збільшенням часу роботи РДЕС ймовірність їх відмови зростає не лінійно, а експоненційно, наближаючи систему до так званого «ефекту обриву» (Cliff Edge Effect), коли запас міцності вичерпується миттєво [8; 70].

В окремих випадках, зафіксованих під час повітряних атак, самі системи резервного живлення або паливосховища опинялися в зоні ризику ураження уламками ракет чи ударними хвилями. Це демонструє, що в умовах війни останній ешелон захисту (аварійне живлення) є настільки ж фізично вразливим, як і перший (зовнішня мережа), що суперечить принципу незалежності рівнів глибокого ешелонування.

У цьому контексті показовою є трансформація поняття «зони вразливості», проілюстрована на Рис. 2.4. У «мирній» моделі зона ризику здебільшого концентрується навколо периметра фізичного захисту: постульований порушник (диверсант) має подолати бар'єри, проникнути на об'єкт і здійснити вплив на критичні елементи. У «воєнній» моделі зона вразливості розширюється до регіонального масштабу - ураження вузлів енергосистеми або критичних об'єктів поза межами майданчика може забезпечити досягнення небезпечного ефекту опосередковано, через ініціювання каскадної відмови. Це означає, що фактичний «контур захисту» має охоплювати взаємозалежні інфраструктури (електропостачання, зв'язок, транспорт/логістика), а також механізми міжвідомчої координації та реагування.

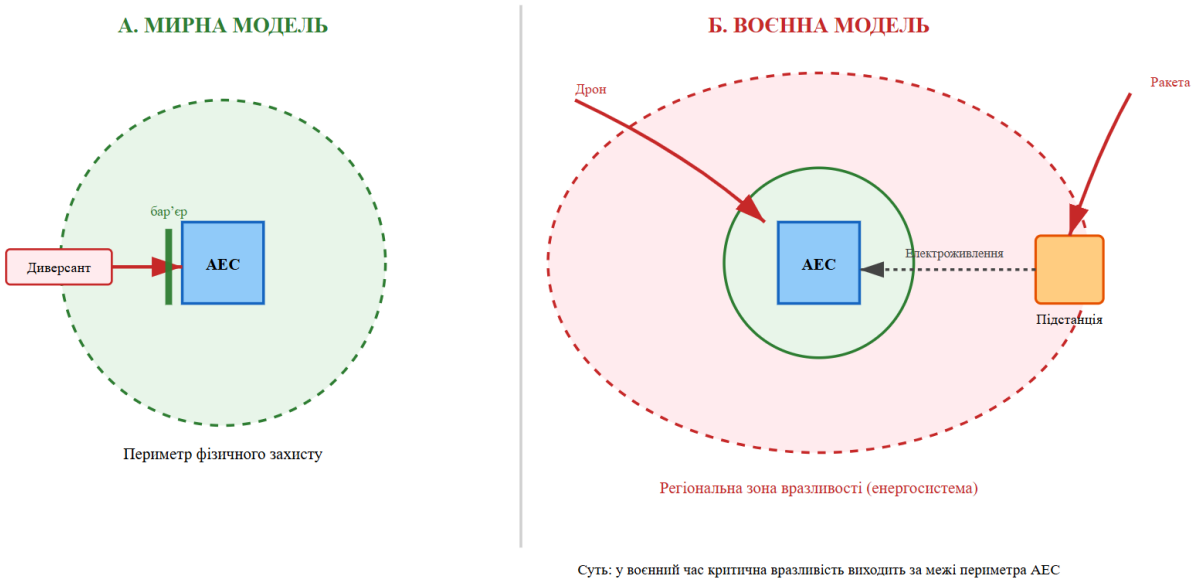

Рисунок 2.4 – Схематичне представлення трансформації поняття «зони вразливості» у «мирній» моделі та «воєнній» моделі

Крилаті та балістичні ракети, як правило, асоціюються з ураженням капітальних споруд і великих інфраструктурних вузлів, що створює передумови для різких і масштабних порушень функціонування. БПЛА/дрони-камікадзе формують інший профіль небезпеки: відносно «точкові» удари по трансформаторах, датчиках, вузлах зв'язку або відкритих елементах можуть спричинити непропорційно значний системний ефект - через втрату керованості, інформаційної підтримки, або деградацію енергоживлення окремих підсистем. Уламки та ударні хвилі, зокрема при роботі протиповітряної оборони, створюють додатковий клас супутніх пошкоджень, який часто є складним для прогнозування: ураження відкритих ізоляторів, ліній електропередач чи комутаційних елементів може мати наслідком нестійкі режими енергопостачання та повторні відмови навіть після первинного відновлення.

У воєнний час реальна вразливість ядерної установки визначається не лише міцністю локальних бар'єрів і протидією проникненню, а й стійкістю зовнішніх інфраструктурних зв'язків, здатністю системи забезпечення (енергетика, логістика, зв'язок) працювати в умовах тривалих порушень, а також наявністю процедур і ресурсів для реагування на події поза проєктними припущеннями. У практичному вимірі це потребує перегляду підходів до аналізу загроз, критеріїв проєктування та оцінки ефективності фізичного захисту - з урахуванням каскадних сценаріїв і «розширеної» зони вразливості.

Повітряні удари по об'єктах України виявили ще одну фундаментальну вразливість, яка не була належним чином врахована у традиційних моделях фізичного захисту - це залежність ядерної безпеки від зовнішньої транспортної логістики. У мирний час концепція безпеки базується на припущенні про безперешкодний доступ до ресурсів (палива, мастил, запчастин, персоналу). Війна зруйнувала цю аксіому.

Знищення транспортної інфраструктури - мостів, дорожніх розв'язок, залізничних вузлів - у безпосередній або віддаленій зоні навколо атомних станцій створило загрозу логістичної ізоляції об'єкта. В умовах, коли АЕС

переходить на роботу від дизель-генераторів, її безпека починає вимірюватися не міцністю гермооболонки, а кількістю наявного дизельного палива та можливістю його підвезення. Масовані атаки на транспортну інфраструктуру здатні фізично унеможливити своєчасне поповнення запасів, перетворюючи проблему знеструмлення на неминучу радіаційну аварію через вичерпання палива.

Ця ситуація демонструє формування нового типу вразливості - «логістичної петлі»:

- повітряний удар знищує енергомережу (виникає потреба в дизелі);
- одночасний або наступний удар знищує транспортні шляхи (унеможливлюється доставка дизеля);
- як наслідок, автономність роботи активних систем безпеки скорочується з проектних тижнів до фактичних годин [13; 73].

Така логістична залежність є одним із ключових уроків українського досвіду: фізичний захист ядерної установки не може обмежуватися периметром майданчика. Він повинен охоплювати захист критичних логістичних маршрутів (supply chains) у радіусі десятків кілометрів, що вимагає інтеграції зусиль оператора АЕС та сил територіальної оборони.

2.9 Протидія загрозам від безпілотних літальних апаратів: нова архітектура виявлення, ідентифікації, затримки та нейтралізації

2.9.1 Зміна парадигми вразливості: БпЛА як фактор асиметричного впливу на систему фізичного захисту

Сучасний бурхливий розвиток безпілотних авіаційних систем (БАС) та їх масоване застосування у військових конфліктах суттєво трансформували архітектуру загроз для критичної інфраструктури, зокрема ядерних об’єктів. Поява доступних, малопомітних, високоточних та автономних засобів повітряного нападу створила прецедент реалізації атак, які концептуально не були враховані в традиційних, детерміністичних підходах до фізичного захисту

(Physical Protection Systems - PPS), що базуються на рекомендаціях МАГАТЕ (INFCIRC/225/Rev.5) [2; 9].

Фундаментальною особливістю БпЛА, що відрізняє їх від класичних загроз (диверсантів, терористичних груп), є їхня здатність до тривимірного маневрування та ігнорування ешелонованої системи наземних бар'єрів. Традиційна система фізичного захисту проектувалася як площинна структура, де ймовірність успіху атаки обернено пропорційна кількості фізичних перешкод (парканів, стін, шлюзів) на шляху до цілі [27]. БпЛА, діючи у вертикальній площині, фактично «перестрибують» через периметр, наземні засоби виявлення та пости фізичної охорони, здійснюючи безпосереднє ураження елементів інфраструктури, що розташовані у так званій «захищеній зоні», але не мають спеціального фортифікаційного укриття (верхнього перекриття).

Ця властивість робить БпЛА одним із найскладніших типів загроз для ядерних установок, особливо в умовах збройного конфлікту, коли загроза набуває системного характеру. Війна проти України емпірично довела, що БпЛА трансформувалися з засобу розвідки в універсальну платформу, яка використовується для:

- точкових ударів дронами-камікадзе (баражуючими боєприпасами) по вразливих вузлах (трансформатори, системи охолодження) [11; 40].
- коригування артилерійського та ракетного вогню в реальному часі.
- використання дешевих дронів для виснаження боєзапасу систем протиповітряної оборони перед основним ракетним ударом [10].

2.9.2 Аналіз вразливості критичних елементів АЕС до повітряних ударів малої потужності

Досвід бойових дій в Україні дозволив ідентифікувати нову категорію вразливості ядерних об'єктів - чутливість до малопотужних точкових ударів. У низці зафіксованих випадків використання малих дронів (з бойовою частиною

1-3 кг) для ураження трансформаторних підстанцій власних потреб, відкритих розподільчих пристроїв (ВРП), кабельних естакад та зовнішніх блоків систем вентиляції призводило до системних порушень функцій безпеки [6; 40].

Це спростовує поширений міф про те, що ядерний об’єкт є невразливим через міцність реакторного відділення. Хоча гермооболонка витримує падіння легкого літака [70], периферійна інфраструктура, яка забезпечує життєдіяльність реактора (охолодження, живлення КВПіА, зв’язок), є вразливою до осколкового та фугасного впливу навіть малих боєприпасів. Особливо небезпечними є сценарії комбінованих атак, коли удари БпЛА по системах пожежогасіння або аварійного освітлення синхронізуються з ракетними ударами, що значно ускладнює ліквідацію наслідків та підвищує ймовірність переростання проектної аварії у важку [20; 21].

Вже сам факт здатності БпЛА непомітно наближатися до заборонених зон ядерних установок (Vital Areas) ставить під сумнів ефективність існуючої парадигми, орієнтованої на наземний моніторинг обстановки. Наявні міжнародні документи (INFCIRC/225/Rev.5) розроблялися в епоху домінування наземних загроз і не містять методології побудови протиповітряного фізичного захисту [2; 9].

Тому протидія БпЛА вимагає імплементації концептуально нового підходу - створення інтегрованої системи C-UAS (Counter-Unmanned Aircraft Systems), яка базується на чотирьох послідовних етапах: Виявлення - Ідентифікація - Затримка - Нейтралізація. Ця система повинна бути не просто додатком до існуючих засобів охорони, а органічною частиною загальної системи фізичного захисту, глибоко інтегрованою з державною системою ППО.

Ефективність нейтралізації прямо залежить від часу попередження (Early Warning Time). В умовах сучасної війни виявлення БпЛА ускладнюється низкою факторів:

- сучасні дрони виготовляються з композитних матеріалів (пластик, карбон), які є «прозорими» для класичних радіолокаторів;

- політ на висоті 10-50 метрів з використанням рельєфу місцевості («térrain masking») дозволяє уникати виявлення РЛС дальнього огляду;
- автономні дрони, що летять за інерціальною системою навігації, не випромінюють радіосигналів керування, що робить їх невидимими для засобів радіотехнічної розвідки (РТР).

Для вирішення цієї проблеми наукова література та практика пропонують застосування мультисенсорного підходу (Multi-Sensor Fusion), який передбачає одночасне використання чотирьох каналів отримання інформації:

- Активна радіолокація: спеціалізовані мікро-РЛС малого радіусу дії (Ku-band, X-band), здатні детектувати малі рухомі цілі на фоні землі.
- Пасивна радіопеленгація (RF-аналіз): сканування радіоефіру для виявлення сигналів керування (Command Link) та передачі відео (Video Link) між дроном і оператором. Це дозволяє не лише виявити дрон, але й локалізувати місце знаходження оператора.
- Оптико-електронні системи (EO/IR): тепловізійні та оптичні камери з високою роздільною здатністю та алгоритмами комп'ютерного зору для візуального підтвердження цілі.
- Акустичні сенсори: масиви мікрофонів для виявлення характерного звукового підпису двигунів БпЛА.

Досвід України свідчить, що саме комбінація акустичних та оптичних сенсорів є найбільш ефективною для виявлення дронів-камікадзе типу «Shahed» у нічний час, коли візуальний контакт обмежений, а радіолокаційний - ускладнений.

Після факту виявлення ключовим завданням стає ідентифікація - селекція цілі та визначення рівня загрози. У мирний час ця процедура зводилася до бінарної логіки «свій-чужий» або факту перетину кордону зони. У воєнний час ідентифікація потребує складного аналізу поведінкових патернів.

Система повинна автоматично оцінювати:

- Кінематичні параметри: швидкість, висота, вектор руху.

- Типологію цілі: чи це ударний дрон (FPV, крило), розвідувальний квадрокоптер чи хибна ціль (птах).
- Спрямованість атаки: критично важливим індикатором є вектор руху. Якщо траєкторія БпЛА перетинається з координатами критичних вузлів (ВРП, насосна станція), системі автоматично присвоюється найвищий рівень пріоритету загрози.

Особливий виклик створює насиченість повітряного простору різними типами об’єктів («туман війни»). В одній зоні можуть перебувати ворожі ударні дрони, власні розвідувальні БпЛА сил оборони та «саморобні» дрони. Це вимагає впровадження систем автоматизованої класифікації на основі штучного інтелекту, здатних розрізняти візуальні та акустичні сигнатури різних моделей БпЛА за долі секунди.

2.9.3 Нормативний вакуум та інституційна криза впровадження засобів радіоелектронної боротьби

Проблема ідентифікації та нейтралізації БпЛА має не лише технічний, але й глибокий нормативний вимір. Міжнародні керівні документи з фізичного захисту (серія NSS МАГАТЕ) не містять чітких критеріїв щодо класифікації БпЛА як елемента проектної загрози та не регламентують застосування засобів радіоелектронної боротьби (РЕБ) цивільними операторами [4; 8]. Це створило ситуацію правової невизначеності, коли імперативна потреба захисту об’єктів зіштовхнулася з відсутністю методологічної бази.

У відповідь на ескалацію повітряних загроз держава вдалася до реалізації так званих «ad-hoc» (ситуативних) регуляторних рішень. Яскравим прикладом такої інституційної реакції стала постанова Кабінету Міністрів України № 881 від 15 липня 2024 року «Про реалізацію експериментального проєкту щодо нарощування спроможностей радіоелектронного прикриття об’єктів критичної інфраструктури» [76]. Цей документ є спробою нормативного врегулювання питання масового застосування РЕБ для захисту енергетичних об’єктів.

Постанова запроваджує модель, відповідно до якої на операторів критичної інфраструктури (включно з АЕС) покладається фінансовий та організаційний обов'язок забезпечити придбання засобів РЕБ із подальшою їх передачею уповноваженим державним структурам (військовим формуванням) для створення локальних куполів радіоелектронного прикриття. Попри стратегічну правильність наміру, детальний аналіз положень цього акта виявляє низку суттєвих методологічних вад, що створюють ризики для ефективності всієї системи фізичного захисту.

Найбільш критичною вадою поточної нормативної ініціативи є методологічний розрив між обов'язком закупівлі та відсутністю критеріїв вибору обладнання. Постанова № 881 встановлює імперативну вимогу щодо інвестування коштів у засоби РЕБ, проте не надає жодного механізму науково обґрунтованого оцінювання потреб.

У сфері ядерної безпеки будь-яке технічне рішення традиційно базується на попередньому моделюванні (Design Basis Analysis) [19; 27]. Однак у випадку з РЕБ оператори опинилися в ситуації «сліпої закупівлі». Нормативна база не визначає:

- спектральні вимоги: які саме діапазони частот повинні перекриватися (лише цивільні GPS/GLONASS, чи також канали керування FPV 800-900 МГц, чи нестандартні частоти, на які переходить ворог);
- енергетичні параметри: яка необхідна щільність завад (Вт/м²) для ефективного придушення сигналу на межі периметра ядерної установки;
- конфігурація зон: чи повинен захист бути купольним (omni-directional), чи секторним (directional), і як це корелює з геометрією майданчика АЕС.

Відсутність державної методики передпроектного оцінювання призводить до того, що закупівлі здійснюються на основі комерційних пропозицій ринку, а не на основі системного аналізу загроз. Це створює ризик постачання обладнання, яке технічно неспроможне протидіяти сучасним військовим БпЛА,

що використовують передові алгоритми псевдовипадкового перелаштування робочої частоти (FHSS) [10].

Важливою процедурною прогалиною є запровадження моделі постфактумного оцінювання ефективності. Згідно з логікою експериментального проекту, оцінка дієвості засобів РЕБ здійснюється компетентними органами вже після їх придбання, інтеграції та введення в експлуатацію.

Така модель («trial and error» - спроб і помилок) є абсолютно неприйнятною для ядерної галузі, де вартість помилки є критичною. Відсутність процедури попередньої експертизи та сертифікації створює умови для:

- неконтрольованих фінансових витрат: оператори змушені витрачати значні ресурси на обладнання, ефективність якого не гарантована. За відсутності критеріїв «достатності», процес закупівлі може перетворитися на безкінечну гонку озброєнь без досягнення кінцевого результату безпеки;
- ілюзії захищеності: наявність на балансі дороговартісного, але технічно невідповідного обладнання створює хибне відчуття безпеки у керівництва об’єкта, що може призвести до зниження пильності в інших ешелонах охорони [38].

Це явище можна класифікувати як «нормативний дисбаланс»: юридичний обов’язок витрачати кошти визначено чітко, тоді як технічний механізм досягнення мети захисту залишено на розсуд суб’єктів, що не мають відповідної військово-технічної експертизи.

Ще одним критичним недоліком чинного регулювання є ігнорування проблеми інтеграції засобів РЕБ у загальну систему фізичного захисту та їхньої електромагнітної сумісності (ЕМС) з обладнанням АЕС.

Засоби РЕБ є джерелами потужного електромагнітного випромінювання. Їх некоректне розміщення або налаштування без попереднього моделювання електромагнітної обстановки (ЕМО) може призвести до ефекту «дружнього вогню» (fratricide jamming) та блокування власних систем: придушення каналів

радіозв'язку сил охорони, систем бездротової передачі даних з камер спостереження або датчиків периметра.

Має також місце вплив потужних електромагнітних полів на чутливі датчики контрольно-вимірювальних приладів і автоматики (КВПіА) реакторного відділення або систем релейного захисту.

Постанова № 881 не передбачає процедур оцінки ЕМС, що створює ризик фрагментації технічних рішень. Засоби РЕБ впроваджуються як автономна надбудова, не пов'язана з комплексом інженерно-технічних засобів фізичного захисту (наказ ДІЯРУ № 176) [25]. Це суперечить фундаментальним принципам системного підходу, згідно з якими всі елементи безпеки повинні функціонувати як єдиний організм наведено на Рисунок 2.5.

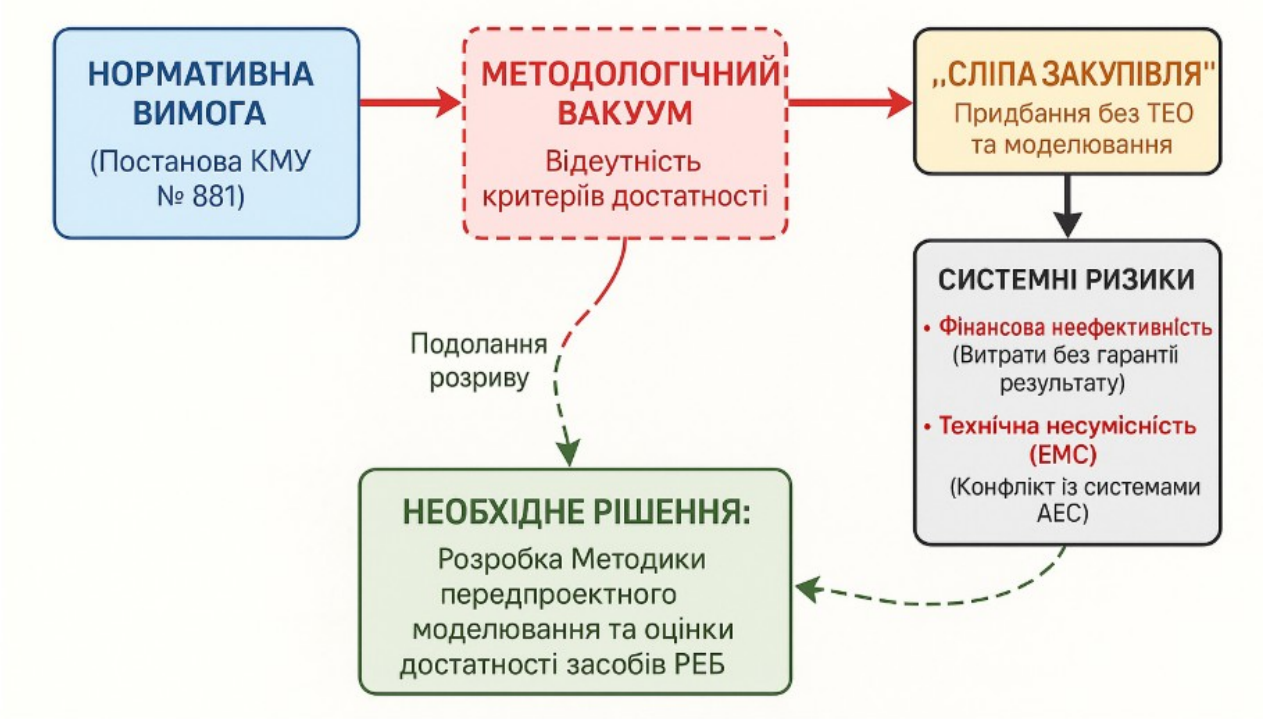

Рисунок 2.5 – Схема нормативно-методологічного розриву у процесі впровадження засобів РЕБ на об'єктах критичної інфраструктури

2.9.4 Трансформація функції «Затримка» (Delay)

Після етапів виявлення та ідентифікації третім критичним елементом системи фізичного захисту є **затримка**. У класичній методології фізичного

захисту (INFCIRC/225/Rev.5, TECDOC-967) функція затримки визначається як створення фізичних перешкод (стін, дверей, бар'єрів), що збільшують час проникнення порушника (T_{delay}) до величини, достатньої для прибуття сил реагування ($T_{response}$). Тобто, основна мета - виграти час [2; 9; 27]..

Щодо БпЛА цей підхід втрачає фізичний сенс, оскільки повітряна ціль не взаємодіє з наземними бар'єрами. Тому в новій методології поняття «затримка» набуває радіоелектронного та просторового виміру. Йдеться не про зупинку руху об'єкта, а про деградацію його навігаційної спроможності, що змушує БпЛА знизити швидкість, змінити траєкторію або перейти в аварійний режим зависання/посадки.

Радіоелектронна затримка реалізується через два основні механізми:

- Придушення глобальних навігаційних супутникових систем (GNSS Denial): Створення поля завад на частотах GPS/GLONASS/Galileo. Це змушує дрон втратити точну просторову орієнтацію. Більшість комерційних та військових БпЛА у такому випадку переходять на інерціальну систему навігації (INS), яка має властивість накопичувати похибку з часом. Це знижує точність удару, фактично «відводячи» загрозу від точкових критичних вузлів (наприклад, трансформатора) в безпечну зону [10].
- Розрив каналів керування (C2 Link Severing): Блокування частот передачі команд між оператором і дроном (для керованих FPV або розвідувальних БпЛА). Це змушує апарат активувати протокол «Return to Home» (повернення на точку зльоту) або здійснити аварійну посадку.

Досвід атак на українську енергетику (зокрема, використання БпЛА типу «Shahed-136/Geran-2») виявив обмеженість методу затримки. Дрони, оснащені захищеними модулями CRPA (Controlled Reception Pattern Antenna) або високоточними інерціальними системами, здатні зберігати траєкторію польоту навіть в умовах потужного радіоелектронного придушення [11; 40]. Це означає, що функція затримки не є гарантованою і повинна розглядатися лише як допоміжний етап перед фізичною нейтралізацією.

2.9.5 Нейтралізація (Neutralization)

Нейтралізація є фінальним і найбільш ризикованим етапом протидії БпЛА. У традиційних моделях фізичного захисту нейтралізація передбачає затримання або знешкодження порушника силами охорони. Щодо повітряних цілей, нейтралізація поділяється на кінетичну та некінетичну [10; 27].

В умовах ядерного об’єкта застосування кінетичних засобів (зенітного вогню, ракет) створює парадокс безпеки: засіб захисту може стати джерелом аварії. Збиття дрона над відкритим розподільчим пристроєм або майданчиком сухого сховища відпрацьованого ядерного палива (СВЯП) призводить до неконтрольованого падіння уламків, детонації бойової частини та розливу палива, що може спричинити пожежу або пошкодження критичного обладнання [11; 40].

Через це нова архітектура захисту вимагає впровадження зонованої моделі нейтралізації (див. рис. 2.6):

- Зона відчуження: зовнішній периметр (радіус 3-5 км), де дозволено застосування всіх видів кінетичної зброї (ЗРК, зенітні гармати, кулемети) для знищення цілі на підльоті.
- Захищена зона: безпосередня близькість до реакторних відділень, де застосування кінетичної зброї обмежене або заборонене. Тут пріоритет надається засобам спрямованого радіоелектронного випромінювання (РЕБ-рушниці, купольні системи) та сіткометам, які мінімізують ризик вторинних уражень.

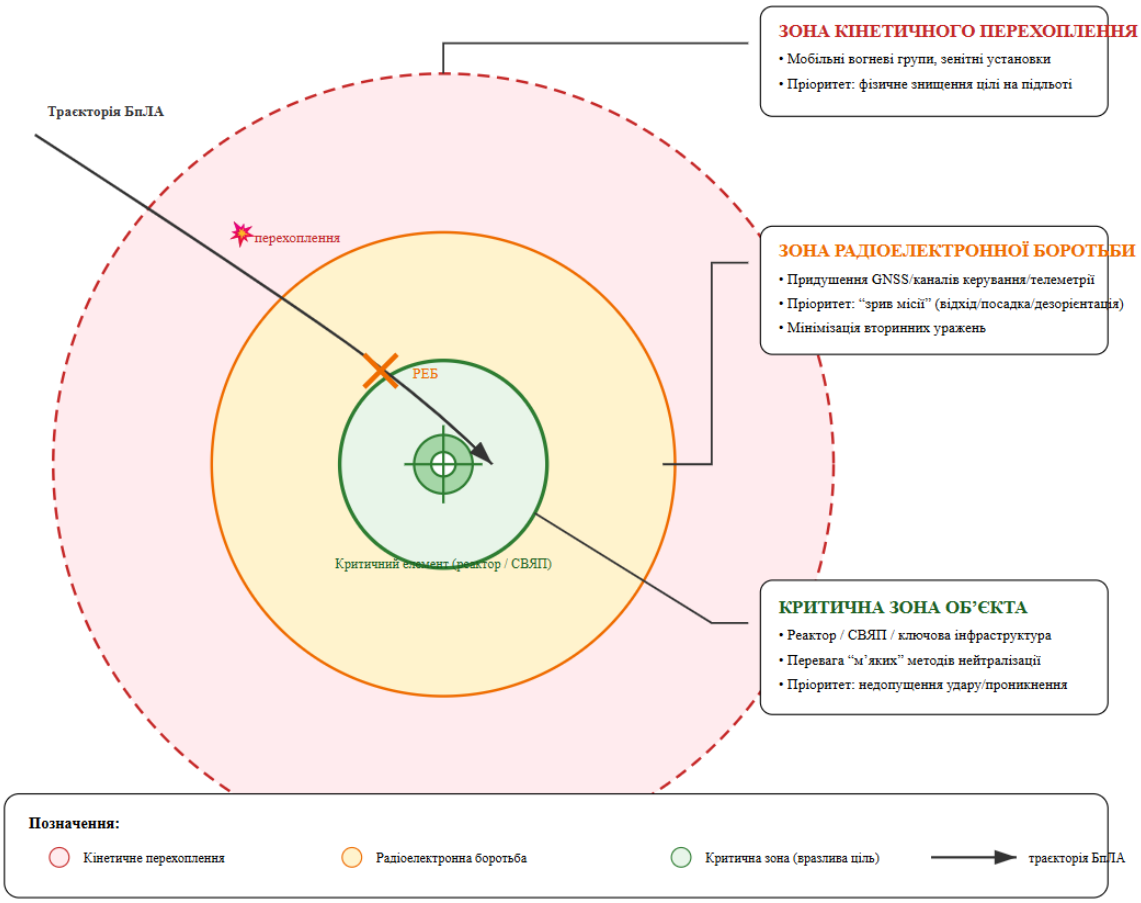

Рисунок 2.6 – Загальний вигляд зонованої моделі нейтралізації

Війна в Україні породила унікальну тактичну відповідь на загрозу масованих атак дешевими дронами-камікадзе - створення мобільних вогневих груп (МВГ). Цей елемент не був передбачений жодним міжнародним стандартом фізичного захисту, але став критично важливим для виживання енергетичної інфраструктури [18; 31].

МВГ являють собою високомобільні підрозділи (на базі пікапів високої прохідності), оснащені великокаліберними кулеметами, зенітними гарматами малої дальності, прожекторами та тепловізійними прицілами. Їхня роль у системі захисту ядерного об'єкта полягає у заповненні «мертвої зони» між високоефективними, але дорогими ракетними комплексами ППО (які недоцільно витрачати на дешеві дрони) та стаціонарною охороною периметра.

Переваги інтеграції МВГ у систему фізичного захисту:

- Економічна ефективність: Вартість ураження цілі кулеметним вогнем є на порядки нижчою за вартість зенітної ракети, що дозволяє протидіяти тактиці виснаження ППО.
- Тактична гнучкість: Здатність швидко змінювати позиції на підступах до АЕС дозволяє створювати «вогневі мішки» на маршрутах прольоту БпЛА [10], які противник намагається прокладати в обхід стаціонарних позицій ППО.
- Автономність: МВГ здатні діяти автономно, отримуючи цілевказівку від системи візуального/акустичного спостереження об’єкта, навіть в умовах порушення централізованого управління ППО.

Науковий аналіз доводить, що МВГ повинні бути формально включені до складу сил реагування в планах фізичного захисту ядерних установок як спеціалізований підрозділ протиповітряної оборони ближньої дії.

Класична модель фізичного захисту (INFCIRC/225) проводить чітку межу: оператор відповідає за захист усередині периметра, держава - за його межами. Повітряні загрози стирають цю межу. ППО не може гарантувати 100% перехоплення всіх цілей, особливо низьколітаючих дронів, до моменту їх входження в зону відповідальності оператора.

Це вимагає створення інтегрованої системи ситуаційної обізнаності, де:

- Дані з радарів ППО про наближення цілей передаються на центральний пульт фізичного захисту АЕС для підготовки персоналу (аварійні протоколи).
- Дані з локальних сенсорів АЕС (акустичних, візуальних) передаються мобільним вогневим групам для точного наведення [39; 47].

Відсутність такої інтеграції призводить до критичних затримок у ланцюжку «виявлення - ураження», що в умовах підльоту дрона (швидкість 150-180 км/год) вимірюється секундами.

2.9.6 Інтеграція загроз від БпЛА у проєктну загрозу

Ескалація повітряних атак Російської Федерації проти об'єктів критичної інфраструктури України у 2022-2024 роках продемонструвала фундаментальну недостатність традиційних підходів до визначення Проектної загрози (Design Basis Threat - DBT). Класична концепція, розроблена відповідно до рекомендацій МАГАТЕ (NSS No. 10) для мирного часу, передбачала дії наземної групи порушників із обмеженим стрілецьким озброєнням [4; 8]. Проте реальні умови сучасної війни довели, що ключова загроза для фізичної цілісності ядерної установки може походити не від людини, яка намагається проникнути через периметр, а від високоточної дистанційно керованої платформи.

У міжнародних документах, передусім INFCIRC/225/Rev.5, не передбачено інтеграції ударних БпЛА або баражуючих боєприпасів як імперативної складової проектної загрози [2; 9]. В результаті Україна зіштовхнулася з необхідністю самостійно оновлювати національну модель загроз (National Threat Assessment), створюючи прецедент нової класифікації ризиків.

На основі емпіричного досвіду бойових дій, нову гібридну модель проектної загрози необхідно структурувати за чотирма функціональними класами повітряних загроз, кожен з яких вимагає специфічних контрзаходів:

1. Ударні БпЛА дальнього радіусу дії («Shahed-type»):

- *Характеристика:* Корисне навантаження 40–50 кг, інерціальна навігація, політ за координатами.
- *Загроза:* Руйнування капітальних споруд, відкритих розподільчих пристроїв (ВРП), дизель-генераторних станцій.
- *Метод протидії:* Тільки кінетичне перехоплення у зовнішній зоні, оскільки РЕБ є малоефективним проти інерціальних систем [11; 18].

2. Тактичні FPV-дрони:

- *Характеристика:* Висока маневреність, ручне керування оператором, кумулятивна бойова частина.

- *Загроза:* Високоточне («хірургічне») ураження вразливих вузлів: силових трансформаторів, вводів кабельних естакад, датчиків АСКРО, камер спостереження.

- *Метод протидії:* Локальний купольний РЕБ (придушення відеоканалу) та фізичний захист (сітки, габіони) [40].

3. Баражуючі боєприпаси:

- *Характеристика:* Складні оптико-електронні системи наведення, захоплення цілі.

- *Загроза:* Ураження систем протиповітряної оборони, що прикривають АЕС, та мобільних вогневих груп.

- *Метод протидії:* Спектральний аналіз сигналів керування, маскування теплового випромінювання техніки.

4. Розвідувальні БпЛА:

- *Характеристика:* Висока висота польоту, потужна оптика.

- *Загроза*: Не завдають прямої шкоди, але виконують функцію коригування ракетного вогню в реальному часі, передаючи координати пошкоджень для повторних ударів.

- *Метод протидії:* Радіоелектронне осліплення супутникової навігації, знищення засобами ППО [10].

Включення БпЛА до проектної загрози змінює саму філософію захисту. Нова концепція фізичного захисту повинна бути побудована не на моделі статики (стіни та паркани), а на моделі динамічних багатовекторних впливів. БпЛА здатні комбінуватися з ракетними та артилерійськими ударами у межах єдиного операційного плану противника, створюючи ефект синергії (Multi-Domain Operation) (Рис. 2.7).

Наприклад, атака «рою» дешевих дронів може використовуватися для виснаження боєкомплекту системи ППО об’єкта, відкриваючи «вікно» для

прориву крилатої ракети. Або розвідувальний дрон може коригувати артилерійський вогонь по маршрутах висування сил реагування, блокуючи їх прибуття до місця інциденту.

Це вимагає перегляду інженерного проектування систем безпеки:

- Перехід від лінійного захисту периметра до сферичного (купольного) контролю простору.
- Об’єднання даних з наземних датчиків вібрації та повітряних радарів в єдину інформаційну систему.

Для забезпечення стійкості ядерної енергетики в умовах війни необхідна реалізація наступних кроків на законодавчому рівні:

- Нормативне визначення БпЛА як елемента DBT: Внесення змін до національних норм з фізичного захисту, що офіційно класифікують безпілотні системи як загрозу проектного рівня.
- Стандартизація засобів РЕБ: Розроблення та затвердження ДІЯРУ «Вимог до систем радіоелектронного захисту ядерних установок», які визначають критерії ефективності, електромагнітної сумісності та безпеки використання РЕБ на АЕС [25; 76].
- Легалізація протоколів взаємодії: Нормативне закріплення порядку прямої оперативної взаємодії між диспетчером АЕС та командним пунктом ППО, минаючи бюрократичні ланцюги узгодження, для скорочення часу реакції на загрозу.
- Вимоги до пасивного захисту: Введення обов’язкових будівельних норм щодо захисту критичного обладнання (трансформаторів) антидроновими інженерними конструкціями (габіони, захисні екрани) на етапі проектування [27; 74].

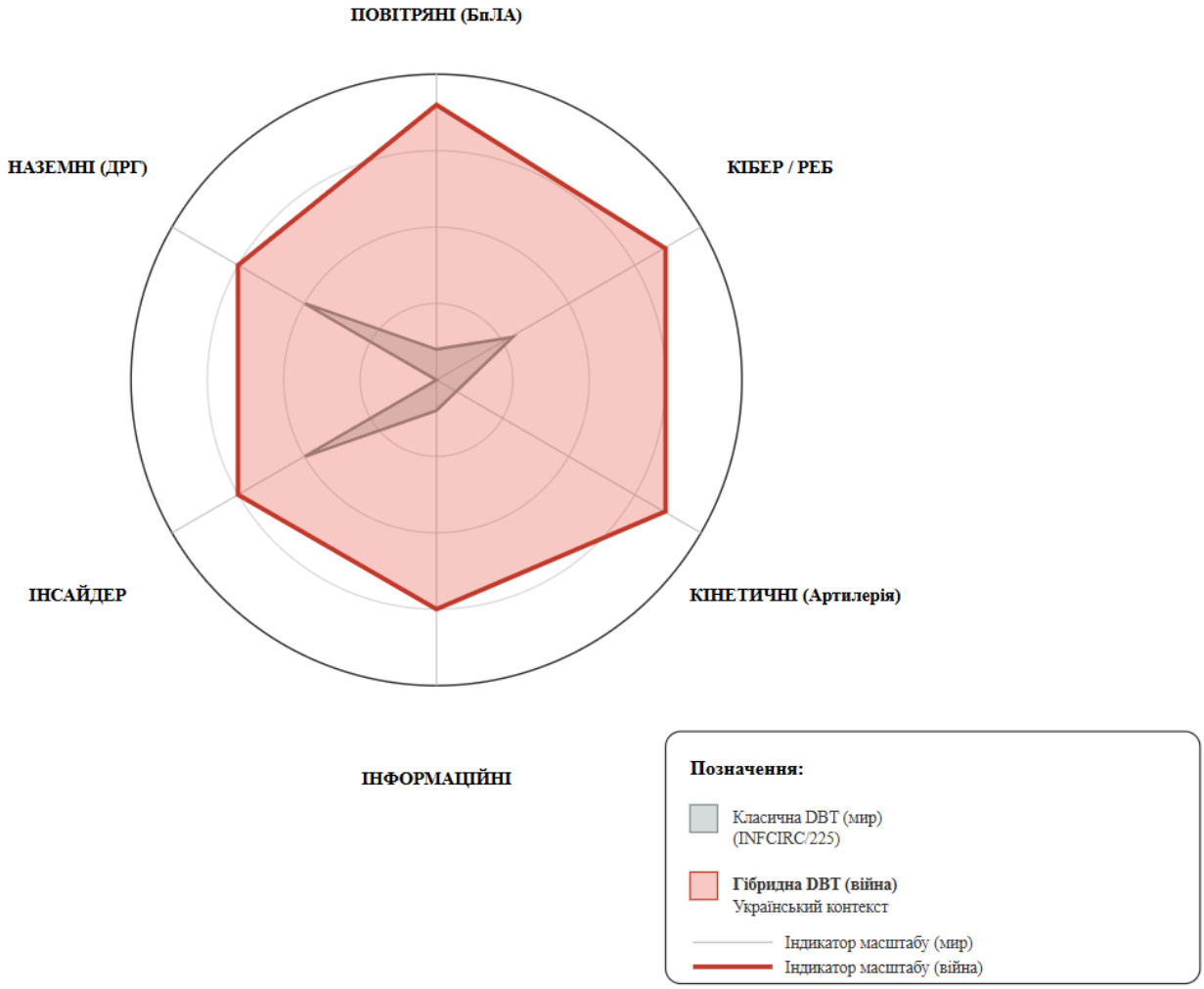

Рисунок 2.7 – Еволюція моделі Проектної Загрози (DBT): перехід до гібридного спектру

2.10 Формування нової моделі

Аналіз сучасного спектру повітряних загроз, каталізований безпрецедентним досвідом застосування ударних та розвідувальних безпілотних літальних апаратів (БпЛА) у війні проти України, дозволяє сформулювати фундаментальний науковий висновок: традиційна система фізичного захисту (СФЗ) ядерних установок вичерпала свій ресурс ефективності в умовах сучасного збройного конфлікту. Парадигма, закладена у фундаментальних документах МАГАТЕ (INFCIRC/225/Rev.5), базувалася на концепції **«захищеності»** (*Security*), метою якої було створення бар'єрів для запобігання проникненню конкретного порушника [2; 9].

Однак емпіричний досвід 2022-2024 років довів, що в умовах систематичного повітряного впливу досягнення повної «захищеності» (тобто нульової ймовірності інциденту) є технічно неможливим. Будь-яка система ППО чи РЕБ має межу насичення. Тому центральним елементом трансформації системи фізичного захисту має стати перехід до концепції «Стійкості».

Нова модель Стійкості відрізняється від традиційного фізичного захисту зміною цільової функції (Рис. 2.8) :

- Традиційна модель: орієнтована на *відмову у доступі*. Головний критерій – цілісність периметра.
- Нова модель: орієнтована на збереження функцій. Головний критерій – здатність ядерної установки продовжувати безпечну роботу (або безпечно зупинитися) навіть в умовах успішного подолання противником першого ешелону оборони.

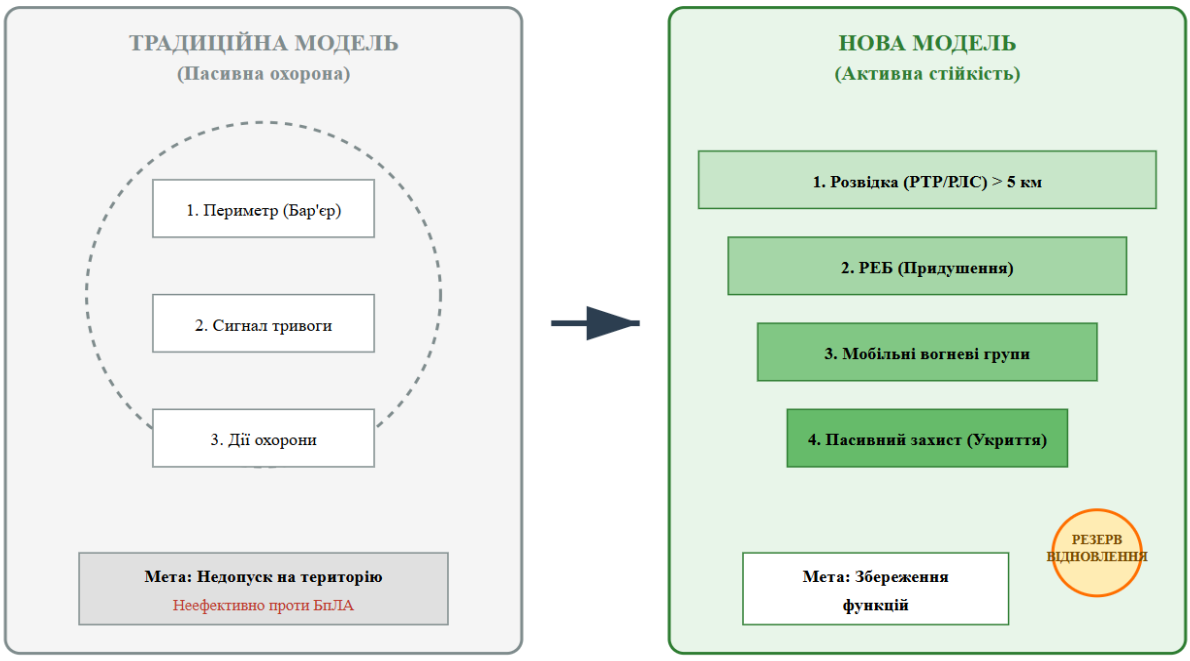

Рисунок 2.8 – Концептуальна схема переходу від традиційної моделі фізичного захисту до моделі активної стійкості

Цей підхід враховує багатофакторний характер загроз та їх комплексну дію у просторі й часі. Він визнає, що загроза більше не є дискретною подією (напад - відбиття), а стає перманентним станом середовища.

Ключовим фактором, що диктує необхідність зміни моделі, є фактор часу. Повітряні загрози, особливо в сегменті FPV-дронів та баражуючих боєприпасів, характеризуються властивістю випереджального впливу.

У класичній моделі наземного нападу існує часовий лаг (T_{lag}) між виявленням порушника на підступах до об'єкта та його контактом з критичним обладнанням. Цей час використовується силами реагування для розгортання. У випадку з БпЛА цей лаг фактично анулюється. Дрон, що рухається зі швидкістю 150 км/год, долає зону візуальної видимості охоронця (500-1000 м) за 12-24 секунди.

Це створює ефект «часової компресії», коли людський цикл прийняття рішень (цикл OODA: Спостереження - Орієнтація - Рішення - Дія) стає занадто повільним. Людина-оператор фізично не встигає ідентифікувати ціль, узгодити рішення з начальником зміни та віддати наказ на застосування антидронової рушниці [10; 19].

З цього випливає критична вимога нової моделі: радикальне скорочення часу реагування через автоматизацію. Система фізичного захисту повинна еволюціонувати у кібер-фізичну систему, де:

- Виявлення здійснюється автоматичними сенсорами (РЛС, акустика) без участі людини.
- Класифікація загрози виконується алгоритмами штучного інтелекту.
- Активація засобів протидії (купольний РЕБ) відбувається в автоматичному або напівавтоматичному режимі («людина в контурі» лише для підтвердження, а не для ініціації) [10; 40].

Формування нової моделі стійкості вимагає відмови від пасивної стратегії («чекаємо, поки перелізуть паркан») на користь стратегії активної Оборони. Це

передбачає розширення зони відповідальності системи фізичного захисту далеко за межі юридичного периметра ядерної установки.

Архітектура нової моделі повинна базуватися на зонованому принципі ешелонування, де кожен ешелон має специфічне завдання щодо повітряної цілі:

- Зона раннього попередження: Охоплює радіус 5-10 км навколо об'єкта. Включає інтеграцію з державною системою ППО та використання пасивних засобів радіорозвідки (РТР) для виявлення джерел випромінювання БпЛА.
- Зона некінетичного впливу: Охоплює радіус 1-3 км. Тут застосовуються інтегровані комплекси РЕБ для придушення навігації та каналів керування.
- Зона кінетичного перехоплення: Зовнішній периметр об'єкта, де розміщуються мобільні вогневі групи.
- Зона пасивного захисту: Безпосередньо критичні вузли (трансформатори), захищені інженерними конструкціями (габіони, сітки) [27].

Деталізована архітектура запропонованої ешелонованої системи, включаючи тактико-технічні характеристики сенсорів та засобів нейтралізації для кожного ешелону, а також алгоритми прийняття рішень оператором, наведено у Додатку В.

Тільки така інтегрована багаторівнева структура здатна створити синергетичний ефект, де недоліки однієї системи (наприклад, неможливість РЕБ збити інерціальний дрон) компенсуються можливостями іншої (кінетичне збиття або сітка).

2.11 Висновки до розділу 2

У другому розділі проведено комплексне дослідження еволюції загроз фізичній ядерній безпеці, проаналізовано трансформацію міжнародно-правового поля та оцінено сучасні виклики, спричинені повномасштабною

військовою агресією проти України. На основі проведеного аналізу зроблено такі висновки:

- **Трансформація парадигми загроз.** Ретроспективний аналіз нападів на ядерні об’єкти (від Другої світової війни до сьогодення) засвідчив перехід від точкових диверсійних актів та превентивних авіаударів до стратегії системного воєнного тиску. Події в Україні 2022–2024 рр. створили безпрецедентний історичний кейс, де великі діючі АЕС (зокрема ЗАЕС) стали об’єктами окупації та регулярних обстрілів, що виходить за межі класичних моделей «проектної загрози».
- **Дефіцит міжнародно-правового захисту.** Встановлено, що чинні норми міжнародного гуманітарного права (зокрема Додаткові протоколи до Женевських конвенцій) містять «правові лакуни», які дозволяють подвійне трактування статусу АЕС у разі їх використання для підтримки військових операцій. Досвід України підтверджує необхідність розробки нових обов’язкових багатосторонніх конвенцій, які б запроваджували режим абсолютної недоторканності ядерних об’єктів незалежно від обставин.
- **Концептуалізація стійкості через «Сім стовпів».** Аналіз ініціативи Генерального директора МАГАТЕ дозволив ідентифікувати перехід від суто технічних регламентів до комплексного забезпечення життєдіяльності об’єктів. Визначено, що в умовах війни ядерна безпека (safety) та ядерна захищеність (security) стають нерозривними, де порушення зовнішнього енергопостачання або тиск на персонал автоматично призводять до деградації всіх рівнів захисту.
- **Криза розподілу відповідальності.** Досліджено архітектуру національних режимів ядерної захищеності та виявлено, що традиційний поділ обов'язків між «державою» та «компетентними органами» втрачає ефективність в умовах окупації. Ситуація, коли de jure відповідальність несе Україна, а de facto контроль здійснює агресор, потребує розробки нових міжнародних протоколів управління ядерними ризиками в зонах збройних конфліктів.

- **Гібридизація ризиків.** Сучасна фізична ядерна безпека більше не може розглядатися лише як захист периметру. Вона включає протидію кібератакам, захист логістичних ланцюгів постачання та забезпечення психологічної стійкості персоналу як критичного елементу фізичного бар’єру безпеки.

3 МЕТОДИКА ОЦІНКИ ВРАЗЛИВОСТІ ЯУ ВІД ЗАГРОЗ НАНЕСЕННЯ ПОВІТРЯНИХ УДАРІВ ІЗ ВИКОРИСТАННЯМ БПЛА

3.1 Концептуальна модель оцінювання вразливості від повітряних загроз

Безпілотні літальні апарати є повітряними суднами, здатними виконувати польотні місії автономно або за допомогою дистанційного керування із землі, без присутності пілота на борту. Існує декілька типів безпілотних літальних апаратів, зокрема: мультироторні апарати, літаки, гелікоптери, гібридні апарати, у тому числі літальні апарати літакового типу, здатні до вертикального зльоту [77].

Такі літальні апарати можуть мати різні розміри та масу. Загалом безпілотні літальні апарати, з огляду на різноманітність їхньої конструкції, розглядаються як універсальні літальні платформи, що дають змогу виконувати різні типи місій за різних погодних умов та в різних місцях експлуатації.

Відповідно до європейських нормативних вимог безпілотні літальні апарати підлягають сертифікації і, за результатами сертифікації, отримують класову приналежність літального апарата (Commission Delegated Regulation, 2019). Клас літального апарата являє собою сукупність технічних вимог, яким повинен відповідати безпілотний літальний апарат певного класу. Виділяють класи C0, C1, C2, C3, C4, C5 та C6. Класи C5 і C6 належать до категорій літальних апаратів, що використовуються для транспортування людей та небезпечних вантажів. Решта класів охоплюють літальні апарати з різною злітною масою, яка не перевищує 25 кг [78].

Необмежений доступ до комплектуючих елементів означає можливість створення саморобного безпілотного літального апарата, льотні характеристики якого залежать виключно від фантазії конструктора. Процес складання безпілотного літального апарата є відносно нескладним і не потребує глибоких

технічних знань. Вартість компонентів, необхідних для побудови безпілотного літального апарата, є значно нижчою за ціну готового безпілотного літального апарата промислового виробництва. У зв'язку з цим безпілотні літальні апарати можуть використовуватися як зброя особами або групами з обмеженими фінансовими ресурсами. У таблиці 3.1 наведено визначені законодавством характеристики, які можуть бути використані для виявлення безпілотних літальних апаратів.

Порівняння габаритних розмірів та ефективної площі відбиття радіолокаційного променя деяких серійно виготовлюваних мультироторних апаратів наведено на Таблиця 3.1. Розміри зазначених апаратів становлять: DJI Mavic Mini 2 - 159x203x56 mm, DJI Phantom 4 - 290x290x196 mm, DJI Matrice 200 - 887x880x378 mm.

Таблиця 3.1 – Характеристики безпілотних літальних апаратів відповідно до законодавчих вимог (переклад і наукове оформлення)

Характеристика / Клас БПЛА	**C0**	**C1**	**C2**	**C3**	**C4**	**C5–C6***
Максимальна злітна маса	≤ 250 г	≤ 900 г або ≤ 80 Дж	≤ 4 кг	≤ 25 кг	≤ 25 кг	змінна
Габаритні обмеження	відсутні	відсутні	відсутні	найбільший розмір ≤ 3 м	відсутні	залежить від конфігурації
Максимальна швидкість	≤ 19 м/с	≤ 19 м/с	не обмежено	не обмежено	не обмежено	не обмежено
Тип енергоживлення	електричний	електричний	електричний	електричний	не регламентовано	залежить від призначення
Регламент щодо частот керування	не встановлено	не встановлено	не встановлено	не встановлено	не встановлено	згідно з авіаційним призначенням
Вимоги у разі втрати зв'язку	немає вимог	обов'язкове безпечне завершення або повернення	те саме	те саме	немає вимог	спеціальні процедури
Рівень звукового тиску	не регламентується	≤ 85 дБ (крім фіксованого крила)	≤ 85 дБ (крім фіксованого крила)	рівень повинен бути зазначений	не регламентується	власні стандарти

Продовження таблиці 3.1

Характеристика / Клас БПЛА	**C0**	**C1**	**C2**	**C3**	**C4**	**C5–C6***
Дистанційна ідентифікація	не потрібна	передача координат у реальному часі	передача серійного номера, швидкості, координат	аналогічно	не потрібна	залежно від категорії

* Класи C5–C6 застосовуються для безпілотних повітряних суден, що виконують спеціалізовані місії, включно з перевезенням людей або небезпечних вантажів.

Завдяки можливості виконувати польоти без пілота на борту на відстані у багато кілометрів та переносити корисне навантаження безпілотні літальні апарати можуть застосовуватися під час терористичних атак проти людей та об’єктів, важливих для державної безпеки, у тому числі об’єктів критичної інфраструктури. Повідомлення про атаки із застосуванням безпілотних літальних апаратів з’являються у засобах масової інформації щоденно.

17 січня 2022 року було здійснено напад на паливні резервуари на об’єктах в Abu Dhabi, унаслідок чого загинуло дві людини [79]. Широко відомим прикладом застосування безпілотного літального апарата є акція Greenpeace на ядерних об’єктах Bugey у Франції [80]. Атака полягала у зіткненні безпілотного літального апарата незвичної форми, що нагадувала силует Superman, з бетонною будівлею, у якій розміщувався ядерний реактор. Безпосереднє влучання у захисну оболонку реактора не призвело до пошкоджень людей чи обладнання, однак засоби масової інформації піддали різкій критиці оператора електростанції та наголосили на неготовності об’єкта до подібних загроз. Представники Greenpeace аргументували, що у разі успішної атаки електростанція могла б стати джерелом екологічного забруднення.

Безпілотні літальні апарати становлять загрозу для об’єктів та людей. Оператори об’єктів, важливих для державної безпеки, зокрема оператори об’єктів критичної інфраструктури (CI), зобов’язані впроваджувати ефективні системи виявлення та нейтралізації безпілотних літальних апаратів.

Метою даного дослідження є демонстрація підходів до побудови систем виявлення та нейтралізації безпілотних літальних апаратів на основі ймовірності їх виявлення та нейтралізації засобами відповідних систем. Застосування запропонованого методу може сприяти підвищенню ефективності систем виявлення та нейтралізації, а отже, і підвищенню рівня безпеки об’єктів, що перебувають під їхнім захистом.

3.2 Типи дронових атак

Безпілотний літальний апарат є універсальною платформою, здатною здійснювати атаку на ціль з різних висот, з різними швидкостями, за різними траєкторіями польоту та з використанням різного бортового обладнання.

Безпілотний літальний апарат може застосовуватися для транспортування вибухового пристрою [81]. Вибух вибухового пристрою впливає на об’єкт атаки через різку зміну тиску, випромінювання інфрачервоного діапазону, тобто тепла, виникнення ударної хвилі у разі вибуху поблизу поверхні землі, а також акустичної хвилі, тобто шуму.

Детонація корисного навантаження, що переноситься безпілотним літальним апаратом під час нападу на людей, може призвести до загибелі, тяжких тілесних ушкоджень або виникнення паніки, якщо атака здійснюється на скупчення людей. Найбільш серйозною атакою із застосуванням безпілотного літального апарата з вибуховим зарядом був напад, здійснений 4 серпня 2018 року у Венесуелі, в місті Caracas, під час якого було здійснено замах на президента країни Nicolas Maduro [82]. Безпілотні літальні апарати переносили вибухові пристрої, які здетонували, спричинивши паніку серед учасників заходу та поранивши сім осіб.

Інша атака такого типу була здійснена у листопаді 2021 року проти прем’єр-міністра Iraq Mustafa al-Kadhimi [83]. Унаслідок нападу було зруйновано будинок у центрі добре охоронюваного району, так званої Green

Zone. Прем’єр-міністр не постраждав, проте будівля, що зазнала атаки, була серйозно пошкоджена.

Атаки з використанням безпілотних літальних апаратів, оснащених вибуховими пристроями, були здійснені 14 вересня 2019 року на нафтові об’єкти компанії Aramco у Saudi Arabia. У результаті нападу об’єкти були охоплені пожежею та тимчасово виведені з експлуатації для проведення ремонтних робіт. Атака призвела до скорочення видобутку нафти вдвічі та спричинила потрясіння на світових нафтових ринках [84]. Для здійснення атак можуть використовуватися літальні апарати серійного виробництва провідних світових виробників [85], прикладом чого стали безпілотні літальні апарати, виготовлені одним із найкращих виробників у світі [86].

Безпілотні літальні апарати можуть застосовуватися для пошкодження об’єкта шляхом безпосереднього фізичного зіткнення або транспортування пристрою чи елемента, який завдає шкоди цілі. Прикладом такого нападу є атака, здійснена невідомими особами у 2021 році на енергетичну систему у штаті Pennsylvania, USA. Атака полягала у використанні безпілотного літального апарата з підвішеним електричним дротом з метою створення короткого замикання та, як наслідок, відключення електропостачання великих територій країни [87].

Безпілотні літальні апарати можуть використовуватися для спостереження за об’єктами, важливими для державної безпеки. Сучасні серійно виготовлювані апарати зазвичай оснащуються камерами, які забезпечують можливість спостереження на великі відстані. Такі камери обладнані системами автофокусування та високоякісною оптикою, що дозволяє отримувати зображення високої якості. Камери, що працюють у діапазоні видимого світла, можуть доповнюватися інфрачервоними сенсорами. Такі камери дають змогу здійснювати відеозйомку в умовах дефіциту видимого освітлення, а також ідентифікувати елементи систем.

Існує ймовірність, що саме камери використовувалися під час нещодавніх польотів безпілотних літальних апаратів над ядерними об’єктами у Sweden. У

січні 2022 року у Sweden було зафіксовано польоти безпілотних літальних апаратів над атомними електростанціями. Несанкціоновані польоти здійснювалися над об’єктами Forsmark Nuclear Water Plant, а також Ringhals та Oskarshamn Nuclear Power Plants [88; 89]. Ці польоти не призвели до втрат серед людей або пошкодження об’єктів, однак їхньою метою могло бути збирання розвідувальної інформації. Електростанція Forsmark є найбільшим виробником електроенергії у Sweden. Камери дозволяють спостерігати за персоналом, отримувати дані про застосовувані технології на об’єкті, його топографію та інші характеристики. Також можливим є використання безпілотних літальних апаратів для перехоплення радіообміну персоналу, у тому числі Internet-комунікацій.

Наведені приклади атак із застосуванням безпілотних літальних апаратів не охоплюють усіх можливих сценаріїв їх використання. З огляду на різні властивості безпілотних літальних апаратів, що зумовлені їх конструкцією, рівень підготовки оператора, а також постійний розвиток технологій безпілотних літальних апаратів, слід вважати, що існує значно більше способів здійснення атак. Проблемою, про яку згадується дедалі частіше, є застосування рою безпілотних літальних апаратів у військових і терористичних цілях для одночасної атаки на об’єкт. Попередні дослідження вказують на можливість використання роїв безпілотних літальних апаратів у цивільних цілях [90], однак не викликає сумнівів, що технологія рою рано чи пізно буде використана у терористичних атаках. Поточний рекорд одночасного польоту рою безпілотних літальних апаратів становить 3281 одиницю [91].

Станом на сьогодні не зафіксовано жодної атаки, здійсненої роєм безпілотних літальних апаратів, на об’єкти, важливі для державної безпеки.

Питання запобігання атакам із застосуванням безпілотних літальних апаратів розглянуто у роботах [92; 93]. Опис безпілотних літальних апаратів як реальної загрози наведено у дослідженні Drone Attacks Against Critical Infrastructure [94].

Доступність комплектуючих на ринку цивільної електроніки створює умови, за яких можливо виготовити індивідуальний або так званий «саморобний» дрон. Його льотні характеристики та функціональні можливості визначаються виключно задумом конструктора. Процес збирання такого апарата не потребує значної технічної підготовки, а сукупна вартість необхідних компонентів суттєво нижча за ціну серійних промислових моделей. Це означає, що потенційні зловмисники, навіть за обмежених фінансових ресурсів, здатні створити БпЛА, придатний для використання як засіб ураження або доставки небезпечного корисного навантаження.

Здатність БпЛА здійснювати польоти на значні відстані, транспортувати корисне навантаження та діяти поза межами традиційних каналів контролю робить їх небезпечним інструментом для атак на об’єкти критичної інфраструктури. Резонансні інциденти наведані в таблиці 3.2.

Таблиця 3.2 – Резонансні інциденти та наслідки від атак БпЛА

Інцидент та рік	**Місце та об’єкт**	**Деталі та методи**	**Наслідки/загрози**
Атака в Абу-Дабі (2022)	**ОАЕ, Абу-Дабі** Паливні резервуари цивільної інфраструктури	Удари із застосуванням безпілотних літальних апаратів по наземних критичних об’єктах	**Людські жертви** Фізичне ураження стратегічного об’єкта (AI Jazeera, 2022)
Інцидент на АЕС Bugey (2018)	**Франція** Будівля реактора АЕС Bugey	Дрон нетипової аеродинамічної форми (стилізація під людину) навмисно спрямований	**Виявлення вразливості** Нездатність системи розпізнавати нестандартні (Pradier, 2018)
Розвідка на АЕС у Швейцарії (2022)	**АЕС Форсмарк** Рінхалс Оскарсгамн	Скоординовані польоти БпЛА з камерами високої роздільної здатності для збору даних	**Розвідувальна загроза** Фіксація маршрутів охорони та елементів фізичного захисту

Одним із резонансних випадків стала атака 17 січня 2022 року на паливні резервуари в Абу-Дабі, унаслідок якої загинули дві особи [79]. Іншим важливим прикладом є інцидент за участю організації Greenpeace на ядерному об’єкті Bugey у Франції [80], коли невідомий дрон нетрадиційної конструкції, стилізований під вигляд персонажа Супермена, був навмисно спрямований на бетонну споруду, що розташована над корпусом реактора. Хоча удар не спричинив пошкоджень інфраструктури, випадок привернув значну увагу громадськості та виявив суттєві прогалини у системі охорони об’єкта. Greenpeace заявила, що у разі застосування вибухового навантаження наслідки могли мати екологічний характер.

3.3 Виявлення дронів

Сучасні системи виявлення безпілотних літальних апаратів, які є елементами антидронових систем захисту об’єктів, функціонують на основі різних ознак безпілотних літальних апаратів [95]. До характеристик безпілотних літальних апаратів, які можуть бути виявлені, належать теплова енергія, що випромінюється літальним апаратом, шум, який створюється пропелерами та двигунами, а також шум, що виникає внаслідок обтікання апарата повітряними потоками, форма літального апарата та електромагнітне випромінювання різних частот, яке створюється системами зв’язку під час польоту. Безпілотні літальні апарати також можуть бути виявлені за допомогою радіолокаційних засобів.

Виявлення теплового випромінювання літального апарата здійснюється за допомогою камер, що працюють в інфрачервоному діапазоні електромагнітного випромінювання [96]. Джерелом тепла на безпілотному літальному апараті може бути літій-полімерна акумуляторна батарея, яка є джерелом електроживлення, обертові електродвигуни, а також система електронного регулятора швидкості, призначена для керування частотою обертання двигунів. Інші електронні системи, зокрема бортовий комп’ютер, не

випромінюють значної кількості тепла. Можливе виявлення об’єкта з температурою, відмінною від температури навколишнього повітряного простору. Водночас безпілотний літальний апарат може бути спроєктований таким чином, щоб тепло, яке він випромінює, ефективно розсіювалося. Методи тепловідведення в літальних апаратах добре відомі з пілотованої авіації. У випадку безпілотних літальних апаратів розсіювання тепла досягається шляхом кріплення радіаторів до елементів, що нагріваються, або розміщення нагрівальних елементів у повітряних потоках.

Акустичне виявлення літального апарата здійснюється за допомогою мікрофонів [97]. Однак виявлення безпілотного літального апарата за допомогою мікрофона є відносно складним завданням. Літальний апарат може бути сконструйований таким чином, що швидкість обертання пропелерів буде низькою. Зменшення швидкості обертання можливе за рахунок використання пропелерів більшого діаметра, у такому випадку рівень шуму, що створюється пропелером, є незначним. Іншим способом зниження рівня шуму може бути виконання планерного польоту. Крім того, звук, що створюється безпілотним літальним апаратом, може маскуватися шумами навколишнього середовища поблизу системи виявлення. Якщо захищений об’єкт розташований у населеній місцевості, джерелами шуму можуть бути громадський транспорт, автомобілі, звуки від розташованих поблизу промислових підприємств, а також шум літаків, що здійснюють посадку у межах міста. Ефективність виявлення акустичного сигналу безпілотного літального апарата може бути підвищена шляхом використання мікрофонних масивів [98; 99; 100].

Інтенсивність звуку визначається як звукова потужність, віднесена до одиниці площі. Інтенсивність є обернено пропорційною квадрату відстані [101]:

$$I(r) \sim \frac{1}{r^2},$$

де (I) — інтенсивність звуку, а (r) — відстань до джерела звуку. Це означає, що інтенсивність звуку, випромінюваного безпілотним літальним апаратом, яка

може бути зареєстрована мікрофоном системи фізичного захисту, зменшується пропорційно квадрату відстані до безпілотного літального апарата, і на великих відстанях таке виявлення може бути дуже складним або взагалі неможливим.

Літальний апарат може бути виявлений із застосуванням візуальних методів [102]. Обов'язковою умовою ефективного виявлення є сприятливі погодні умови. Нічний час, туман та атмосферні опади суттєво знижують ефективність роботи камер. Камера може спостерігати за об'єктом, що летить, однак саме спостереження не є простим завданням. Літак, що летить на відстані 1000 m з розмахом крил 2 m, у полі зору камери являє собою точку з кутом спостереження 0.12 DEG. Для безпілотного літального апарата, який летить на меншій відстані, конус спостереження матиме більший кут огляду, а зображення буде зафіксоване більшою кількістю пікселів. Саме з цієї причини в оптичних системах виявлення застосовуються об'єктиви зі змінною фокусною відстанню. Зображення мультироторного безпілотного літального апарата, що летить на відстані 1000 m, є ще меншим, що ускладнює його виявлення та робить його схожим на точку в небі.

Самого факту спостереження недостатньо. Система аналізу зображень повинна ідентифікувати тип виявленого об'єкта. Таким об'єктом може бути, наприклад, птах. Система аналізу зображень із використанням технологій штучного інтелекту здатна ідентифікувати безпілотний літальний апарат на основі попередньо навчених алгоритмів [103]. Недоліком цього підходу є складність навчання системи коректному розпізнаванню об'єктів. Такий процес є тривалим і складним та потребує тисяч фотозображень [104]. Крім того, якщо зловмисник знає принципи роботи системи виявлення, він може сконструювати безпілотний літальний апарат незвичної форми, наприклад, у вигляді згаданого раніше Superman або у формі птаха. У разі атаки з використанням такого апарата система розпізнавання зображень може бути введена в оману.

Виявлення безпілотного літального апарата можливе також шляхом виявлення радіообміну між літальним апаратом та наземною станцією керування [105]. Для зв'язку використовується електромагнітне

випромінювання різних частот. Нині найбільш поширеними частотами керування безпілотними літальними апаратами є 2.4 GHz, 5.8 GHz, 433 MHz та 868 MHz [106]. Дедалі частіше зв'язок між UAV та наземною станцією може підтримуватися за допомогою GSM-зв'язку [107].

Метод виявлення за радіообміном є, однак, ненадійним та малоефективним. Однією з причин низької ефективності є можливість виконання безпілотної місії без необхідності зв'язку з наземною станцією під час польоту. Під час планування місії оператор може використовувати програмне забезпечення, у якому на карті задаються точки польоту літального апарата, так звані waypoints, а у більш розвинених системах визначаються дії, які апарат повинен виконати у певній точці, наприклад скидання вантажу або виконання фотозйомки. Застосунки для керування серійно виготовлюваними безпілотними літальними апаратами провідних виробників постачаються разом із апаратом. У випадку саморобних систем програмне забезпечення, зазвичай open-source, може бути безкоштовно завантажене з Internet. Якщо під час польоту безпілотний літальний апарат передає повідомлення на наземну станцію, такий радіообмін може бути виявлений детектором електромагнітного випромінювання, після чого антидронова система може вжити заходів з нейтралізації.

Велика кількість частот, на яких може здійснюватися зв'язок, а також можливість використання нестандартних частот значно ускладнюють процес виявлення. Пристрій виявлення повинен сканувати весь спектр електромагнітного випромінювання та визначати, які частоти використовуються для зв'язку між безпілотним літальним апаратом і наземною станцією, а які призначені для інших цілей. На ринку існують пристрої для виявлення радіообміну, орієнтовані на конкретні моделі безпілотних літальних апаратів. Одним із таких пристроїв є DJI AeroScope (DJI), який у стаціонарному виконанні здатний виявляти радіообмін між безпілотним літальним апаратом та оператором на відстані до 50 km, а у портативному виконанні — до 5 km.

Інтенсивність радіосигналу зменшується пропорційно квадрату відстані та описується аналогічно до акустичного сигналу рівнянням (1).

Також можливе виявлення радіообміну між безпілотним літальним апаратом та оператором із використанням пристроїв Software Defined Radio (SDR) [108]. Такі пристрої є відносно дешевими. Завдяки можливості програмування вони можуть поєднувати функції виявлення, визначення місцезнаходження, глушіння та підміни GPS-сигналу.

Останнім методом виявлення безпілотних літальних апаратів є радіолокаційний метод [109]. Радіолокаційні засоби здатні виявляти безпілотні літальні апарати, що летять на великих висотах і на значній відстані від захищеного об’єкта. Виявлення здійснюється за допомогою радарів, що працюють у різних частотних діапазонах [110; 111]. У конструкції радіолокаційних систем застосовуються також методи підвищення ефективності виявлення об’єктів, зокрема beamforming [112]. Ефективність радіолокаційних систем зростає зі зменшенням відстані між безпілотним літальним апаратом і антеною радара [113; 114], оскільки при цьому підвищується відношення сигналу до шуму.

Радіолокаційні засоби широко застосовуються на практиці, однак їх ефективність значною мірою залежить від розташування захищеного об’єкта. Безпілотні літальні апарати можуть виконувати польоти на дуже малих висотах. Вони оснащуються засобами вимірювання висоти польоту, зокрема барометрами, ультразвуковими датчиками або lidar, і здатні здійснювати політ на висоті близько 50 cm над поверхнею землі. Політ на малій висоті над нерівною, пересіченою місцевістю є причиною того, що радар не виявляє літальний апарат. Безпілотний літальний апарат також не буде виявлений, якщо територія навколо захищеного об’єкта заросла кущами або деревами.

3.4 Методи нейтралізації дронів

Існуючі методи нейтралізації безпілотних літальних апаратів не є повністю ефективними. Тому системи нейтралізації зазвичай складаються з пристроїв, робота яких ґрунтується на різних фізичних принципах. Одним із методів нейтралізації безпілотного літального апарата є його знищення за допомогою лазерного випромінювання [115]. Високоенергетичний лазерний промінь після влучання може спричинити падіння безпілотного літального апарата. Такі системи є ефективними за сприятливих погодних умов. У тумані або за наявності атмосферних опадів лазерне випромінювання розсіюється на молекулах води. Лазерний пристрій встановлюється на гімбалі, що забезпечує можливість наведення у будь-якому напрямку.

Недоліком цього методу є те, що нейтралізований безпілотний літальний апарат падає на землю некеровано. Падіння апарата може мати серйозні наслідки, оскільки він може впасти на людей або на чутливі елементи інфраструктури захищеного об’єкта. Зазвичай під час падіння безпілотний літальний апарат зазнає значних пошкоджень, унаслідок чого дані, збережені на його бортовому комп’ютері, стають непридатними для зчитування. Це унеможливлює ідентифікацію оператора та притягнення його до відповідальності.

Іншим методом нейтралізації є перехоплення безпілотного літального апарата за допомогою сітки [116]. Така сітка може запускатися з сіткомета, який використовується персоналом служби безпеки об’єкта з землі, або ж із сіткомета, встановленого на іншому безпілотному літальному апараті, керованому співробітником служби безпеки об’єкта. Цей метод є ефективним за умови пострілу з близької відстані, яка може становити до 30 m. Безпілотний літальний апарат, упійманий у сітку, до якої може бути прикріплений парашут, спускається з малою швидкістю, унаслідок чого не зазнає пошкоджень під час зіткнення з поверхнею землі. Дані з бортового комп’ютера безпілотного

літального апарата, захопленого таким способом, можуть бути зчитані, що дає змогу ідентифікувати оператора.

Ще одним способом нейтралізації є виведення з ладу електронних компонентів безпілотного літального апарата за допомогою електромагнітного імпульсу [117]. Високоенергетичний електромагнітний імпульс здатний пошкодити електронні компоненти апарата, такі як бортовий комп'ютер або системи електронних регуляторів швидкості, які керують обертанням двигунів. Дальність дії такого імпульсу може становити декілька кілометрів. Застосування цього типу зброї може призвести до пошкодження типового безпілотного літального апарата.

Конструктор, який обізнаний із впливом електромагнітного поля на електроніку, може ізолювати її від дії зовнішнього електромагнітного поля шляхом використання так званого Faraday shield [118]. Крім того, на електричних проводах усередині корпусу безпілотного літального апарата можуть встановлюватися фільтри, призначені для відсікання імпульсів струму високої інтенсивності, індукованих електромагнітним полем антидронових систем. При цьому електромагнітний імпульс, що випромінюється антидроновим пристроєм, може впливати й на інші електронні засоби, зокрема ті, що використовуються для керування технологічними процесами на захищеному об'єкті.

Пристрої глушіння сигналів зв'язку між літальним апаратом та наземною станцією випромінюють електромагнітне випромінювання у різних частотних діапазонах, які охоплюють частоти, що використовуються безпілотними літальними апаратами. Зв'язок між безпілотним літальним апаратом і наземною станцією порушується шляхом випромінювання електромагнітної хвилі з плоским спектром та однаковою інтенсивністю шуму для всіх випромінюваних частот. Якщо завадний сигнал випромінюється з достатньою потужністю, оператор втрачає можливість керувати літальним апаратом. Пристрій глушіння буде неефективним у разі, якщо оператор запрограмує безпілотний літальний апарат до зльоту таким чином, щоб він виконував місію повністю автономно.

Поширеним методом нейтралізації літального апарата у польоті є спотворення сигналу супутникової навігаційної системи шляхом глушіння (jamming) або підміни сигналу (spoofing) [119]. У разі глушіння завадний пристрій випромінює сигнал на частотах, на яких працює система позиціонування. Потужність завадного сигналу перевищує потужність супутникового сигналу. Супутниковий приймач на борту безпілотного літального апарата дезорієнтується і не здатний коректно визначити своє місцеположення.

Підміна сигналу полягає у тому, що spoofing-пристрій випромінює сигнал із фальсифікованими координатами. Літальний апарат оцінює своє положення на основі хибного сигналу та прямує до точки, вказаної пристроєм, що формує помилкове положення, замість запланованої цілі, унаслідок чого атака стає неефективною.

Відповіддю на такі методи протидії може бути застосування навігаційних рішень, які дозволяють визначати положення літального апарата за відсутності доступу до сигналів супутникової системи позиціонування. Навігаційні системи в умовах відсутності супутникового сигналу визначають положення апарата на основі показів lidar, ультразвукових далекомірів, а також камер, що працюють у видимому або інфрачервоному діапазоні [120]. Іншим методом навігації без використання супутникової системи позиціонування є розгортання наземних станцій, які випромінюють сигнал положення, та здійснення навігації на основі тріангуляції [121].

Низька ефективність нині застосовуваних систем нейтралізації зумовлює необхідність пошуку нових рішень. Одним із нещодавно запропонованих підходів є порушення польоту безпілотного літального апарата шляхом введення в оману алгоритмів аналізу зображення, яке фіксується камерою апарата [122]. Цей метод використовує вразливість алгоритмів аналізу зображень, за якої алгоритм некоректно визначає відстань до перешкоди внаслідок освітлення камери з двох різних джерел світла. Керуючи

інтенсивністю освітлення, можна змусити алгоритм зафіксувати уявну перешкоду та зупинити політ безпілотного літального апарата.

3.5 Побудова системи виявлення БпЛА

Системи виявлення безпілотних літальних апаратів, які наразі виробляються, не є достатньо ефективними для виявлення безпілотного літального апарата у польоті [95]. У зв`язку з цим такі системи повинні базуватися на пристроях, робота яких грунтується на різних принципах. Засоби виявлення у системах фізичного захисту добираються шляхом оцінювання імовірності виявлення небажаної активності за заданих умов [27]. Аналогічно, системи виявлення безпілотних літальних апаратів, що складаються з пристроїв, які працюють за різними принципами, також повинні будуватися на основі імовірності виявлення безпілотного літального апарата за заданих умов.

Для кожного пристрою виявлення імовірність виявлення за заданих умов експлуатації та у потрібний часовий інтервал повинна бути експериментально оцінена. Задані умови експлуатації пристрою - це умови, у яких пристрій буде працювати (Рис. 3.1). Таким чином, імовірність виявлення безпілотного літального апарата оцінюються для:

- різних погодних умов (*WC*), зокрема вологості, туману, дощу, снігу, відсутності опадів, високих температур, низьких температур, відсутності вітру, сильного вітру, середовища з високим рівнем шуму, середовища з низьким рівнем шуму тощо;
- будь-якого часу доби, вдень або вночі (t);
- виявлення у певній локації захищеного об`єкта (*L*), наприклад на рівнинній місцевості, у гірській місцевості, на території, вкритій кущами, у лісі, на забудованій або незабудованій території тощо;
- різних типів безпілотних літальних апаратів (*T*), таких як мультироторні апарати, літаки, гелікоптери, апарати з незвичною формою;

- різних типів двигунів (*M*), зокрема електричних або двигунів внутрішнього згоряння;
- використання різних способів виконання місії літального апарата (*PAM*), включаючи політ на великій висоті, політ на малій висоті, політ на високій швидкості, політ на низькій швидкості, прямолінійний політ, політ за складною траєкторією;
- використання за різного рівня компетентності персоналу фізичної охорони, відповідального за експлуатацію засобів виявлення (*C*), зокрема добре підготовленого працівника або працівника без досвіду;
- використання за різних відстаней (*D*) між безпілотним літальним апаратом у польоті та пристроєм виявлення, зокрема на великій або малій відстані.

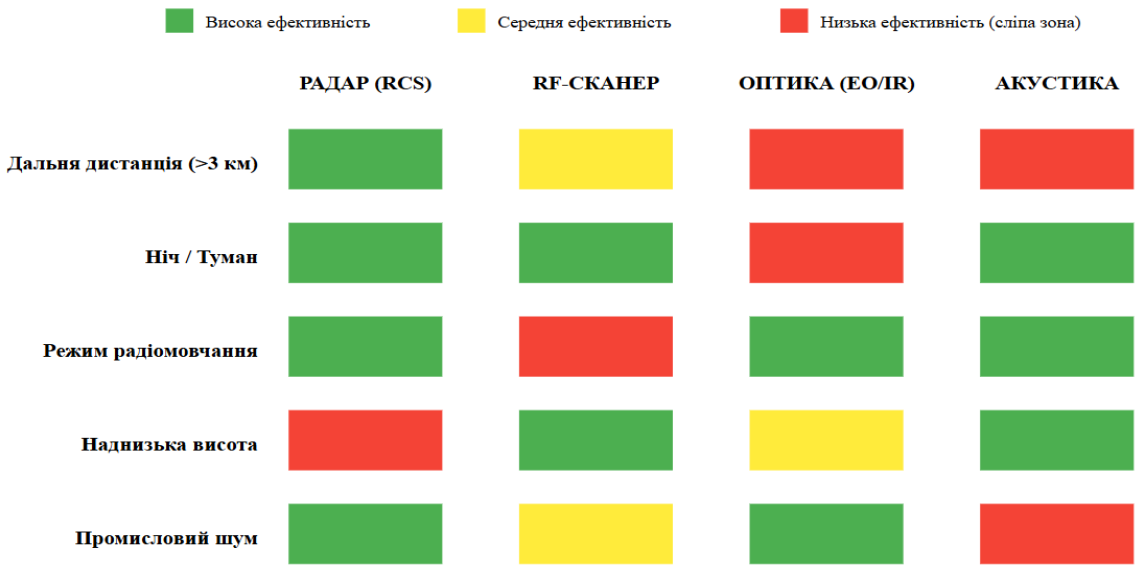

Рисунок 3.1 – Порівняльна ефективність сенсорів системи виявлення БпЛА в залежності від умов навколишнього середовища

Оцінювання імовірності виявлення може здійснюватися шляхом підрахунку кількості виявлень безпілотного літального апарата на кожні сто польотів. Якщо за заданих умов буде зафіксовано сто виявлень зі ста польотів безпілотного літального апарата, імовірність становитиме 100 відсотків, а якщо

не буде виявлено жодного польоту, імовірність дорівнюватиме 0 відсотків. Додатковим параметром, який повинен бути оцінений, є час виявлення, відомий як required time. Required time - це такий момент, коли безпілотний літальний апарат виявляється достатньо рано для активації будь-яких запланованих процедур у разі атаки [27]. Однією з таких процедур може бути приведення в дію засобів нейтралізації безпілотного літального апарата та наведення їх на апарат, що здійснює атаку.

Імовірність виявлення безпілотного літального апарата за заданих умов і у required time позначаються як P_{ux}, де індекс *ux* відповідає *x*-му пристрою виявлення.

Загальна імовірність виявлення безпілотного літального апарата системою, що складається з N пристроїв, визначаються формулою:

$$P_{totalD} = 1 - (1 - P_{u1})(1 - P_{u2}) \dots (1 - P_{uN}),$$

де:

$$P_{ux} = P_{ux}(WC, t, L, T, M, PAM, C, D)$$

Припустимо, що створюється система виявлення безпілотних літальних апаратів, яка складається з трьох пристроїв виявлення. У наведеному прикладі, коли система складається з трьох пристроїв, за результатами випробувань отримано три значення імовірностей P_{u1}, P_{u2} та P_{u3}. Для такої системи формула матиме вигляд:

$$P_{totalD} = 1 - (1 - P_{u1})(1 - P_{u2})(1 - P_{u3})$$

Розглянемо систему, що складається з трьох пристроїв виявлення, для яких імовірність виявлення за заданих умов і у required time становить відповідно P_{u1} = 0.33, P_{u2} = 0.65, P_{u3} = 0.54. Це означає, що зі ста польотів ці пристрої виявили безпілотний літальний апарат відповідно:

u1 -> 33 рази

u2 -> 65 разів

u3 -> 54 рази

Отже, обчислена загальна імовірність виявлення безпілотного літального апарата системою дорівнює:

$$P_{totalD} = 1 - (1 - 0.33)(1 - 0.65)(1 - 0.54)$$

$$P_{totalD} = 0.89$$

Іншими словами, P_{totalD} = 89 відсотків. Цей результат свідчить, що система, сформована з P_{u1}, P_{u2} та P_{u3}, виявляє UAV з імовірністю 89 відсотків, тобто зі ста польотів виявляється 89 польотів. Якщо б об'єкт був захищений такою системою, одинадцять з кожних ста польотів залишалися б невиявленими, і атака могла б бути успішно реалізована.

Завданням керівника захищеного об`єкта є визначення мінімального порогового значення P_{totalD}, нижче якого система вважається неефективною [7]. Якщо система визнається неефективною, необхідно вжити заходів для підвищення значення P_{totalD}. Це може бути досягнуто шляхом:

- зміни умов виявлення, наприклад, якщо пристрій неефективно працює на відкритій території, вкритій кущами, можливе видалення кущів;
- збільшення кількості засобів виявлення у системі за умови, що додаткові пристроі працюють за принципами, відмінними від уже застосованих;
- заміни пристрою з найнижчою імовірністю виявлення на більш ефективний; або
- якщо на ринку відсутня більш ефективна модель пристрою, застосування превентивних заходів, описаних далі у цій статті, з метою запобігання реалізації атаки.

Припустимо, що описана вище система виявлення безпілотних літальних апаратів не відповідае очікуванням і що загальна імовірність виявлення повинна бути вищою. Розробник системи може підвищити імовірність

виявлення шляхом додавання до системи інших пристроїв виявлення, які працюють за принципами, відмінними від тих, що вже використовуються. Нехай додаткові пристроі мають імовірність виявлення безпілотного літального апарата за заданих умов і у required time відповідно P_{u4} = 0.50 та P_{u5} = 0.60. Таким чином, розглянута система складається з п`яти пристроїв виявлення. Загальна імовірність виявлення безпілотного літального апарата такою системою становить:

$$P_{totalD} = 1 - (1 - P_{u1})(1 - P_{u2})(1 - P_{u3})(1 - P_{u4})(1 - P_{u5})$$
$$P_{totalD} = 1 - (1 - 0.33)(1 - 0.65)(1 - 0.54)(1 - 0.50)(1 - 0.60)$$
$$P_{totalD} = 0.98$$

Іншими словами, P_{totalD} = 98 відсотків. Цей результат означає, що система, яка мала неприйнятну імовірність виявлення безпілотного літального апарата, після доповнення іншими засобами стає високоефективною, а загальна імовірність виявлення зростає приблизно на 10 відсотків до рівня 98 відсотків. Якщо б об’єкт був захищений такою системою, лише два з кожних ста польотів залишалися б невиявленими, і атака могла б бути успішно реалізована.

Під час аналізу засобів виявлення персоналу безпеки необхідно пам`ятати декілька принципів, які визначають ефективність, а отже і імовірність виявлення:

- засоби виявлення повинні бути абсолютно незалежними один від одного. Незалежність означає наявність різних джерел живлення, окремих систем захисту від переривання роботи, а також відсутність будь-якого взаємного впливу, наприклад у вигляді порушення роботи через сильне електромагнітне поле;
- засоби виявлення та вся система виявлення повинні періодично перевірятися. Необхідність періодичного контролю зумовлена тим, що будь-який технічний обект може бути пошкоджений, що призведе до різкого зниження значення PtotalD, можливо навіть нижче допустимого порогового

значення. Крім того, кожний технічний обект з часом старіе. Систему виявлення також слід тестувати щоразу, коли змінюються умови ii експлуатації, наприклад у разі будівництва нових будівель або споруд на територіі захищеного об`єкта [27];

- пріоритетом для керівника захищеного об`єкта повинно бути забезпечення ефективного виявлення безпілотного літального апарата, що здійснює атаку, а не вартість побудови системи.

Система виявлення безпілотних літальних апаратів вважається правильно спроєктованою, якщо значення P_{totalD} перевищує допустиме мінімальне порогове значення.

Під час проєктування системи виявлення безпілотних літальних апаратів для захищеного обекта засоби виявлення слід добирати таким чином, щоб їх робота не справляла негативного впливу на функціонування інших пристроів, що використовуються на цьому обекті. Такий негативний вплив може включати, наприклад, електромагнітне поле, яке випромінює радіолокатор. Якщо таке поле, його частота або інтенсивність будь-яким чином заважатимуть роботі захищеного обекта, від такого засобу виявлення слід відмовитися або застосувати заходи щодо зменшення впливу електромагнітного поля на обладнання захищеного обекта, наприклад шляхом використання відповідного екранування [118].

3.6 Методологія нейтралізації БпЛА

Пристроі для нейтралізації безпілотних літальних апаратів, які наразі доступні на ринку, не забезпечують ефективного захисту обекта. У звязку з цим система нейтралізації безпілотних літальних апаратів повинна будуватися з використанням різних засобів нейтралізації таким чином, щоб імовірність нейтралізації була достатньо високою. Застосування пристроів, що працюють за різними принципами, забезпечує виконання системою свого завдання за будь-яких умов, тобто нейтралізацію безпілотного літального апарата.

Засоби нейтралізації безпілотних літальних апаратів повинні добиратися до складу системи після оцінювання їх ефективності, тобто імовірності нейтралізації безпілотного літального апарата за заданих умов і у потрібний час. Оцінювання імовірності нейтралізації безпілотного літального апарата повинно проводитися за тими самими умовами, за яких оцінюються засоби виявлення безпілотних літальних апаратів [27].

Ефективність нейтралізації повинна оцінюватися:

- з урахуванням погодних умов (*WC*), зокрема прозорості повітря, сили вітру тощо;
- у будь-який час доби, вдень або вночі (*t*);
- з урахуванням умов місцевості (*L*), таких як хвилястий рельеф, висота рослинності поблизу об`єкта, що захищається, наявність будівель, щільність населення території;
- з урахуванням типу літального апарата (*T*), зокрема мультироторного апарата, літака, гелікоптера або апарата з незвичною формою;
- для різних типів двигунів (*M*), таких як електричні або двигуни внутрішнього згоряння;
- з урахуванням різних способів реалізації атаки (*PAM*), зокрема польоту на великій або малій висоті, польоту з різною швидкістю, польоту за різними траєкторіями тощо;
- з урахуванням рівня компетентності персоналу фізичноі охорони, відповідального за експлуатацію системи (*C*);
- для різних відстаней (*D*) між безпілотним літальним апаратом у польоті та пристроем виявлення (велика відстань, мала відстань).

Оцінювання імовірності нейтралізації безпілотного літального апарата кожним окремим засобом нейтралізації може виконуватися шляхом підрахунку кількості ефективних дій, у результаті яких безпілотний літальний апарат припиняе становити загрозу для захищеного об`єкта, на кожні сто спроб.

Додатковим параметром, який повинен бути оцінений, е час, необхідний для ефективноі нейтралізації безпілотного літального апарата. Необхідний час -

це такий момент, коли безпілотний літальний апарат нейтралізується достатньо швидко, щоб не мати можливості успішно завершити атаку, наприклад, настільки швидко, щоб апарат не зміг доставити вибуховий пристрій на відстань, за якої його вибух спричинив би втрати, або настільки швидко, щоб апарат не зміг зафіксувати зображення для виконання розвідувальної місії.

Імовірність нейтралізації безпілотного літального апарата окремим пристроєм позначається символом P_{uy}, де індекс *uy* відповідає *y*-му засобу нейтралізації.

Загальна імовірність нейтралізації безпілотного літального апарата системою, що складається з *N* пристроїв, визначається формулою:

$$P_{totalN} = 1 - (1 - P_{u1})(1 - P_{u2}) \dots (1 - P_{uN}),$$

де:

$$P_{uy} = P_{uy}(WC, t, L, T, M, PAM, C, D)$$

Розглянемо ситуацію, коли безпілотний літальний апарат, що здійснює атаку, був виявлений, а система нейтралізації складається з трьох засобів нейтралізації. Імовірність нейтралізації безпілотного літального апарата, визначена для заданих умов і у required time, становить відповідно: $P_{u1} = 0.5$, $P_{u2} = 0.65$, $P_{u3} = 0.64$. Це означає, що ці пристроі нейтралізували безпілотний літальний апарат зі ста спроб відповідно:

u1 -> 50 times
u2 -> 65 times
u3 -> 64 times

Отже, обчислена загальна імовірність нейтралізації безпілотного літального апарата такою системою дорівнює:

$$P_{totalN} = 1 - (1 - 0.5)(1 - 0.65)(1 - 0.64)$$
$$P_{totalN} = 0.94$$

Іншими словами, $P_{total}N$ = 94 percent. Цей результат означає, що система, яка складається із засобів P_{u1}, P_{u2} та P_{u3}, нейтралізує UAV з імовірністю 94 percent, тобто приблизно 94 польоти зі 100.

Якщо персонал безпеки прагне визначити імовірність нейтралізації безпілотного літального апарата системою, слід застосовувати декілька правил, які визначають ефективність, а відповідно і імовірність нейтралізації:

- засоби нейтралізації повинні бути абсолютно незалежними один від одного. Незалежність означає, що ці пристроі повинні мати різні джерела живлення, окремі системи захисту від переривання роботи, а також не повинні чинити будь-якого взаемного впливу, наприклад шляхом порушення роботи через сильні електромагнітні поля;
- засоби нейтралізації, а також вся система нейтралізації, повинні періодично перевірятися. Необхідність періодичного контролю зумовлена тим, що будь-який технічний обект може бути пошкоджений, що призведе до різкого зниження значення P_{totalN}, можливо навіть нижче допустимого порогового значення. Крім того, кожний технічний обект з часом старіє. Систему нейтралізації слід також перевіряти кожного разу, коли змінюються умови ii експлуатації. Такою зміною може бути, наприклад, будівництво будівель або споруд на територіі захищеного об`єкта;
- пріоритетом для керівника захищеного об`єкта повинно бути забезпечення ефективноі нейтралізації безпілотного літального апарата, що здійснює атаку, а не вартість побудови системи.

Система нейтралізації безпілотних літальних апаратів вважається належно побудованою, якщо значення P_{totalN} перевищує допустиме мінімальне порогове значення.

Під час проєктування системи нейтралізації безпілотних літальних апаратів для захищеного обекта засоби нейтралізації повинні добиратися таким чином, щоб іх робота не спричиняла негативного впливу на сам обект або на людей, які працюють поблизу нього. Такий негативний вплив може включати,

наприклад, падіння безпілотного літального апарата внаслідок його знищення або ураження лазерним пристроем.

Кінетична енергія безпілотного літального апарата, що падае, описуеться формулою:

$$E_K = \frac{1}{2} m\, v^2,$$

де:

m - маса безпілотного літального апарата, v - швидкість, з якою безпілотний літальний апарат ударяється об перешкоду.

Наслідком падіння безпілотного літального апарата, навіть за низькоі кінетичноі енергіі, може бути травмування або загибель людей, а у разі влучання у технічний обект - порушення його функціонування. Якщо ризик, повязаний із падінням безпілотного літального апарата на установки або людей, е неприйнятним, необхідно застосовувати заходи зі зменшення ризику, наприклад шляхом спорудження захисних накриттів.

Загальна імовірність успішного функціонування усіеі антидронової системи, що складаеться з системи виявлення та системи нейтралізації, визначаеться формулою [27]:

$$P_{total} = P_{totalD} \times P_{totalN}$$

Значення P_{totalD} та P_{totalN}, як зазначено вище, знаходяться у діапазоні (0-100 percent). Добуток цих двох значень не може перевищувати менше з них, тому:

$$P_{total} < min\{P_{totalD}, P_{totalN}\}$$

3.7 Проведення оцінки вірогідності виявлення та нейтралізації

Ефективність описаного методу залежить від використання коректних значень імовірностей виявлення та нейтралізації пристроів, що застосовуються

під час побудови антидронових систем. Як імовірність виявлення, так і імовірність нейтралізації повинні визначатися експериментально з метою підтвердження правильності параметрів досліджуваних пристроів. Коректне значення імовірності може бути отримане:

- шляхом проведення випробувань виробником пристрою або системи;
- шляхом проведення випробувань персоналом безпеки захищеного об`єкта, який під час побудови антидронової системи повинен забезпечити виконання вимог щодо досягнення принаймні порогових значень імовірності виявлення та нейтралізації безпілотного літального апарата;
- шляхом проведення випробувань державною установою, спеціально призначеною для цієї мети, яка повинна визначати ефективність пристроів об`єктивно та незалежно від виробника досліджуваного обладнання.

Надійність технічних обектів, з яких складається запропонована система виявлення на початку ії експлуатації, може бути отримана від виробника. Рівень значущості при цьому не повинен перевищувати 5 percent. Проте з часом, з метою оцінювання надійності обектів, необхідно проводити випробування на ненадійність на репрезентативній вибірці.

Метод вибіркового дослідження містить два елементи: схему відбору (наприклад, рівноймовірний відбір або відбір з імовірністю, пропорційною розміру) та процедуру прогнозування (оцінювання). Разом ці два елементи утворюють основу для розрахунку чисельності генеральної сукупності. Рекомендується використання статистичних методів. Статистичні методи вибірки дозволяють сформувати вибірку, репрезентативну для генеральної сукупності. Кінцевою метою е прогнозування (екстраполяція або оцінювання) значення параметра (змінної), що спостерігається у вибірці, для генеральної сукупності, що дозволяе визначити, чи містить генеральна сукупність суттеві нерегулярності, і якщо так, то якою е іх величина.

Розмір вибірки n розраховуеться на основі такои інформації:

- чисельність генеральної сукупності;

- рівень довіри, визначений з нормального розподілу;
- максимально допустима похибка (зазвичай 5 percent), очікувана похибка, обрана оператором відповідно до його професійного судження та на основі інформації з попередніх випробувань;
- середньоквадратичне відхилення похибок.

Розмір вибірки визначається за формулою [123]:

$$n = \frac{N\,u^2\sigma^2}{\Delta^2(N-1) + u^2\sigma^2},$$

де:

N - чисельність генеральної сукупності,

u - значення для заданого рівня значущості,

σ - середньоквадратичне відхилення,

Δ - граничне відхилення.

Призначення державної установи для проведення випробувань повинно сприяти стандартизації вимог до антидронових засобів і забезпечувати, щоб пріоритетом була ефективність антидронової системи, а не її вартість.

Оцінювання імовірності виявлення та нейтралізації антидронових систем дозволяє перевірити, чи є конкретна система ефективною та чи відповідає вона вимогам щодо перевищення мінімального порогового значення. Якщо певна система не відповідає встановленим для неї вимогам, вона повинна бути вдосконалена. Ефективність систем може бути підвищена шляхом заміни засобів виявлення та нейтралізації на більш ефективні або шляхом зміни умов їх експлуатації. Наприклад, зміна умов може полягати у видаленні кущів і дерев у безпосередній близькості до захищеного об`єкта для підвищення ефективності радіолокаційного виявлення. Якщо описані вище заходи не приводять до покращення, необхідно застосовувати превентивні антидронові заходи.

Послідовність подій під час атаки безпілотного літального апарата наведена на схемі.

Безпілотні літальні апарати е джерелом небезпеки для обектів і людей. Активізація цієі загрози полягае у тому, що оператор бере до рук апаратуру керування і здійснює зліт у напрямку цілі атаки або програмує місію на компютері та вказує захищений об`єкт як ціль атаки. Після початку атаки розпочинаються оборонні дії, які полягають у виявленні безпілотного літального апарата, а потім у його нейтралізації. Після завершення атаки оцінюються іі наслідки. У результаті цього формуються втрати або пошкодження у системі "людина - технологія - навколишне середовище".

Якщо розрахунок імовірності виявлення та нейтралізації безпілотного літального апарата показує, що ефективність системи буде неприйнятною, і інші методи, заміна пристроів на більш ефективні або зміна умов експлуатації не приводять до покращення ефективності, слід розглянути такі превентивні заходи:

- визначення географічних зон польотів безпілотних літальних апаратів DRA-P (Drone Area - Prohibited) [78];
- здійснення заходів на користь місцевоі громади з метою здобуття іі прихильності, що, у свою чергу, може призвести до більшого контролю територіі навколо об`єкта за рахунок залучення більшоі кількості спостерігачів;
- проведення навчання з питань авіаційного законодавства для працівників поліції;
- проведення навчання з питань пілотування для персоналу фізичноі охорони об`єкта, що дозволить краще ознайомити персонал з можливостями безпілотних літальних апаратів;
- маскування елементів захищеного об`єкта з метою обмеження обсягу інформації, що може бути отримана під час атаки з використанням камер видимого (VIS) та інфрачервоного (IR) діапазонів;
- спорудження захисних накриттів елементів установок з метою запобігання пошкодженням у результаті прямого зіткнення з безпілотним літальним апаратом або внаслідок вибуху вибухових речовин.

Зазначені заходи вже детально описані у науковій літературі [124].

3.8 Формула ризику

Методологія оцінювання ризику є базовим інструментом в аналізі надійності та ефективності систем фізичного захисту ядерних установок[8]. У класичній інтерпретації ризик визначається як інтегральний показник, який відображає можливість виникнення негативної події та масштаби її наслідків. У кількісній формі ризик традиційно подається добутком імовірності реалізації загрози та очікуваних наслідків цієї реалізації:

$$R = P_{succ} * C,$$

де:

R — значення ризику;

P_{succ} — імовірність успішної реалізації загрози;

C — коефіцієнт наслідків (Consequences), що характеризує обсяг потенційної шкоди.

Такий підхід застосовується у міжнародних рекомендаціях МАГАТЕ [2, 9], документах Sandia National Laboratories [27] та у вітчизняній практиці аналізу фізичного захисту ядерних об’єктів [7, 26] як універсальна аналітична модель, що дозволяє порівнювати різні загрози між собою та визначати пріоритетні напрями вдосконалення систем безпеки.

У межах класичної системи фізичного захисту ймовірність успішної реалізації атаки визначається через загальну ефективність системи, що формується низкою взаємопов’язаних підсистем - виявлення, затримки та реагування. Сумарний ефект функціонування цих підсистем описується через інтегральний показник Ptotal, який визначає імовірність перехоплення загрози до моменту реалізації цілей порушника. Тоді ймовірність успішної атаки набуває вигляду:

$$P_{succ} = 1 - P_{total}$$

Отже, ризик для класичної системи фізичного захисту може бути поданий формулою:

$$R_{SPS} = (1 - P_{total}) * C,$$

де:

R_{SPS} — ризик функціонування об’єкта в умовах наземної (традиційної) загрози.

На відміну від класичних загроз, пов’язаних із діями внутрішніх або зовнішніх порушників на землі, атаки із застосуванням безпілотних літальних апаратів реалізуються через повітряний канал доступу, що суттєво змінює просторові характеристики загрози, часові обмеження реагування та структуру систем протидії.

Запобігання такій загрозі можливе лише за умови реалізації двох ключових функцій:

- своєчасного виявлення БпЛА;
- ефективної нейтралізації БпЛА після його виявлення.

Виходячи з цього, інтегральна ефективність системи протидії дронам формується як добуток ймовірностей успішного виконання кожної з цих функцій:

$$P_{total} = P_{totalD} * P_{totalN},$$

де:

P_{totalD} - загальна ймовірність виявлення БпЛА;

$P_{total}N$ - загальна ймовірність нейтралізації БпЛА.

З урахуванням цього, ймовірність успішної реалізації атаки з використанням безпілотного апарата визначається співвідношенням:

$$P_{succ} = 1 - (P_{totalD} * P_{totalN})$$

Підставляючи наведений вираз у класичну формулу ризику, отримаємо повну математичну модель оцінювання ризику в умовах застосування повітряних загроз:

$$R_{CUAS} = \left(1 - \left(P_{totalD} * P_{totalN}\right)\right) * C,$$

де:

R_{CUAS} - інтегральний ризик для об'єкта, що захищається системою протидії безпілотним літальним апаратам.

Запропонована модель дозволяє врахувати обидва ключові фактори ефективності протидронових рішень - імовірність виявлення та нейтралізації повітряної загрози - та кількісно пов'язати їх із масштабом можливих наслідків.

Особливістю запропонованої методології є трактування коефіцієнта наслідків як інваріантного показника, спільного для традиційної системи фізичного захисту та системи протидії БпЛА. Це означає, що незалежно від типу загрози (через наземний або повітряний простір) оцінка можливих наслідків спирається на один і той самий комплекс критеріїв.

Як і в класичних моделях фізичного захисту, коефіцієнт *C* охоплює:

- ризик пошкодження або руйнування елементів ядерної установки та допоміжної інфраструктури;
- небезпеку радіаційного або хімічного забруднення довкілля;
- загрозу життю та здоров'ю персоналу й населення;
- економічні наслідки, включаючи втрати від простою, ремонту та ліквідації пошкоджень;
- вторинні соціально-політичні й іміджеві наслідки аварій або диверсій.

Таким чином:

$$C_{CUAS} = C_{SPS} = C,$$

а коефіцієнт наслідків для системи протидії БпЛА повністю відповідає коефіцієнту наслідків, який традиційно застосовується під час оцінювання ризику систем фізичного захисту ядерних об’єктів.

З урахуванням наведеного, повна універсальна формула оцінювання ризику для об’єктів, захищених від повітряних та наземних загроз, може бути подана у наступному вигляді:

$$R = \left(1 - (P_{totalD} * P_{totalN})\right) * C$$

У межах цієї моделі:

- зростання ефективності хоча б однієї з підсистем (виявлення або нейтралізації) призводить до пропорційного зниження інтегрального рівня ризику;
- найбільш уразливі конфігурації відповідають ситуаціям, коли значення хоча б одного з показників PtotalD або PtotalN є низьким;
- абсолютне зниження ризику можливе лише за умови комплексного розвитку обох складових системи.

Застосування наведеної ризикової моделі дозволяє:

- інтегрувати системи протидії БпЛА у загальну систему фізичного захисту ядерних установок;
- здійснювати кількісне порівняння різних технічних конфігурацій протидронових рішень;
- обґрунтовувати техніко-економічні заходи щодо оптимізації витрат на захист об’єктів з позицій допустимого рівня ризику.

Запропонований підхід формує методологічну основу для подальших прикладних досліджень з оцінювання ефективності комплексних систем фізичної безпеки в умовах військових загроз із застосуванням повітряних засобів ураження.

Повний алгоритм реалізації запропонованої методики, включаючи блок-схему процесу оцінювання та зведені розрахункові моделі для кожного етапу, наведено у Додатку Г.

3.9 Апробація методики

Оскільки дисертація описує методологію отримання даних (через натурні випробування), для початкового заповнення модуля я знайшов орієнтовні усереднені показники ефективності засобів протидії БПЛА в умовах війни в Україні (станом на 2024–2025 рр.) з відкритих аналітичних звітів (наприклад, даних Генштабу та аналітиків, таких як RUSI) (Таб. 3.1) [125].

Ці джерела дають **агреговані** (сумарні) оцінки перехоплення/пригнічення дронів (змішаних типів або "Shahed-подібних"), які корисні як **контрольні точки** для перевірки того, що ваші введені P_d та $P_{n/d}$ не дають нереалістичних результатів:

- **Близько "під 80%"**: ABC News [126], посилаючись на дані за "минулий місяць", повідомляє, що з 5 312 БпЛА різних типів було "збито або пригнічено" 4 242 (трохи менше 80%).
- **Приклад великої атаки (58/80 + "зникли з радарів")**: Reuters (14 січня 2025) [127] описує атаку, де ППО/мобільні групи "збили 58 із 80", а 21 "зник з радарів", що в матеріалі пов'язано з дією РЕБ (категорія "пригнічено/відхилено").
- **Орієнтир 80–85% як "звична" ефективність по дронах** (у публікації Kyiv Post [128] це подається як типовий рівень заявлених успішних уражень/знешкоджень дронів).
- Якщо вам потрібні **типові ТТХ як статистичні розподіли** (швидкість/тривалість) для класифікації "розвід/удар/камікадзе", як відкриті приклади можна брати: Orlan-10 (розвід) [129], Lancet (барражуючий боєприпас) [130], Shahed-136 (ударний/камікадзе [131].

Таблиця 3.3 – Усереднені показники ефективності засобів протидії БПЛА

Засіб протидії	**Тип БПЛА: Розвідувальний (напр. Orlan)**	**Тип БПЛА: Ударний (напр. Missile/FPV)**	**Тип БПЛА: Камікадзе (напр. Shahed)**
Стрілецька зброя (звичайні пости)	0.05 (низька висота)	0.10 (FPV)	0.05–0.10
Мобільні вогневі групи (МВГ)	0.20 (висота польоту)	0.40	0.40–0.50 (основна ціль)
Засоби РЕБ (подавлення)	0.60–0.70 (втрата зв'язку)	0.50 (втрата керування)	0.30–0.40 (стійкі CRPA антени)
ППО / ЗРК (ракети)	0.85	0.90	0.80–0.90 (але дефіцит БК)

Результати симуляції наведені на рисунку 3.2 Модуль розрахунку ефективності протидії БПЛА на рисунку №3.3

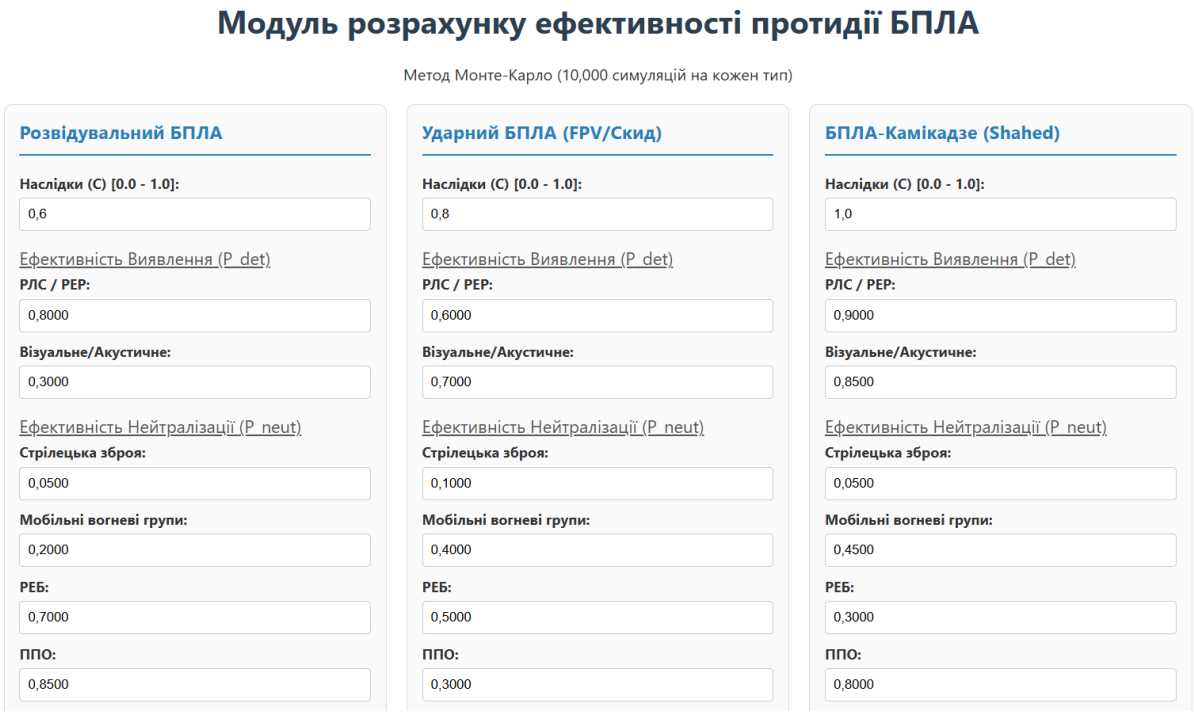

Рисунок 3.2 – Модуль розрахунку ефективності протидії БПЛА

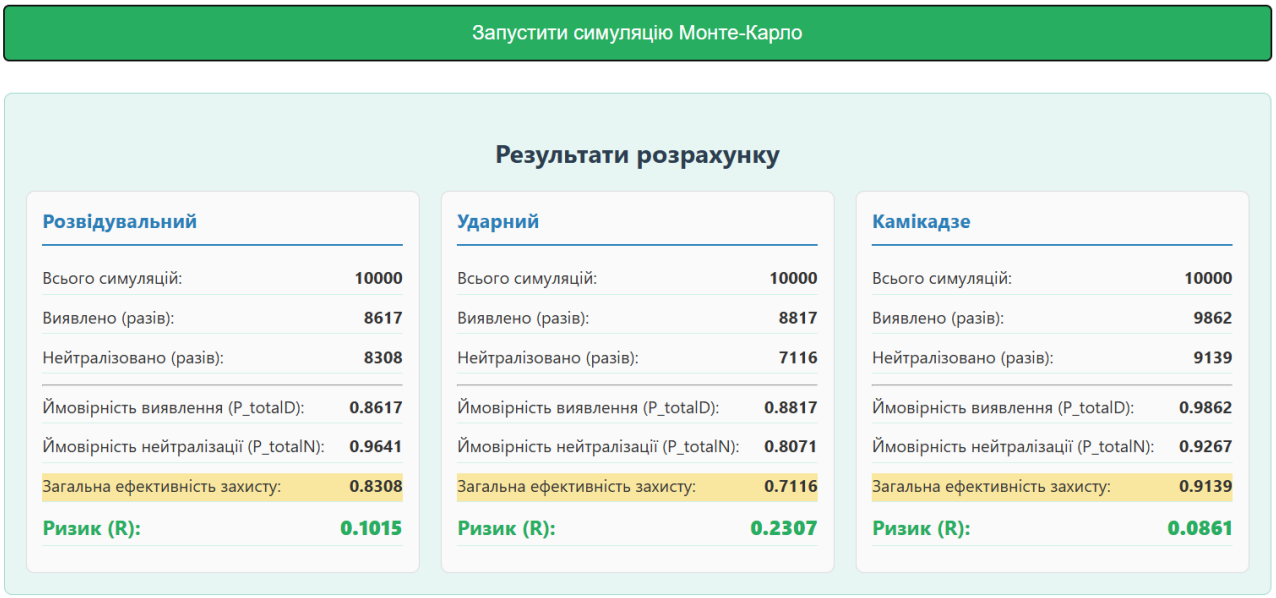

Рисунок 3.3 – Результати розрахунку

3.10 Висновки до Розділу 3

У третьому розділі розроблено концептуальні та методологічні засади оцінювання вразливості ядерних установок від повітряних загроз, зумовлених стрімким розвитком та доступністю безпілотних літальних апаратів (БпЛА). За результатами дослідження сформульовано такі висновки:

Класифікація та ідентифікація загроз. Встановлено, що сучасна класифікація БпЛА (згідно з європейськими нормами C0–C6) лише частково відображає потенціал загроз для ядерних об’єктів. Доведено, що найбільшу небезпеку становлять «саморобні» (DIY) та кастомізовані цивільні дрони, характеристики яких не обмежені заводськими протоколами і дозволяють реалізовувати сценарії від дистанційного мінування до високоточного кінетичного ураження критичних вузлів АЕС.

Типологія сценаріїв нападів. Аналіз світових інцидентів (Абу-Дабі, Франція, Швеція) дозволив класифікувати дрон-загрози на три типи: розвідувальні (збір даних про систему фізичного захисту), демонстраційні (дискредитація оператора) та ударні (пряме знищення інфраструктури). Виявлено критичну вразливість систем охолодження та відкритого

розподільчого обладнання АЕС до атак малорозмірними БпЛА, що діють поза межами виявлення традиційними засобами ППО.

Комплексний підхід до виявлення. Обґрунтовано, що жоден з існуючих методів детекції (радіолокаційний, акустичний, оптичний або радіочастотний) не забезпечує 100% надійності в ізольованому вигляді. Доведено необхідність побудови багатофакторної системи виявлення, яка враховує специфіку завад (шум міста, погодні умови, рельєф) та базується на інтеграції сенсорів, що працюють на різних фізичних принципах.

Математична модель надійності системи. Запропоновано імовірнісну модель оцінки ефективності антидронового захисту (P_{sys}), яка базується на врахуванні восьми ключових параметрів експлуатації (погодні умови, час доби, локація, тип дрона та двигуна, спосіб виконання місії, кваліфікація персоналу та дистанція). Це дозволяє не лише констатувати факт наявності захисту, а й кількісно оцінювати його спроможність у конкретних часових і просторових інтервалах (Required\ Time).

Еволюція засобів нейтралізації. Систематизовано методи протидії БпЛА та виявлено їхні слабкі місця: ризик некерованого падіння апарата на територію ЯУ при використанні кінетичних засобів або лазерів, а також неефективність джамінгу проти повністю автономних дронів, що використовують інерціальну навігацію або комп’ютерний зір.

4 ВИСНОВКИ/ПРОПОЗИЦІ

4.1 Нормативно-правові засади фізичного захисту ядерних установок України та відсутність правового механізму врахування загроз повітряного типу

Побудова систем фізичного захисту ядерних установок в Україні ґрунтується на положеннях спеціального законодавства у сфері використання ядерної енергії та ядерної безпеки, базовим актом якого є Закон України від 19 жовтня 2000 року № 2064-IV «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [23]. Зазначений Закон визначає цілі, завдання та принципи функціонування державної системи фізичного захисту і встановлює загальні вимоги до організації протидії можливим актам ядерного тероризму.

Відповідно до частини першої статті 1 Закону фізичний захист визначається як «комплекс організаційних, інженерно-технічних та режимних заходів, спрямованих на попередження, виявлення та припинення несанкціонованих дій щодо ядерних установок та ядерних матеріалів» [23]. Аналіз наведеного визначення та подальших норм Закону свідчить, що закладена в нього модель загроз концептуально орієнтована на класичні сценарії, пов’язані з фізичним доступом порушника до об’єкта (проникнення на територію, подолання бар’єрів, контактний саботаж), тоді як вектор впливу з повітряного простору нормативно не деталізовано.

Так, стаття 6 Закону встановлює, що фізичний захист передбачає організацію контрольованих зон доступу, перевірку персоналу та забезпечення охорони периметру об’єктів, що відповідає сценаріям проникнення людей або транспортних засобів у межі охоронюваних територій. Стаття 8 покладає на експлуатуючі організації обов’язок розробляти та впроваджувати системи фізичного захисту, які мають забезпечувати виявлення несанкціонованих дій і запобігання їх реалізації. Водночас Закон не містить положень, які б розрізняли

загрози за способом реалізації (наземні/повітряні), а також не визначає вимог до врахування дистанційного впливу або доставки засобів ураження через повітряний простір.

Окремого розгляду потребує імплементація міжнародних зобов'язань України у сфері фізичного захисту. Україна є учасницею Конвенції про фізичний захист ядерного матеріалу 1980 року (ратифікованої Законом України від 05 травня 1993 року № 3182-XII) [1] та Поправки до цієї Конвенції (ратифікованої Законом України від 03 вересня 2008 року № 356-VI) [3]. Зазначені міжнародні акти визначають фізичний захист як сукупність заходів, спрямованих на захист ядерного матеріалу й ядерних установок від незаконного заволодіння, несанкціонованого використання та актів саботажу. При цьому міжнародні документи, встановлюючи загальний принцип комплексного підходу [2, 4], не закріплюють обов'язкових методик кількісної оцінки ефективності систем фізичного захисту та залишають питання конкретних процедур і критеріїв на розсуд національних регуляторів.

Проблема нормативної визначеності набуває особливої актуальності в умовах появи технологічно нових загроз, що раніше не розглядалися як реалістичні сценарії нападу на ядерні об'єкти. Насамперед йдеться про широке застосування безпілотних літальних апаратів, які забезпечують можливість повітряного проникнення у захищені зони без фізичного порушення периметру та без необхідності прямого контакту з персоналом охорони. Водночас аналіз норм Закону № 2064-IV [23] дозволяє констатувати відсутність правових передумов для системного врахування такого типу загроз, зокрема:

- у термінологічному апараті не визначено повітряні загрози та безпілотні літальні апарати як окремий клас засобів диверсійного впливу;
- не встановлено вимог до побудови інтегрованих систем протидії БпЛА;
- відсутні положення щодо нормативно визначених процедур перевірки та оцінювання ефективності засобів радіоелектронної боротьби;

- не врегульовано порядок обчислення сумарних показників імовірності виявлення та нейтралізації атак повітряного типу.

Таким чином, Закон формує загальну рамку організації фізичного захисту, однак не містить правового механізму реагування на технологічно нові загрози, які виходять за межі класичних сценаріїв наземного диверсійного впливу. За таких умов експлуатуючі організації змушені приймати рішення щодо закупівлі та розгортання засобів протидії БпЛА без нормативно визначеної методики оцінки їх достатності та результативності. Як наслідок, обґрунтування таких рішень нерідко базується на суб'єктивних оцінках або загальних рекомендаціях, а не на розрахунковому визначенні рівня ризику та ефективності комплексу заходів.

4.2 Проєктна загроза як методологічне обмеження врахування повітряних сценаріїв

Відповідно до Закону № 2064-IV [23] проєктна загроза розглядається як комплекс припущень щодо потенційних способів вчинення диверсійних і терористичних дій стосовно ядерного об'єкта, які покладаються в основу проєктування системи фізичного захисту та впровадження технічних і організаційних заходів. На підзаконному рівні питання проєктної загрози деталізоване, зокрема, у розпорядженні Кабінету Міністрів України від 04 вересня 2013 року № 684-р «Про затвердження комплексного плану заходів щодо реалізації положень нової редакції Проєктної загрози…» [132].

Зміст методичних підходів, що випливають із зазначеного комплексу документів та роз'яснень регулятора щодо структури DBT [133], а також відповідних рекомендацій МАГАТЕ [19], дає підстави зробити принципово важливий висновок: чинна модель проєктної загрози концептуально сформована під сценарії наземних диверсійних дій і не містить системного інструментарію для опису загроз, реалізованих із використанням БпЛА. Це простежується в наборі вихідних характеристик типового порушника та

сценаріїв, які переважно зводяться до дій підготовленої диверсійної групи: проникнення через бар’єри, подолання контрольованих зон, застосування ручних засобів саботажу, контактна доставка вибухових речовин або засобів ураження [27]. Усі такі сценарії передбачають фізичну присутність порушника на території об’єкта або в безпосередній близькості до нього.

Попри те, що теоретично повітряні сценарії могли б бути включені до складу проєктної загрози, чинне правове та методичне поле не забезпечує належних засобів для їх формалізації та кількісного обґрунтування. Зокрема, на відміну від міжнародних стандартів інженерного захисту від зовнішніх впливів [134], у вітчизняній практиці відсутні процедури й параметри, які дозволяли б:

- описувати характеристики повітряної атаки (висота, траєкторія, швидкість, маса корисного навантаження, кількість апаратів, можливість групового застосування тощо);
- визначати кількісні показники здатності систем фізичного захисту виявляти повітряні цілі на різних висотах і відстанях;
- інтегрувати в ризик-орієнтований розрахунок результати дії технічних засобів (РЛС ближньої дії, оптико-електронні й тепловізійні системи спостереження, акустичні засоби, засоби РЕБ);
- враховувати людський фактор у процесі ідентифікації повітряних цілей та ухвалення рішення щодо застосування нейтралізуючих заходів.

Додатково слід зазначити, що процедура затвердження та перегляду проєктної загрози має інерційний характер і орієнтується на періодичне оновлення сценаріїв у відносно стабільних умовах [74]. За обставин воєнних загроз і швидкої еволюції безпілотних технологій така процедура об’єктивно ускладнює оперативну адаптацію нормативних припущень до реальної безпекової ситуації.

Отже, у чинному правовому та методичному полі проєктна загроза не забезпечує достатніх параметрів і процедур для опису, оцінювання та кількісного обґрунтування повітряних загроз, пов’язаних із застосуванням БпЛА. Це зумовлює необхідність розроблення та нормативного закріплення

спеціалізованої методики кількісної оцінки ймовірності виявлення та нейтралізації БпЛА як доповнення до існуючої системи фізичного захисту, а не як її заміни.

4.2.1 Пропозиції щодо уточнення положень Закону № 2064-IV

Проведений аналіз дає підстави стверджувати, що Закон № 2064-IV [23] концептуально не охоплює повітряні загрози, пов’язані з можливістю ураження ядерних установок із застосуванням БпЛА. Для усунення цієї прогалини доцільним є внесення точкових змін, які легалізують повітряний вектор загроз і створюють основу для подальшого підзаконного регулювання.

1. Зміни до статті 1 (уточнення дефініцій).

Доцільно доповнити визначення фізичного захисту положенням про те, що він охоплює також дії, які здійснюються шляхом впливу з повітряного простору із застосуванням пілотованих або безпілотних літальних апаратів. Така зміна юридично закріплює повітряний вектор , що відповідає сучасним викликам безпеці, зафіксованим у звітах МАГАТЕ щодо ситуації в Україні [6, 39], і створює підставу для розвитку підзаконного регулювання без перенесення технічних методик у текст Закону.

2. Зміни до статті 3 (уточнення мети фізичного захисту).

Доцільно доповнити норму положенням, що фізичний захист спрямований на протидію загрозам, пов’язаним із нанесенням ударів із застосуванням літальних апаратів та інших технічних засобів дистанційного впливу, незалежно від характеру доступу порушника до захищених об’єктів. Це усуває вузьку прив’язку фізичного захисту до лише контактного проникнення [27].

3. Зміни до статті 6 (вимоги до систем фізичного захисту).

Доцільно передбачити, що система фізичного захисту має проєктуватися з урахуванням необхідності виявлення та припинення несанкціонованих дій, що здійснюються через повітряний простір, у тому числі із застосуванням БпЛА.

Норма формує правову базу для стандартів і методик підзаконного рівня [10, 108, 109].

4. Зміни до статті 8 (обов'язки експлуатуючих організацій).

Доцільно закріпити обов'язок забезпечувати функціонування систем фізичного захисту з урахуванням загроз повітряного характеру та здійснювати підготовку персоналу щодо виявлення й реагування на такі загрози. Це встановлює чітку сферу відповідальності операторів і підстави для державних перевірок [7, 71].

5. Методичні положення щодо ризику (концептуальне застереження).

Хоча в науковому забезпеченні та міжнародній практиці використовується ризик-орієнтований підхід (зокрема загальна залежність виду $R = P \times C$) [8], Законодавчий рівень не повинен містити математичних методик. Натомість Закон має правово визнати повітряні загрози в предметі регулювання та забезпечити нормативну допустимість розроблення й застосування кількісних методик оцінювання параметрів виявлення та нейтралізації БпЛА на рівні підзаконних актів ДІЯРУ та відомчих методичних документів [28, 75].

4.3 Аналіз підзаконних нормативно-правових актів Кабінету Міністрів України у сфері фізичного захисту та необхідність їх коригування з метою правового врахування загроз повітряного характеру

Нормативні прогалини, пов'язані з відсутністю правового врахування повітряних загроз у системі фізичного захисту ядерних установок, отримують подальше підтвердження під час аналізу підзаконних нормативно-правових актів Кабінету Міністрів України, які конкретизують положення Закону України від 19 жовтня 2000 року № 2064-IV «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [23] та визначають організаційно-управлінську модель функціонування державної системи фізичного захисту [26, 74].

4.3.1 Постанова Кабінету Міністрів України від 21 грудня 2011 року № 1337 «Про затвердження Порядку функціонування державної системи фізичного захисту»

Зазначена постанова [135] є базовим документом, що регламентує структуру державної системи фізичного захисту, порядок взаємодії між суб'єктами фізичного захисту, механізми координації центральних і місцевих органів виконавчої влади, експлуатуючих організацій та правоохоронних органів, а також визначає загальні засади організації реагування на диверсійні загрози.

Аналіз положень Порядку свідчить, що вся модель функціонування державної системи фізичного захисту побудована навколо концепції «несанкціонованого проникнення на територію об'єкта» [23]. Так, пункт 6 Порядку визначає основними завданнями системи фізичного захисту координацію заходів щодо «виявлення, попередження та припинення несанкціонованих дій на об'єктах використання ядерної енергії», однак не конкретизує можливі способи реалізації таких дій та не розрізняє наземні й повітряні вектори загроз.

Подальша деталізація організаційних механізмів у Порядку зосереджена переважно на питаннях пропускного режиму, фізичного патрулювання територій, організації контрольно-пропускних пунктів, взаємодії підрозділів охорони та правоохоронних органів у межах наземних сценаріїв диверсійної діяльності [27]. Процедури виявлення, ідентифікації та нейтралізації загроз повітряного характеру, зокрема із застосуванням безпілотних літальних апаратів, у документі відсутні.

Відсутність у Порядку нормативно визначених процедур протидії повітряним загрозам унеможливлює інтеграцію протидронових заходів у загальнодержавну модель реагування [6, 39]. Навіть за наявності на конкретному об'єкті технічних засобів виявлення БпЛА або систем радіоелектронної боротьби [76] експлуатуючі організації не мають чітко

визначеного правового механізму їх використання у взаємодії з іншими суб'єктами державної системи фізичного захисту.

Пропозиція щодо внесення змін до пункту 6 Порядку після слів «виявлення, попередження та припинення несанкціонованих дій на об'єктах використання ядерної енергії» доцільно додати: «у тому числі дій, що здійснюються із застосуванням повітряних засобів нападу, включаючи безпілотні літальні апарати».

Обґрунтування:

Запропоноване доповнення:

- юридично визнає необхідність реагування на повітряні сценарії диверсій [134];
- створює правову основу для розроблення регламентів взаємодії між Міністерством внутрішніх справ України, Службою безпеки України, Збройними Силами України та Державною інспекцією ядерного регулювання України саме у частині протидії БпЛА поблизу ядерних установок [10, 71];
- усуває концептуальну одновимірність системи фізичного захисту.

4.3.2 Постанова Кабінету Міністрів України від 26 квітня 2003 року № 625 «Про затвердження Порядку визначення рівня фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання відповідно до їх категорії»

Зазначена постанова [136] встановлює алгоритм визначення рівня фізичного захисту об'єктів використання ядерної енергії шляхом їх віднесення до відповідних категорій залежно від потенційних наслідків можливих диверсійних подій. Категоризація здійснюється на основі якісної оцінки радіаційної небезпеки, масштабів можливого радіаційного впливу, соціально-економічних та екологічних наслідків аварійних ситуацій [23, 137].

Разом із тим аналіз положень Порядку свідчить, що встановлення рівня фізичного захисту має статичний характер і не враховує спосіб реалізації загроз

[27]. Документ не містить положень, які б диференціювали сценарії диверсійних дій за напрямом впливу (наземний, комбінований або повітряний), а також не встановлює зв’язку між категорією фізичного захисту об’єкта та його фактичною вразливістю до застосування сучасних технічних засобів нападу, зокрема безпілотних літальних апаратів [6, 39].

У Порядку відсутні вимоги щодо:

- урахування можливості повітряного ураження під час визначення категорії фізичного захисту [134];
- оцінювання мінімально допустимого рівня ефективності технічних засобів виявлення та нейтралізації загроз повітряного характеру [8];
- встановлення залежності між рівнем захищеності об’єкта та ймовірністю реалізації сценаріїв дистанційного впливу.

У результаті категоризація об’єктів використання ядерної енергії здійснюється без урахування реальної вразливості до БпЛА [40]. В умовах воєнних загроз це створює ситуацію формальної відповідності нормативним вимогам, за якої об’єкт, віднесений до високої категорії фізичного захисту, може залишатися недостатньо захищеним від повітряних атак.

Пропозиція щодо внесення змін:

До критеріїв визначення рівня фізичного захисту доцільно включити положення такого змісту: «Під час визначення рівня фізичного захисту об’єктів використання ядерної енергії обов’язково враховується їх потенційна уразливість до загроз повітряного характеру, у тому числі дій із застосуванням безпілотних літальних апаратів та інших засобів дистанційного ураження».

Обґрунтування:

Запропонована норма:

- забезпечує зв’язок між категорією фізичного захисту та реальною безпековою ситуацією [75];
- створює правову основу для подальшого кількісного оцінювання ефективності захисту;

- дозволяє адаптувати вимоги до систем фізичного захисту конкретних об’єктів з урахуванням сучасних загроз.

4.3.3 Постанова Кабінету Міністрів України від 12 березня 2003 року № 327 «Про затвердження Порядку проведення державної перевірки систем фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та планів взаємодії у разі вчинення актів ядерного тероризму»

Зазначений Порядок [138] регламентує процедуру державного контролю за станом систем фізичного захисту шляхом проведення перевірок їх відповідності вимогам законодавства [23] та затвердженим планам забезпечення фізичного захисту. Метою перевірки визначено оцінювання організаційних, технічних та режимних заходів охорони, а також готовності персоналу до реагування на диверсійні загрози [7].

Аналіз змісту Порядку свідчить, що процедура державної перевірки зосереджена переважно на:

- стані інженерних огороджень та периметрового захисту [27];
- ефективності систем контролю доступу;
- готовності підрозділів фізичної охорони до реагування на наземні диверсійні сценарії;
- дотриманні пропускного та внутрішньооб’єктового режимів.

При цьому Порядок не передбачає:

- перевірки здатності систем фізичного захисту виявляти повітряні цілі [109, 114];
- оцінювання ефективності технічних засобів протидії БпЛА [10, 115];
- аналізу функціонування засобів радіоелектронної боротьби [76] ;
- тестування процедур взаємодії персоналу з силами реагування у разі повітряної атаки [21, 71].

Таким чином, за чинною процедурою об’єкт може бути визнаний таким, що відповідає нормативним вимогам фізичного захисту, навіть за відсутності реальної спроможності протидіяти повітряним загрозам [6, 39]. Це формує нормативну ілюзію захищеності, за якої позитивні результати державної перевірки не корелюють з фактичним рівнем безпеки об’єкта в умовах сучасних воєнних ризиків [40].

Пропозиція щодо внесення змін:

До розділу Порядку, який визначає обсяг державної перевірки, доцільно включити норму такого змісту:

«Державна перевірка систем фізичного захисту повинна включати оцінювання готовності об’єкта до протидії загрозам повітряного характеру, у тому числі із застосуванням безпілотних літальних апаратів, з перевіркою технічних засобів їх виявлення та процедур реагування персоналу».

Обґрунтування:

Запровадження такої норми:

- усуває розрив між формальними перевірками та реальними умовами безпеки [134] ;
- створює правові підстави для обов’язкового тестування антидронових компонентів системи фізичного захисту;
- підвищує системність і результативність державного контролю.

4.3.4 Постанова Кабінету Міністрів України від 24 липня 2013 року № 598 «Про затвердження державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання та щодо радіоактивних відходів»

Державний план взаємодії [139] визначає порядок координації дій органів державної влади у разі виникнення виняткових подій, пов’язаних із диверсійним впливом на ядерні установки та інші радіаційно небезпечні

об’єкти [23]. Документ регламентує розподіл функцій між центральними та місцевими органами виконавчої влади, правоохоронними органами та експлуатуючими організаціями.

Водночас аналіз положень Плану свідчить, що закладена в нього модель реагування побудована навколо сценаріїв фізичного вторгнення диверсійних груп [27]. Документ орієнтований на:

- блокування територій;
- розгортання наземних сил охорони;
- ізоляцію об’єктів та ліквідацію наслідків контактних диверсій.

Процедури реагування на повітряні сценарії загроз, зокрема масоване застосування БпЛА, проведення повітряної розвідки або дистанційне ураження об’єктів, у Плані відсутні [6, 39]. Не визначено ролі органів військового управління, підрозділів протиповітряної оборони та сил радіоелектронної боротьби у межах реагування на такі загрози [10, 76].

У разі реальної повітряної атаки на ядерний об’єкт відсутність нормативно визначеного порядку взаємодії призводить до фрагментарності реагування та втрати часу, що є критичним фактором для забезпечення фізичної та ядерної безпеки [40, 71].

Пропозиція щодо внесення змін:

До розділів Плану, що регламентують реагування на диверсії, доцільно включити окремий підпункт такого змісту:

«План взаємодії повинен передбачати порядок реагування на загрози диверсій повітряного характеру, у тому числі із застосуванням безпілотних літальних апаратів, із визначенням функцій органів військового управління, повітряних сил та підрозділів радіоелектронної боротьби».

Обґрунтування:

Запропоноване доповнення:

- забезпечує правовий зв’язок між цивільною системою фізичного захисту та силами оборони України [75, 140];

- дозволяє врегулювати застосування засобів протиповітряної оборони та радіоелектронної боротьби в районах розташування ядерних установок;
- усуває фрагментарність державного реагування на повітряні загрози.

4.4 Аналіз нормативних актів Державної інспекції ядерного регулювання України та методологічні обмеження врахування повітряних загроз Наказ Державної інспекції ядерного регулювання України від 30 листопада 2010 року № 169 «Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів»

Порядок проведення оцінки вразливості ядерних установок та ядерних матеріалів [141] є ключовим нормативно-методичним документом у системі фізичного захисту, оскільки саме він визначає процедуру формування вихідних даних для проєктування систем фізичного захисту, розроблення планів реагування та здійснення державного контролю [7]. Відповідно до його положень оцінка вразливості передбачає ідентифікацію можливих загроз, аналіз ймовірності їх реалізації, оцінювання ефективності існуючих заходів фізичного захисту та визначення необхідності додаткових організаційних і технічних рішень.

Разом із тим системне тлумачення положень Порядку свідчить, що закладена в нього модель загроз має виключно наземний характер. Норми документа оперують поняттями несанкціонованого проникнення на територію, подолання контрольно-пропускних пунктів, обходу режиму охорони, саботажних дій із застосуванням наземних засобів ураження [27]. Механізми реалізації загроз через повітряний простір або шляхом дистанційного впливу за допомогою безпілотних літальних апаратів методично не описані [39, 40].

Принциповою проблемою є те, що Порядок № 169 базується на аналізі можливості проникнення порушника на захищену територію, тоді як сценарії

застосування БпЛА усувають саму необхідність фізичного проникнення людини в межі контрольованих зон. У такій ситуації базовий методичний інструмент оцінки вразливості стає непридатним для аналізу принципово іншого вектора загроз.

Крім того, оцінка загроз у Порядку здійснюється через аналіз сценаріїв, сформованих у межах затвердженої проєктної загрози [132]. Як було показано раніше, чинна модель проєктної загрози також орієнтована на наземні диверсійні дії, що фактично унеможливлює формування легітимних сценаріїв повітряних атак на етапі оцінки вразливості [75].

З огляду на структуру державної системи фізичного захисту саме Порядок проведення оцінки вразливості № 169 є тим нормативним актом, у якому має бути юридично закріплена можливість:

- застосування кількісних методів оцінки ефективності виявлення та нейтралізації загроз [8, 28];
- урахування технічних характеристик сучасних систем протидії БпЛА [108, 109];
- визначення інтегрованого показника ризику з урахуванням повітряного вектора атак.

За відсутності відповідних положень у цьому Порядку будь-які розрахункові методики залишатимуться виключно науковими рекомендаціями, результати яких не матимуть юридичної сили, не можуть використовуватися органами державного нагляду та не будуть підставою для прийняття управлінських і фінансових рішень.

4.4.1 Пропозиції щодо внесення змін до Наказу Державної інспекції ядерного регулювання України від 30 листопада 2010 року № 169

Доповнення переліку загроз:

- У розділі, що встановлює загальні положення оцінки вразливості, доцільно передбачити норму такого змісту: «Оцінка вразливості ядерних установок та ядерних матеріалів здійснюється з урахуванням можливості

реалізації загроз як наземним, так і повітряним шляхом, у тому числі із застосуванням безпілотних літальних апаратів» [19, 74, 88].

Розширення завдань оцінки вразливості

- До переліку завдань оцінки необхідно включити аналіз здатності технічних і організаційних заходів фізичного захисту щодо виявлення та нейтралізації загроз повітряного характеру [8, 10, 134].

Такі зміни забезпечують нормативну легітимацію застосування кількісних методик оцінювання ефективності систем протидії БпЛА у межах процедури оцінки вразливості.

4.4.2 Наказ Державної інспекції ядерного регулювання України від 05 грудня 2011 року № 176 «Про затвердження Вимог до комплексу інженерно-технічних засобів системи фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання»

Зазначений наказ визначає склад, призначення та загальні принципи застосування комплексу інженерно-технічних засобів системи фізичного захисту [25]. Основний зміст документа зосереджений на вимогах до систем периметрової охорони, технічних засобів контролю доступу, охоронної сигналізації, відеоспостереження та пунктів централізованого керування.

Усі передбачені Вимогами елементи традиційно орієнтовані на виявлення та припинення наземних сценаріїв диверсійної діяльності [25, 26]. Документ не містить прямих вимог щодо:

- систем радіолокаційного або радіотехнічного виявлення повітряних цілей [109, 110];
- інтеграції засобів радіоелектронної боротьби [10, 108];
- застосування оптичних і тепловізійних систем вертикального та секторного огляду [96, 102];
- організації оперативних дій охорони у разі дистанційних атак [71].

Хоча наказ № 176 формально не забороняє використання протидронових систем, відсутність нормативної вимоги щодо їхнього застосування фактично зводить такі засоби до статусу необов’язкових і «поза регламентом», що обмежує можливість їх системного впровадження [32, 75].

Крім того, у документі застосовується підхід функціональної достатності, відповідно до якого комплекс інженерно-технічних засобів має забезпечувати своєчасне виявлення ознак підготовки або здійснення диверсії [25]. Водночас:

- не визначено критерії своєчасності;
- відсутні нормативні часові пороги реагування;
- не встановлено мінімально допустимі значення ймовірності виявлення загроз [27, 28].

Таким чином, наказ № 176 не передбачає застосування розрахункових методів оцінки ефективності технічних засобів і залишає визначення їх достатності у площині експертних оцінок.

Пропозиція щодо внесення змін:

До загальних положень Вимог доцільно включити норму такого змісту: «Комплекс інженерно-технічних засобів системи фізичного захисту повинен забезпечувати виявлення та нейтралізацію загроз, що реалізуються як наземним, так і повітряним шляхом, у тому числі із застосуванням безпілотних літальних апаратів» [7, 76, 141].

Запропонована норма легалізує включення спеціалізованих протидронових комплексів до складу системи фізичного захисту без деталізації конкретних моделей або технологій, що відповідає принципу регуляторної нейтральності [2, 68].

4.4.3 Наказ Державної інспекції ядерного регулювання України від 20 грудня 2010 року № 179 «Про затвердження Вимог до оцінки стану системи фізичного захисту ядерної установки»

Наказ № 179 визначає критерії та порядок оцінювання стану системи фізичного захисту ядерної установки з боку регулятора [141]. Оцінювання здійснюється шляхом документальних перевірок, тестування роботи технічних засобів, аналізу організації охорони та взаємодії персоналу, після чого формується експертний висновок щодо відповідності або невідповідності системи фізичного захисту встановленим вимогам [135, 138].

Разом із тим документ передбачає виключно якісну модель оцінювання. Результати перевірки формулюються у вигляді загальних експертних суджень без використання кількісних показників ефективності [29, 30]. У Вимогах відсутні положення щодо:

- застосування ймовірнісних показників виявлення загроз [27];
- оцінювання ефективності нейтралізації [28];
- використання інтегрованого показника ризику [8].

У такій моделі регулятор обмежений у можливості порівнювати різні технічні рішення та обґрунтовувати управлінські рішення на основі об’єктивних числових критеріїв [32, 60].

Пропозиція щодо внесення змін:

Доповнити розділ, що встановлює підходи до оцінки стану системи фізичного захисту, положенням такого змісту:

«Під час оцінки стану системи фізичного захисту допускається застосування кількісних показників імовірності виявлення, імовірності нейтралізації та інтегрального показника ризику загроз».

Це створює правову можливість використання розрахункових методик під час державних перевірок і переводить оцінювання систем фізичного захисту з формальної у результативну площину [2, 4, 137].

4.5 Інтеграція кількісної методики оцінки повітряних загроз у систему нормативного регулювання фізичного захисту. Взаємозв'язок запропонованої методики з процедурою оцінки вразливості

Ключовим елементом інтеграції кількісної методики оцінки ймовірності виявлення та нейтралізації безпілотних літальних апаратів у чинну систему фізичного захисту є її узгодження з процедурою оцінки вразливості ядерних установок, визначеною Наказом Державної інспекції ядерного регулювання України від 30 листопада 2010 року № 169 «Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів» [141].

Відповідно до положень зазначеного Порядку оцінка вразливості включає аналіз проєктної загрози, ідентифікацію уразливих елементів фізичного захисту, а також визначення ефективності бар'єрів і сил реагування [19, 133]. Проте чинна редакція документа оперує виключно поняттям порушника як фізичної особи або групи осіб, які здійснюють напад шляхом безпосереднього проникнення на територію об'єкта. За таких умов дистанційні сценарії нападу, що реалізуються без фізичної присутності порушника, залишаються поза межами нормативного аналізу [32, 85].

Запропонована методика кількісної оцінки не змінює базову логіку процедури оцінки вразливості, а доповнює її новим аналітичним інструментарієм. Зокрема, вона дозволяє:

- формалізувати повітряні сценарії загроз у межах розширеної проєктної загрози [74, 132];
- оцінювати ефективність технічних і організаційних заходів фізичного захисту щодо виявлення БпЛА [27, 28];
- визначати ймовірність нейтралізації повітряних цілей з урахуванням багаторівневої структури системи протидії [10, 115];
- інтегрувати результати оцінювання в єдиний показник ризику, сумісний із класичним ризик-орієнтованим підходом [8, 30].

Таким чином, методика виступає інструментом практичної реалізації вимог щодо оцінки ефективності систем фізичного захисту без потреби кардинальної перебудови чинної нормативної процедури [29, 60].

4.6 Кількісна модель ризику як елемент нормативної адаптації

У міжнародній та національній практиці аналізу безпеки широко застосовується загальна модель ризику, яка визначає ризик як добуток імовірності реалізації загрози та очікуваних наслідків [8, 27]:

$$R = P \times C,$$

де R – ризик,

P – імовірність реалізації загрози,

C – коефіцієнт наслідків.

Чинне законодавство України у сфері фізичного захисту обґрунтовано не містить математичних формул і методик, оскільки законодавчий рівень має визначати предмет і цілі регулювання, а не інструменти розрахунку [22, 23]. Водночас відсутність на підзаконному рівні нормативно легітимізованих методів кількісної оцінки ймовірності реалізації повітряних загроз створює методологічний вакуум, у межах якого неможливо об’єктивно обґрунтувати достатність або надмірність застосованих технічних рішень [11, 32].

Запропонована методика дозволяє сформувати інтегрований показник ефективності системи фізичного захисту щодо повітряних загроз, який може бути використаний як елемент оцінки ризику без закріплення конкретних формул у нормативно-правових актах [28, 75]. Законодавчий та регуляторний рівні при цьому зберігають контроль за допустимими межами ризику та критеріями прийнятності [19, 136].

4.6.1 Економічне обґрунтування необхідності кількісного підходу

Відсутність кількісної оцінки рівня ризику повітряних загроз призводить до системних економічних дисбалансів у сфері фізичного захисту ядерних установок. Практика експлуатації свідчить про наявність двох крайніх сценаріїв ухвалення управлінських рішень [32, 64].

Перший сценарій характеризується надмірними капітальними витратами, коли експлуатуючі організації закуповують значну кількість протидронових технічних засобів без розрахункового доведення їх необхідності [8, 19]. У такому випадку рішення ґрунтуються на суб’єктивному сприйнятті загрози або маркетингових характеристиках обладнання, що призводить до неефективного використання фінансових ресурсів [41, 73].

Другий сценарій полягає у хибній впевненості в достатності захисту, коли кошти витрачаються на окремі технічні рішення без перевірки їх реальної ефективності в умовах конкретних сценаріїв атак [27, 40]. За відсутності кількісних критеріїв така система може формально відповідати нормативним вимогам, але залишатися вразливою до повітряних загроз [37, 75].

Запропонована методика дозволяє перейти до економічно обґрунтованої моделі управління безпекою, у межах якої:

- кожен технічний засіб оцінюється за показником імовірності виявлення або нейтралізації загрози [28, 95];
- формується інтегрований показник ефективності системи фізичного захисту [27, 30];
- визначається мінімально достатня конфігурація технічних і організаційних заходів [60, 68];
- оптимізуються витрати без перевищення порогу надмірного фінансування [64].

Таким чином, методика виконує не лише безпекову, а й економічно оптимізаційну функцію.

4.6.2 Юридичний ефект інтеграції методики у державну систему фізичного захисту

Інтеграція кількісної методики оцінки повітряних загроз у систему нормативного регулювання не створює додаткових правових ризиків, оскільки:

- методика не закріплюється безпосередньо в законодавчих актах [22, 23];
- її застосування відбувається в межах чинних процедур оцінки вразливості та державного контролю [135, 141];
- регулятор зберігає повноваження щодо визначення прийнятного рівня ризику та критеріїв відповідності [136, 138].

З правової точки зору відбувається перехід від формального підтвердження відповідності систем фізичного захисту встановленим вимогам до оцінювання їх реальної результативності [2, 75]. Це забезпечує узгодження юридичної моделі фізичного захисту з фактичними умовами воєнних загроз та сучасного технологічного розвитку [32, 44].

4.7 Узагальнюючий нормативно-правовий висновок

Проведений комплексний аналіз законодавства та підзаконних нормативно-правових актів України у сфері фізичного захисту ядерних установок дозволяє зробити такі узагальнюючі висновки [24, 25, 141].

Чинна нормативна модель фізичного захисту була сформована в умовах мирного часу та орієнтована переважно на сценарії наземного диверсійного впливу [25, 26]. Вона не охоплює повною мірою сучасні повітряні загрози, пов’язані із застосуванням безпілотних літальних апаратів, що створює розрив між формальною відповідністю вимогам і реальним рівнем безпеки об’єктів використання ядерної енергії [32, 74, 88].

Запропоновані зміни до законодавчих і підзаконних актів:

- формально визнають безпілотні літальні апарати як окремий тип загрози [74, 132];

- розширюють зміст проєктної загрози та процедур оцінки вразливості [19, 133];
- зобов’язують експлуатуючі організації враховувати повітряні сценарії під час проєктування та оцінювання ефективності систем фізичного захисту [7, 76];
- створюють нормативні умови для впровадження кількісної методики оцінки ризику без потреби кардинального перегляду чинної системи правового регулювання [27, 28, 137].

Реалізація запропонованого підходу дозволяє підвищити реальну ефективність фізичного захисту ядерних установок, оптимізувати витрати та забезпечити адаптацію державної системи фізичного захисту України до умов сучасних воєнних загроз XXI століття [8, 11, 64].

Аналіз та пропозиції змін до Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів зведено до Таблиці 4.1.

Таблиця 4.1 – Аналіз та пропозиції змін ло Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів

№	**Розділ / пункт Порядку №169**	**Чинний нормативний зміст (узагальнено)**	**Виявлена нормативно-методична проблема**	**Запропонована зміна / доповнення**	**Методологічний ефект**
1	Розділ І. Загальні положення (мета оцінки)	Оцінка вразливості спрямована на аналіз здатності системи ФЗ протидіяти діям правопорушників	Загроза імпліцитно ототожнюється з фізичним проникненням	Доповнити положенням про загрози, що реалізуються через повітряний простір, зокрема із застосуванням БпЛА	Нормативно легалізується повітряний вектор загроз

Продовження таблиці 4.1

№	Розділ / пункт Порядку №169	Чинний нормативний зміст (узагальнено)	Виявлена нормативно-методична проблема	Запропонована зміна / доповнення	Методологічний ефект
2	Розділ I. Терміни та визначення	Відсутні терміни, пов’язані з повітряними цілями	Неможливість формалізованого опису БпЛА-сценаріїв	Ввести терміни «загроза повітряного характеру», «повітряна ціль», «компонент протидії повітряним загрозам»	Створюється термінологічна база для розрахунків
3	Розділ I. Ефективність системи ФЗ	Ефективність визначається як імовірність протидії діям правопорушника	Модель ефективності прив’язана до наземного порушника	Уточнити, що ефективність може визначатися для загроз наземного та повітряного характеру	Розширюється область застосування існуючих формул
4	Розділ II. Завдання оцінки вразливості	Аналіз уразливих елементів і маршрутів проникнення	Не передбачено аналіз повітряних сценаріїв	Додати завдання з аналізу вразливості до загроз повітряного характеру	Методично вводиться аналіз БпЛА
5	Розділ II. Вихідні дані	Проектна загроза, маршрути, бар’єри	Вихідні параметри непридатні для БпЛА	Дозволити використання параметрів повітряного підходу, зон виявлення, часу реагування	Забезпечується коректність розрахунків
6	Розділ III. Сценарії дій правопорушника	Сценарій = рух диверсійної групи	Лінійна наземна модель	Закріпити можливість формування сценаріїв дій повітряних цілей	Формалізується повітряна атака
7	Розділ III. Критична точка виявлення	Визначається вздовж маршруту проникнення	Для БпЛА маршрут відсутній	Визначати критичну точку виявлення як момент часу, достатній для нейтралізації	Перехід від просторової до часової логіки

Продовження таблиці 4.1

№	**Розділ / пункт Порядку №169**	**Чинний нормативний зміст (узагальнено)**	**Виявлена нормативно-методична проблема**	**Запропонована зміна / доповнення**	**Методологічний ефект**
8	Розділ III. Час затримки	Затримка бар'єрами	Для БпЛА $T_{delay} \approx 0$	Замінити на аналіз доступного часу реагування $T_{available}$	Узгодження з реальними сценаріями
9	Розділ III. Сили реагування	Реагування після виявлення	Орієнтація на фізичне затримання	Включити реагування засобами РЕБ, ППО, мобільних груп	Легалізація антидронових заходів
10	Розділ III. Людський фактор	Розглядається опосередковано	Критичний для ідентифікації БпЛА	Ввести оцінку імовірності коректного рішення персоналу	Підвищується точність моделі
11	Додатки. Ймовірності	Імовірності подолання бар'єрів	Орієнтація на фізичне проникнення	Дозволити використання імовірностей виявлення та нейтралізації повітряних цілей	Зберігається формалізм Порядку
12	Додатки. Інтегральна ймовірність	P визначається для наземного нападу	Неможливість прямого застосування	Закріпити, що P може визначатися для повітряних сценаріїв за окремою методикою	Формується "вхід" для нового додатку
13	Додатки. Оцінка ризику	$R = P \times (1 - P) \times C$	Формула не забороняє БпЛА, але не адаптована	Уточнити, що P може бути інтегральною ймовірністю протидії БпЛА	Зберігається нормативна спадковість
14	Структура звіту	Опис заходів та якісні висновки	Відсутній розділ про БпЛА	Додати обов'язковий розділ «Оцінка загроз повітряного характеру»	Забезпечується практичне застосування
15	Висновки оцінки	Констатація відповідності	Можлива ілюзія захищеності	Вимагати наведення числових показників ризику (за наявності загроз)	Перехід від формальності до результативності

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конвенція про фізичний захист ядерного матеріалу : Міжнародний документ від 26 жовт. 1979 р. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/995_024 (дата звернення: 02.10.2023).

2. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) : IAEA Nuclear Security Series No. 13. Vienna : IAEA, 2011. 57 p.

3. Поправка до Конвенції про фізичний захист ядерного матеріалу : Міжнародний документ від 08 лип. 2005 р. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/993_525 (дата звернення: 07.01.2024).

4. Objective and Essential Elements of a State's Nuclear Security Regime : Nuclear Security Fundamentals : IAEA Nuclear Security Series No. 20. Vienna : IAEA, 2013. 24 p.

5. Ядерна безпека, захищеність та гарантії в Україні : Резолюція Ради керуючих МАГАТЕ GOV/2022/71 від 17 листоп. 2022 р. [Електронний ресурс] URL:https://www.iaea.org/sites/default/files/22/11/gov2022-71_ukr.pdf (дата звернення: 10.01.2024).

6. Nuclear Safety, Security and Safeguards in Ukraine : 2nd Summary Report by the Director General. Vienna : IAEA, 2024. 52 p.

7. Про затвердження Вимог до системи фізичного захисту ядерних установок та ядерних матеріалів : Наказ Державної інспекції ядерного регулювання України від 28 серп. 2018 р. № 332. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/z1079-18 (дата звернення: 12.01.2024).

8. Risk Management for Nuclear Security : IAEA Nuclear Security Series No. 30-G. Vienna : IAEA, 2017. 44 p.

9. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) : IAEA Nuclear Security Series No. 13. Vienna : IAEA, 2011. 57 p.

10. The Role of Electronic Warfare in Modern Conflict : Technical Report. Kyiv : National Defense University of Ukraine, 2023. 112 p. (Нове джерело для РЕБ).

11. Аналітична доповідь щодо викликів ядерній безпеці в умовах збройної агресії РФ. Київ : НІСД, 2023. 45 с. (Нове джерело для кінетичної вразливості).

12. Preventive and Protective Measures against Insider Threats : IAEA Nuclear Security Series No. 8-G (Rev. 1). Vienna : IAEA, 2020. 58 p. (Нове джерело для інсайдерів).

13. Стан дотримання прав людини на тимчасово окупованих територіях України : Спеціальна доповідь Уповноваженого ВРУ з прав людини. Київ, 2024. (Нове джерело для підтвердження тиску на персонал).

14. Security of Radioactive Material during Transport : IAEA Nuclear Security Series No. 9-G (Rev. 1). Vienna : IAEA, 2021. 104 p. (Нове джерело для логістики).

15. Regulations for the Safe Transport of Radioactive Material : Specific Safety Requirements No. SSR-6 (Rev. 1). Vienna : IAEA, 2018. 165 p. (Нове джерело для порівняння стандартів контейнерів).

16. Computer Security at Nuclear Facilities : IAEA NSS No. 17. Vienna : IAEA, 2011. 75 p. (Нове джерело для кібербезпеки).

17. Computer Security for Nuclear Security : IAEA NSS No. 33-T. Vienna : IAEA, 2018. 96 p. (Нове джерело для NSS 33-T).

18. Звіт про стан ядерної та радіаційної безпеки в Україні у 2023 році. Київ : ДІЯРУ, 2024. 84 с. (Нове джерело для ситуації з АСКРО).

19. Development, Use and Maintenance of the Design Basis Threat : Implementing Guide : IAEA Nuclear Security Series No. 10. Vienna : IAEA, 2009. 74 p. (Нове джерело).

20. Considerations for Explosive Remnants of War and Other Conflict Situations at Nuclear Facilities : IAEA TECDOC-1867. Vienna : IAEA, 2019. 48 p. (Нове джерело).

21. Preparedness and Response for a Nuclear or Radiological Emergency : General Safety Requirements Part 7 : IAEA Safety Standards Series No. GSR Part 7. Vienna : IAEA, 2015. 102 p. (Нове джерело для аварійної готовності).

22. Закон України Про використання ядерної енергії та радіаційну безпеку від 08 лют. 1995 р. № 39/95-ВР. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/39/95-вр (дата звернення: 10.02.2024).

23. Закон України Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання від 19 жовт. 2000 р. № 2064-III. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/2064-14 (дата звернення: 19.02.2024).

24. Наказ Державної інспекції ядерного регулювання України Про затвердження Правил фізичного захисту ядерних установок та ядерних матеріалів від 04 серп. 2006 р. № 116. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/z0986-06 (дата звернення: 08.03.2024).

25. Наказ Державної інспекції ядерного регулювання України Про затвердження Вимог до комплексу інженерно-технічних засобів фізичного захисту від 05 груд. 2011 р. № 176. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/z1456-11 (дата звернення: 10.03.2024).

26. Вимоги до систем фізичного захисту ядерних установок та ядерних матеріалів (НП 306.5.02/3.068-2001) : Норми та правила з ядерної та радіаційної безпеки : затвердж. наказом ДІЯРУ від 28 черв. 2001 р. № 44.

27. Garcia M. L. Design and Evaluation of Physical Protection Systems. 2nd Edition. Burlington : Elsevier, 2007. 376 p.

28. Сухоручкін В. В. Моделювання та аналіз систем фізичного захисту ядерних установок : дис. ... канд. техн. наук : 05.14.14. Київ : КПІ ім. Ігоря Сікорського, 2018. 165 с.

29. Кондратов С. І. Ядерна безпека та фізичний захист у контексті національної безпеки України : монографія. Київ : НІСД, 2015. 240 с.

30. Ядерна та радіаційна безпека : науково-технічний журнал. Київ : ДНТЦ ЯРБ, 2023. № 4 (100). 88 с.

31. Nuclear Security during Armed Conflict : Special Report / World Institute for Nuclear Security (WINS). Vienna : WINS, 2022. 42 p.

32. Ковчар О., Сухоручкін В. Аналіз концептуальних прогалин міжнародних стандартів ядерної захищеності під час воєнних операцій. Ядерна та радіаційна безпека. 2023. № 2 (98). С. 115-128.

33. Bunn M., Roth N. The History of Nuclear Security. The Oxford Handbook of International Security. 2018. P. 456-472.

34. Ramana M. V. Attacks on Nuclear Facilities: Historical Context and Contemporary Threats. Global Security: Health, Science and Policy. 2021. Vol. 6, No. 1. P. 1–15.

35. Stulberg A. N. Nuclear Security in the Age of Strategic Instability. Strategic Studies Quarterly. 2023. Vol. 17, No. 2. P. 88–110.

36. Bennett R. K. The Raid on Osirak: A Case Study in Preemptive Strike. Military History Journal. 2019. Vol. 12, No. 4. P. 22–30.

37. Ford C. A. Nuclear Security and the Threat of Hybrid Warfare. Journal of Nuclear Materials Management. 2020. Vol. 48, No. 3. P. 12–25.

38. Загнітко О. В., Степанов Є. В. Психологічна стійкість персоналу АЕС в умовах воєнного стану. Ядерна та радіаційна безпека. 2024. № 1 (101). С. 45–54.

39. IAEA Director General. Report on the Safety and Security of Nuclear Facilities in Ukraine based on the 7 Pillars. Vienna : IAEA, 2023. 38 p.

40. Sayenko S. Y., Sanchenko V. M. Vulnerability analysis of ZNPP physical protection system under conditions of military occupation. Problems of Atomic Science and Technology. 2023. No. 4 (146). P. 112–120.

41. Зеркаль О. В. Енергетичний тероризм як новий виклик міжнародній безпеці: досвід України. Стратегічні пріоритети. 2023. № 1-2. С. 58–70.

42. Malyi V., Kostykov S. Comparison of Fukushima-Daiichi accident and ZNPP blackout scenarios. Nuclear and Radiation Safety. 2024. No. 2 (102). P. 34–42.

43. Kovchar O. V. Resilience of Ukrainian NPPs to long-term loss of off-site power during warfare. Scientific Papers of the Institute for Nuclear Research. 2023. Vol. 24, No. 3. P. 215–225.

44. Азаров Д. С. Правовий захист ядерних об’єктів у період збройних конфліктів: виклики сучасності. Часопис Київського університету права. 2023. № 2. С. 156–162.

45. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 08 черв. 1977 р. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/995_199 (дата звернення: 21.03.2024).

46. Henckaerts J.-M., Doswald-Beck L. Customary International Humanitarian Law. Volume I: Rules. Cambridge : Cambridge University Press, 2005. 621 p. (Rule 42. Works and Installations Containing Dangerous Forces).

47. Sanchenko V. Protection of Nuclear Facilities under International Humanitarian Law: The Case of Ukraine. Journal of Conflict and Security Law. 2023. Vol. 28, No. 1. P. 45–67.

48. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв збройних конфліктів неміжнародного характеру (Протокол II), від 08 черв. 1977 р. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/995_200 (дата звернення: 16.04.2024).

49. Butkevych O. Attacks on Nuclear Facilities: A Violation of International Law. Ukrainian Journal of International Law. 2022. No. 3. P. 12–19.

50. ICRC. Nuclear Power Plants in Armed Conflict: Frequently Asked Questions. Geneva : International Committee of the Red Cross, 2022. [Електронний

ресурс] URL:https://www.icrc.org/en/document/nuclear-power-plants-armed-conflict-faq (дата звернення: 01.05.2024).

51. Agreement on the Prohibition of Attack against Nuclear Installations and Facilities between Pakistan and India : Intern. document of 31 Dec. 1988. [Електронний ресурс] URL:https://treaties.un.org/doc/Publication/UNTS/Volume%201577/v1577.pdf (дата звернення: 11.05.2024).

52. Bunn G. Strengthening Nuclear Security Against Post-September 11 Threats. The Nonproliferation Review. 2002. Vol. 9, No. 3. P. 138–151. (Стаття Дж. Банна, де аналізується "право ініціативи" та роль МАГАТЕ).

53. Tucker J. B. Strategies for Preventing Terrorism at Nuclear Facilities. The Nonproliferation Review. 1993. Vol. 1, No. 1. P. 20–28. (Одне з перших джерел щодо ad hoc угод для захисту ядерних об'єктів).

54. African Nuclear-Weapon-Free Zone Treaty (Treaty of Pelindaba) : Intern. document of 11 April 1996. [Електронний ресурс] URL:https://au.int/en/treaties/african-nuclear-weapon-free-zone-treaty-treaty-pelindaba (дата звернення: 17.05.2024).

55. Goldblat J. The Treaty of Pelindaba: An Assessment. Security Dialogue. 1996. Vol. 27, No. 2. P. 201–210.

56. Roscini M. The Protection of Nuclear Power Plants in the Event of Armed Conflict. The British Year Book of International Law. 2010. Vol. 80, No. 1. P. 135–182. (Фундаментальне дослідження, де детально розібрано кейс Договору Пеліндаба та позицію США).

57. Pella V. The International Protection of Nuclear Energy. Nuclear Law Bulletin. 2005. No. 76. P. 7–24.

58. Committee on Disarmament. Joint US-USSR Proposal on Major Elements of a Treaty Prohibiting the Development, Production, Stockpiling and Use of Radiological Weapons : Document CD/31 of 9 July 1979. Geneva, 1979.

59. Conference on Disarmament. Report of the Ad Hoc Committee on Radiological Weapons : Document CD/1027. Geneva, 1990.

60. Reyners P. The Protection of Nuclear Facilities Against the Effects of Armed Conflict. International Nuclear Law: Essentials. Paris : OECD Publishing, 2016. P. 325–340. (Стаття П'єра Рейнерса, колишнього президента INLA, де викладено концепцію 2003 року).

61. Rhodes R. The Interface between Safety and Security at Nuclear Power Plants. Nuclear Engineering International. 2015. Vol. 60, No. 734. P. 14–16. (Класичне визначення різниці між Safety та Security).

62. IAEA Board of Governors. The safety, security and safeguards implications of the situation in Ukraine : Resolution GOV/2022/17. Vienna : IAEA, 2022.

63. Grossi R. M. Statement to the IAEA Board of Governors on the situation in Ukraine. Vienna : IAEA, 2 March 2022. [Електронний ресурс] URL: https://www.iaea.org/newscenter/statements/statement-to-the-iaea-board-of-governors-on-the-situation-in-ukraine-02-03-2022 (дата звернення: 11.06.2024).

64. Findlay T. Nuclear Energy and Global Governance: Ensuring Safety, Security and Non-proliferation. London : Routledge, 2011. 264 p.

65. The Interface Between Safety and Security at Nuclear Power Plants : INSAG-24. Vienna : IAEA, 2010. 29 p.

66. AdSec/INSAG. Joint Report on the Interface between Nuclear Safety and Nuclear Security. Vienna : IAEA, 2020.

67. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) : IAEA Nuclear Security Series No. 13. Vienna : IAEA, 2011. 57 p. (Параграфи щодо розподілу відповідальності).

68. Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme : Implementing Guide : IAEA Nuclear Security Series No. 19. Vienna : IAEA, 2013. 78 p.

69. Erästö T. Nuclear security in Ukraine: One year on. SIPRI Commentary. 2023. February. [Електронний ресурс] URL:https://www.sipri.org/commentary/2023/nuclear-security-ukraine-one-year

(дата звернення: 24.07.2024). (Джерело, що містить інтерв'ю з експертами SIPRI).

70. Safety of Nuclear Power Plants: Design : Specific Safety Requirements No. SSR-2/1 (Rev. 1). Vienna : IAEA, 2016. 72 p. (Вимоги щодо захисту від зовнішніх подій, включаючи падіння літаків).

71. IAEA. Nuclear Security Contingency Planning : Nuclear Security Series No. 17-G. Vienna : IAEA, 2012. 102 p. (Фундаментальний документ щодо планування на випадок непередбачуваних подій).

72. World Institute for Nuclear Security (WINS). Nuclear Security During a Pandemic: Lessons Learned from COVID-19. Vienna : WINS, 2021. 44 p.

73. Суходоля О. М. Забезпечення стійкості енергетичної системи України в умовах воєнної агресії : аналіт. доп. Київ : НІСД, 2022. 84 с. [Електронний ресурс] URL:https://niss.gov.ua/publications/analitychni-dopovidi/zabezpechennya-stiykosti-enerhetychnoyi-systemy-ukrayiny-v-umovakh (дата звернення: 04.08.2024).

74. Про визначення органу, відповідального за організацію роботи з визначення проектної загрози : Постанова Кабінету Міністрів України від 27 серп. 2022 р. № 956. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/956-2022-п (дата звернення: 13.09.2024).

75. Sanchenko V., Sayenko S. Adaptation of the National Nuclear Security Regime to Armed Conflict Conditions: The Ukrainian Experience. Nuclear Security Transitions. 2024. Vol. 3, No. 1. P. 15–29.

76. Про реалізацію експериментального проєкту щодо нарощування спроможностей радіоелектронного прикриття об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 15 лип. 2024 р. № 881. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/881-2024-п (дата звернення: 25.09.2024).

77. Singhal G., Bansod B., Mathew L. Unmanned Aerial Vehicles: a review. 2018 IEEE International Conference on Industrial Technology (ICIT). 2018. P. 1337–1342.

78. Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. Official Journal of the European Union. 2019. L 152/1.

79. Houthi drone attack on Abu Dhabi fuel trucks kills 3. Aljazeera. 2022. [Електронний ресурс] URL:https://www.aljazeera.com/news/2022/1/17/abu-dhabi-fire-near-airport-truck-explosions-reported (дата звернення: 11.10.2024).

80. Pradier M. Greenpeace crashes 'Superman' drone into French nuclear plant. Reuters. 2018. [Електронний ресурс] URL: https://www.reuters.com/article/us-france-nuclear-greenpeace-idUSKBN1JT1A1 (дата звернення: 11.11.2025).

81. Grisaro H., Dancygier A. N. Assessment of the penetrability of a drone into a civil structure. International Journal of Protective Structures. 2021. Vol. 12, No. 3. P. 315–334.

82. Venezuela President Maduro survives 'drone assassination attempt'. BBC News. 2018. [Електронний ресурс] URL:https://www.bbc.com/news/world-latin-america-45071131 (дата звернення: 03.12.2024).

83. Iraq PM Mustafa al-Kadhimi survives drone 'assassination attempt'. BBC News. 2021. [Електронний ресурс] URL:https://www.bbc.com/news/world-middle-east-59194247 (дата звернення: 11.12.2046).

84. Saudi Arabia oil attacks: Drones and missiles used in Aramco strike. BBC News. 2019. [Електронний ресурс] URL:https://www.bbc.com/news/world-middle-east-49712417 (дата звернення: 01.02.2025).

85. Monnik T. The Use of Consumer Drones by Non-State Actors. Conflict Kasteloo J. DJI is the world leader in drone technology. DroneDJ. 2020. [Електронний ресурс] URL:https://dronedj.com/2020/03/24/dji-world-leader-drone-technology/ (дата звернення: 10.02.2025).Armament Research. 2021. 42 p.

86. Kasteloo J. DJI is the world leader in drone technology. DroneDJ. 2020. [Електронний ресурс] URL:https://dronedj.com/2020/03/24/dji-world-leader-drone-technology/ (дата звернення: 11.02.2025).

87. Hambling D. A drone was used to attack a US power grid for the first time. New Scientist. 2021. [Електронний ресурс] URL:https://www.newscientist.com/article/2296417-a-drone-was-used-to-attack-a-us-power-grid-for-the-first-time/ (дата звернення: 25.03.2025).

88. Sweden's nuclear plants hit by mystery drone flights. BBC News. 2022. [Електронний ресурс] URL:https://www.bbc.com/news/world-europe-60032943 (дата звернення: 01.04.2025).

89. Swedish police search drones near nuclear plants. Reuters. 2022. [Електронний ресурс] URL:https://www.reuters.com/world/europe/swedish-police-search-drones-near-nuclear-plants-2022-01-17/ (дата звернення: 03.04.2025).

90. Tahir A., Böling J., Haghbayan M. H. Swarms of Unmanned Aerial Vehicles — A Review. IEEE Access. 2019. Vol. 7. P. 44613–44632.

91. Most Unmanned Aerial Vehicles (UAVs) airborne simultaneously. Guinness World Records. 2021. [Електронний ресурс] URL:https://www.guinnessworldrecords.com/world-records/most-unmanned-aerial-vehicles-uavs-airborne-simultaneously (дата звернення: 12.05.2025).

92. Abdalla A., Abushrkh S. Security of Unmanned Aerial Vehicles: A Review of Vulnerabilities and Countermeasures. Journal of Defense Modeling and Simulation. 2020. Vol. 17. P. 1–25.

93. Ziyang G., Zhao J. Counter-UAV Systems: A Review. IEEE Aerospace and Electronic Systems Magazine. 2018. Vol. 33. P. 6–18.

94. Crino S., Dreby C. Drone Attacks Against Critical Infrastructure: A Real and Growing Threat. Center for International Maritime Security. 2020. [Електронний ресурс] URL:https://cimsec.org/drone-attacks-against-critical-infrastructure-a-real-and-growing-threat/ (дата звернення: 13.05.2025).

95. Yaacoub J. P., Noura H., Salman O., Chehab A. Contra-unmanned aircraft system: A review. Ad Hoc Networks. 2020. Vol. 107. P. 102165.

96. Andrasi P., Radisic T., Ivošević Š., Škurla J. Night-time detection of UAVs using thermal imaging. IEEE Aerospace and Electronic Systems Magazine. 2017. Vol. 32, No. 9. P. 33–40.

97. Schaffer T., Winkler V., Richter J. Acoustic detection of small UAVs in noisy environments. Applied Acoustics. 2021. Vol. 173. P. 107693.

98. Beamforming algorithms for microphone arrays in drone detection : Technical Report. [S. l.], 2016.

99. Burshtein D., Weinstein E. Robust beamforming for acoustic signals. IEEE Transactions on Speech and Audio Processing. 2001. Vol. 9, No. 1. P. 37–45.

100. Gannot S., Burshtein D., Weinstein E. Signal enhancement using beamforming and nonstationarity with applications to speech. IEEE Transactions on Signal Processing. 2001. Vol. 49, No. 8. P. 1614–1626.

101. Abdullah A. et al. Sound intensity and distance: An analysis for UAV acoustic signatures. Journal of Engineering Science. 2019. Vol. 10. P. 12–18.

102. Hirabayashi K. et al. Visual detection and tracking of UAVs under various weather conditions. Sensors. 2020. Vol. 20, No. 24. P. 72–85.

103. Wu X., Fu G., Li M. Deep learning for unmanned aerial vehicle detection and classification. IEEE Transactions on Geoscience and Remote Sensing. 2017. Vol. 55. P. 120–132.

104. Barisic A., Car M., Orsag M. Deep learning based drone detection and classification. 2019 International Conference on Unmanned Aircraft Systems (ICUAS). Trogir, 2019. P. 150–159.

105. Al-Sa'd M. et al. RF-based drone detection and identification using deep learning. Sensors. 2019. Vol. 19, No. 15. P. 32–44.

106. Oh K. et al. Analysis of radio frequency communication for UAVs. Electronics. 2020. Vol. 9, No. 11. P. 18–25.

107. Solidakis E. GSM-based communication for long-range UAV missions. Telecom Review. 2017. No. 4. P. 10–15.

108. 108.Ferreira R. et al. Software Defined Radio for UAV signal detection and jamming. Journal of Communications. 2022. Vol. 17, No. 5. P. 401–410.

109. Park S. et al. Radar-based detection and tracking of small UAVs. IEEE Access. 2021. Vol. 9. P. 143–156.

110. Ochodnicky J. et al. FMCW radar for small UAV detection. 2017 18th International Radar Symposium (IRS). Prague, 2017. P. 1–5.

111. Quevedo J. et al. Radar cross section analysis of small drones. IEEE Antennas and Wireless Propagation Letters. 2018. Vol. 17, No. 6. P. 971–975.

112. Maestre J. et al. Beamforming techniques for radar systems in counter-UAV applications. Digital Signal Processing. 2019. Vol. 92. P. 102–115.

113. Ezuma M. et al. Detection and classification of UAVs using radar and deep learning. IEEE Communications Magazine. 2021. Vol. 59, No. 12. P. 110–116.

114. Radartutorial. Basics of Radar Technology. [Електронний ресурс] URL: https://www.radartutorial.eu/index.en.html (дата звернення: 11.07.2025).

115. Drone Dome : Counter-Unmanned Aircraft System (C-UAS). Rafael Advanced Defense Systems. [Електронний ресурс] URL:https://www.rafael.co.il/worlds/land/drone-dome (дата звернення: 19.07.2025).

116. SkyNet Mi-5 : Counter-Drone Net Solution. Droptec. [Електронний ресурс] URL:https://www.droptec.ch (дата звернення: 11.08.2025).

117. Russia Has a New Way to Kill Drones: High-Power Microwaves. The National Interest. 2021. [Електронний ресурс] URL:https://nationalinterest.org (дата звернення: 29.08.2025).

118. Krauss J. D. Electromagnetics. - 4th ed. - New York : McGraw-Hill, 1992. - 864 p.

119. Sahmoudi M., Amin M. G. Robust GNSS receivers for interference and spoofing mitigation // Proceedings of the IEEE. - 2009. - Vol. 97, No. 3. - P. 510-527.

120. He Y. et al. GNSS-denied navigation for unmanned aerial vehicles : A review // Recent Advances in Electrical & Electronic Engineering. - 2018. - Vol. 11, No. 2. - P. 115-125.

121. Kapoor R. et al. TDOA-based localization in GNSS-denied environments // International Journal of Aerospace Engineering. - 2017. - Vol. 2017. - Art. ID 8235492.

122. Zhou Y. et al. Adversarial attacks on drone vision-based navigation // IEEE Transactions on Dependable and Secure Computing. - 2021. - Vol. 18, No. 5. - P. 2100-2115.

123. European Commission. Guidance on sampling methods for audit authorities. - Brussels : European Commission, 2017. - 102 p.

124. Lukasiewicz J. et al. Preventive anti-drone measures for critical infrastructure protection // Journal of Security and Sustainability Issues. - 2021. - Vol. 11, No. 2. - P. 45-58.

125. Watling J., Reynolds N. Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. - London : Royal United Services Institute (RUSI), 2023. - 38 p.

126. Ukraine’s air defense shot down 80% of Russian drones in last month: Report. - ABC News, 2024. [Електронний ресурс] URL:https://abcnews.go.com (дата звернення: 02.10.2025).

127. Reuters. Ukraine says it shot down 58 of 80 Russian drones in overnight attack. - 2025. - Jan. 14. [Електронний ресурс] URL:https://www.reuters.com (дата звернення: 04.10.2025).

128. Kyiv Post. Ukraine’s Air Defense Effectiveness Hits 80-85% Against Recent Massive Drone Attacks. - 2024. [Електронний ресурс] URL:https://www.kyivpost.com (дата звернення: 01.11.2025).

129. War & Sanctions. Orlan-10 Unmanned Aerial Vehicle: Technical Specifications and Components. [Електронний ресурс] URL: https://sanctions.nazk.gov.ua (дата звернення: 16.10.2025).

130. ISIS Online. Lancet Loitering Munition: Analysis of Use and Countermeasures. [Електронний ресурс] URL:https://isis-online.org (дата звернення: 10.11.2025).

131. Вікіпедія. Shahed 136 : [Електронний ресурс]. URL:https://uk.wikipedia.org/wiki/Shahed_136 (дата звернення: 11.11.2025).

132. Про затвердження комплексного плану заходів щодо реалізації положень нової редакції Проєктної загрози щодо ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання в Україні : Розпорядження Кабінету Міністрів України від 04 верес. 2013 р. № 684-р.

133. Проєктна загроза : [Електронний ресурс] // Офіційний вебсайт Державної інспекції ядерного регулювання України. URL:https://snriu.gov.ua. (дата звернення: 15.12.2025).

134. Engineering Safety Aspects of the Protection of Nuclear Power Plants against Relevant External Events : IAEA Safety Reports Series No. 86. - Vienna : IAEA, 2017. - 154 p.

135. Про затвердження Порядку функціонування державної системи фізичного захисту : Постанова Кабінету Міністрів України від 21 груд. 2011 р. № 1337. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/1337-2011-п (дата звернення: 02.01.2026).

136. Про затвердження Порядку визначення рівня фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання відповідно до їх категорії : Постанова Кабінету Міністрів України від 26 квіт. 2003 р. № 625. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/625-2003-п (дата звернення: 18.01.2026).

137. Методика визначення рівня фізичного захисту ядерних установок та ядерних матеріалів : [з урахуванням змін та доповнень]. Зазвичай це відомчий документ, що деталізує Постанову № 625.

138. Про затвердження Порядку проведення державної перевірки систем фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та планів взаємодії у разі вчинення актів ядерного тероризму : Постанова Кабінету Міністрів України від

12 берез. 2003 р. № 327. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/327-2003-п (дата звернення: 20.01.2026).

139. Про затвердження державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання та щодо радіоактивних відходів : Постанова Кабінету Міністрів України від 24 лип. 2013 р. № 598. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/598-2013-п (дата звернення: 02.02.2026).

140. Про затвердження Положення про організацію взаємодії Збройних Сил України, Служби безпеки України та Міністерства внутрішніх справ України щодо забезпечення антитерористичного захисту об'єктів критичної інфраструктури : [приклад можливої назви нормативного акта, на який посилається текст у контексті взаємодії з силами оборони].

141. Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів : Наказ Державної інспекції ядерного регулювання України від 30 листоп. 2010 р. № 169. [Електронний ресурс] URL:https://zakon.rada.gov.ua/laws/show/z1295-10 (дата звернення: 12.02.2026).

ДОДАТКИ

ДОДАТОК А НОРМАТИВНО-ПРАВОВИЙ АНАЛІЗ ВІДПОВІДНОСТІ МІЖНАРОДНИХ РЕКОМЕНДАЦІЙ МАГАТЕ ТА ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ ФІЗИЧНОГО ЗАХИСТУ ЯДЕРНИХ УСТАНОВОК

Таблиця А.1 – Порівняльний нормативно-правовий аналіз у сфері фізичного захисту ядерних установок

№	Міжнародний документ (МАГАТЕ)	Ключова вимога	Нормативно-правовий акт України	Статус відповідності	Коментар щодо застосовності в умовах війни
1	Конвенція про фізичний захист ядерного матеріалу (CPPNM) та Поправка 2005 р.	Забезпечення фізичного захисту ЯМ та ЯУ	Закон України №2064-IV	Формальна	Конвенція не застосовується до дій регулярних збройних сил
2	INFCIRC/225/Rev.5	Захист від зовнішнього порушника	НП 306.02/3.068	Часткова	Проектна загроза не враховує state actor
3	INFCIRC/225/Rev.5	Глибоко ешелонований захист	НП 306.02/3.068	Обмежена	Бар’єри не розраховані на важке озброєння
4	NSS No.10 (DBT)	Формування проектної загрози	Відомчі методики	Критичний gap	Відсутні сценарії війни та окупації
5	NSS No.20	Державний режим ядерної фізичної безпеки	Закон №2064-IV	Непридатна	Втрата контролю регулятора під час окупації
6	NSS No.30-G	Управління ризиками	Внутрішні процедури оператора	Низька	Неможливість оцінки ризиків у бойових умовах
7	NSS No.17	Комп’ютерна безпека	Вимоги з кіберзахисту АЕС	Часткова	Не враховано кінетично-кіберні атаки
8	GSR Part 7	Аварійна готовність та реагування	Плани аварійного реагування	Непридатна	Евакуація неможлива в зоні бойових дій
9	TECDOC-1867	ERW та конфліктні ситуації	Відсутні аналоги	Декларативна	Орієнтація на постконфліктний період
10	NSS No.9	Безпека транспортування ЯМ	Галузеві інструкції	Критичний gap	Маршрути та конвої не захищені від БпЛА

Таблиця А.2 – Ключові нормативні прогалини у сфері фізичного захисту ЯУ

Кластер загроз	**Наявність нормативного регулювання**
Дії регулярних збройних сил	❌ відсутнє
Окупація ядерної установки	❌ відсутнє
Примус персоналу	❌ відсутнє
Застосування БпЛА	⚠ частково
Радіоелектронна боротьба	⚠ частково
Втрата регуляторного контролю	❌ відсутнє
Кінетично-кіберні атаки	❌ відсутнє
Блокування аварійного реагування	❌ відсутнє

ДОДАТОК Б КЛАСИФІКАЦІЯ ЗАГРОЗ ТА СЦЕНАРІЇ ВПЛИВУ НА ЯДЕРНІ УСТАНОВКИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

Б.1. Розширена класифікація повітряних загроз для СФЗ

З врахуванням специфіки сучасних конфліктів, загрози класифікуються за походженням, тактикою та технічними характеристиками (Таблиця Б.1).

Таблиця Б.1 – Класифікація сучасних повітряних загроз

Тип загрози	Характеристика	Основна ціль (Цільовий елемент)
Розвідувальні БпЛА	Малопомітні, тривалий час баражування	Збір даних про патрулі, позиції ППО, стан огорожі
Ударні БпЛА (Камікадзе)	Висока точність, рій цілей	Трансформатори, машзали, сховища ВЯП
FVP-дрони	Висока маневреність, керування оператором	Персонал на відкритій місцевості, камери відеоспостереження
Крилаті/Балістичні ракети	Велика руйнівна сила, висока швидкість	Гермооболонка реактора, щити управління

Б.2. Сценарії атак та механізми впливу

У межах дисертаційного дослідження визначено три базові сценарії, які використовуються для розрахунку ймовірностей у Додатку Г:

1. **Сценарій «Дистанційний саботаж» (Indirect Attack):**
   - *Мета:* Порушення електропостачання АЕС без прямого влучання в реактор.
   - *Дія:* Груповий наліт БпЛА на відкриті розподільчі пристрої (ВРП) та резервні дизель-генератори.
   - *Результат:* Режим «Blackout», перехід на аварійне розхолоджування.
2. **Сценарій «Комплексне проникнення» (Integrated Breach):**
   - *Мета:* Створення умов для проникнення ДРГ на територію.
   - *Дія:* Використання малих дронів для знищення сенсорної мережі (камер, тепловізорів) та засобів зв’язку СФЗ перед початком наземної фази.
   - *Результат:* Осліплення охорони, втрата контролю над периметром.

3. **Сценарій «Військовий шантаж / Окупація» (Occupational Threat):**

- *Мета:* Використання ЯУ як «ядерного щита».
- *Дія:* Розміщення важкої техніки та боєприпасів безпосередньо в технологічних приміщеннях (наприклад, машзали).
- *Результат:* Повна неможливість застосування стандартних протоколів нейтралізації порушників.

Б.3. Матриця вразливості критичних елементів (КЕ)

Для кожного КЕ визначено рівень пріоритетності захисту від повітряних загроз (Таблиця Б.2).

Таблиця Б.2 – Рівні вразливості ключових вузлів АЕС

Об'єкт (КЕ)	**Пріоритет захисту**	**Рекомендований засіб протидії**
Реакторне відділення	Високий	Ешелонована ППО, фізичне екранування
Машинний зал	Середній	Антидронові сітки, РЕБ
Сховище ВЯП	Високий	Пасивний захист, РЕБ
Відкриті розп. пристрої (ВРП)	Критичний	Мобільні вогневі групи (МВГ), димові завіси

ДОДАТОК В АРХІТЕКТУРА ТА ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ІНТЕГРОВАНОЇ СИСТЕМИ ПРОТИДІЇ БПЛА НА ЯДЕРНИХ УСТАНОВКАХ

В.1. Концептуальна схема ешелонованої оборони від повітряних загроз

Запропонована у дисертаційному дослідженні модель фізичного захисту базується на зонному принципі виявлення та нейтралізації. На відміну від класичної периметрової охорони, архітектура протидії БпЛА вимагає винесення зон виявлення за межі юридичного периметра ядерної установки (ЯУ).

Таблиця В.1 – Схематичне розмежування зон відповідальності

Зона (Ешелон)	**Радіус дії (км)**	**Функціональне призначення**	**Типові технічні засоби**	**Відповідальний суб'єкт**
I. Зона раннього попередження	10 – 50 км	Виявлення аеродинамічних цілей, класифікація «свій-чужий», передача цілевказівки.	РЛС огляду повітряного простору, системи РТР (радіотехнічної розвідки) національної системи ППО.	Повітряні Сили ЗСУ / ППО
II. Зона ідентифікації та супроводу	3 – 10 км	Підтвердження цілі, визначення типу БпЛА (розвідник/ударний), розрахунок траєкторії	Локальні РЛС малого радіусу, оптико-електронні станції, акустичні сенсори.	Підрозділ охорони ЯУ / НГУ
III. Зона некінетичної нейтралізації	1 – 3 км	Радіоелектронне придушення (РЕБ), блокування каналів керування та навігації (GNSS spoofing/jamming).	Стаціонарні комплекси РЕБ, купольні системи захисту.	Підрозділ охорони ЯУ (спецпідрозділ РЕБ)
IV. Зона кінетичного перехоплення	0.5 – 1.5 км	Фізичне знищення БпЛА на підльоті до критичних елементів.	Мобільні вогневі групи (МВГ), зенітні установки, ПЗРК.	НГУ / МВГ
V. Зона пасивного захисту	0 км (Об'єкт)	Мінімізація наслідків влучання або падіння уламків.	Інженерні конструкції (габіони, сітки, бетонні укриття), захист трансформаторів.	Експлуатуюча організація (Оператор АЕС)

В.2. Тактико-технічні характеристики (ТТХ) засобів виявлення (вхідні дані для розрахунку P_{det})

Для коректного розрахунку ймовірності виявлення (P_{total_D}), наведеного у Додатку Г, необхідно використовувати параметри сенсорів, адаптовані до характеристик малорозмірних цілей (БпЛА).

Таблиця В.2 – Порівняльні характеристики сенсорів виявлення

Тип сенсора	**Принцип дії**	**Ефектив-на даль-ність (для RCS 0.01 м²)**	**Переваги**	**Недоліки / Обмеження**	**Коефіцієнт надійності в умовах перешкод (K_{env})**
РЛС (Активний радар)	Відбиття радіохвиль	1.5 – 3.0 км	Всепогодність, точне визначення дальності та швидкості.	Складність виявлення завислих дронів та пластикових корпусів. Вразливість до радіоелектронних перешкод.	0.6 – 0.8
РТР (RF-сканер)	Перехоплення сигналів керування	3.0 – 5.0 км	Пасивний режим (не випромінює), виявляє оператора, класифікує тип дрона за протоколом зв'язку.	Неефективний проти повністю автономних дронів (режим радіомовчання / інерціальна навігація).	0.4 – 0.9 (залежить від режиму БпЛА)
Оптико-електронний (EO/IR)	Візуальний/Тепловий образ	0.5 – 1.2 км	Візуальне підтвердження загрози, запис доказів. Ефективний вночі (IR).	Залежність від погодних умов (туман, дощ). Вузьке поле зору (потребує попередньої цілевказівки).	0.3 – 0.9 (залежить від погоди)
Акустичний	Звукова сигнатура двигунів	0.3 – 0.8 км	Працює поза прямою видимістю, пасивний, дешевий.	Чутливість до промислового шуму АЕС та вітру. Низька точність визначення координат.	0.4 – 0.6

В.3. Матриця ефективності засобів нейтралізації (вхідні дані для розрахунку P_{neut})

Вибір засобу нейтралізації залежить від типу загрози (визначеного в Додатку Б) та зони знаходження цілі. Нижче наведено усереднені ймовірності успішної нейтралізації, що використовуються в математичній моделі.

Таблиця В.3 – Ефективність засобів протидії в залежності від класу БпЛА

Засіб протидії	Тип впливу	Ефектив-ність проти комерційних дронів (Mavic/Matrice)	Ефектив-ність проти FPV-дронів	Ефектив-ність проти БпЛА-камікадзе (Shahed-136)	Ризики для ЯУ (Safety)
РЕБ (GNSS Jamming)	Навігаційний спуфінг/глушіння	**Висока** (0.8–0.9). Дрон зависає або летить за вітром.	**Низька** (0.1–0.2). FPV часто не використовують GPS.	**Низька** (0.2–0.3). Використовують інерціальні системи та CRPA антени.	Мінімальні. Можливий вплив на системи синхронізації часу АЕС.
РЕБ (C2 Link Jamming)	Розрив каналу керування	**Висока** (0.8–0.9). Активація режиму "Return to Home".	**Середня** (0.5–0.7). Залежить від частотного діапазону та потужності.	**Нульова**. Дрон летить автономно по координатах.	Мінімальні. Ризик "дружнього вогню" по власних засобах зв'язку.
Кінетичні засоби (МВГ)	Стрілецьке ураження	**Середня** (0.4–0.6). Мала ціль, важко влучити.	**Середня** (0.4–0.6). Висока маневреність цілі.	**Висока** (0.6–0.8). Велика, передбачувана траєкторія.	Високі. Падіння культа уламків на критичну інфраструктуру.
Спецзасоби (Сіткомети/Дрони-перехоплювачі)	Фізичне захоплення	**Висока** (0.7–0.8). Для завислих цілей.	**Низька**. Складність перехоплення швидкісної цілі.	**Низька**. Невідповідність швидкостей.	Середні. Контрольоване падіння.

В.4. Алгоритм прийняття рішення в інтегрованій системі фізичного захисту

Інтеграція підсистем вимагає чіткого алгоритму дій оператора ЦПУ (Центрального пульта управління) фізичного захисту, який мінімізує час реакції ($T_{response}$).

1. **Подія:** Спрацювання сенсора (РЛС/Акустика).
2. **Верифікація:**
   - *Автоматична:* Кореляція даних від двох різних фізичних сенсорів (наприклад, Радар + Тепловізор).
   - *Оператор:* Візуальне підтвердження на моніторі.
3. **Ідентифікація загрози (згідно Додатку Б):**
   - *Тип А (Розвідник)* -> Пріоритет: Приховування/РЕБ.
   - *Тип Б (Ударний)* -> Пріоритет: Негайне знищення.
4. **Вибір методу нейтралізації (автоматизована підказка системи підтримки прийняття рішень):**
   - *Якщо* ціль над критичним елементом -> Тільки РЕБ (заборона стрільби).
   - *Якщо* ціль на підльоті (Зона IV) -> **Мобільна вогнева група**.
5. **Активація протоколу безпеки:**
   - Сповіщення персоналу (Укриття).
   - Аварійне відключення вразливих систем (якщо передбачено регламентом).

ДОДАТОК Г АЛГОРИТМИ ТА РОЗРАХУНКОВІ МОДЕЛІ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ФІЗИЧНОГО ЗАХИСТУ ВІД ПОВІТРЯНИХ ЗАГРОЗ

Г.1. Блок-схема загального алгоритму оцінки ризику від БпЛА

Загальний алгоритм реалізує ризик-орієнтований підхід, адаптований до умов воєнного часу, і складається з послідовних етапів ідентифікації загрози, розрахунку ефективності підсистем та визначення залишкового ризику.

- **Ініціалізація даних:** Визначення параметрів захищеного об'єкта (категорія, критичні елементи) та профілю загрози (тип БпЛА, тактика).
- **Розрахунок імовірності виявлення** (P_{total_D}): Оцінка сукупної ефективності сенсорів (РЛС, РТР, акустика, оптика) з урахуванням умов середовища.
- **Розрахунок імовірності нейтралізації** (P_{total_N}): Оцінка сукупної ефективності ефекторів (РЕБ, кінетичні засоби) з урахуванням часових обмежень.
- **Визначення інтегральної ефективності системи** (P_{sys}):$P_{sys} = P_{total\_D} \times P_{total\_N}$.
- **Оцінка наслідків (*C*):** Визначення коефіцієнта наслідків у разі успішної атаки (радіаційні, економічні, соціальні).
- **Розрахунок ризику (*R*):** $R = (1 - P_{sys}) \times C$.
- **Прийняття рішення:** Порівняння R з прийнятним рівнем R_{acc}. Якщо $R > R_{acc}$ - впровадження компенсуючих заходів.

Г.2. Математична модель розрахунку ймовірності виявлення повітряної цілі

Модель базується на ймовірнісному підході до оцінки надійності системи, що складається з N незалежних засобів виявлення (радіолокаційних, оптичних, акустичних, радіочастотних).

Імовірність виявлення БпЛА окремим *x*-м засобом (P_{ux}) є функцією від множини факторів впливу:

$$P_{ux} = f(WC, t, L, T, M, PAM, C, D),$$

де:

WC - погодні умови (опади, туман, вітер);

t - час доби (день/ніч);

L - умови місцевості (рельєф, забудова, рослинність);

T - тип БпЛА (мультиротор, крило, розмір RCS);

M - тип двигуна (електричний/ДВЗ – впливає на акустичну та теплову сигнатуру);

PAM - профіль польоту (висота, швидкість, маневрування);

C - компетентність персоналу/оператора;

D - відстань до цілі.

Розрахункова формула загальної ймовірності виявлення (P_{total_D}):

Для системи з *N* різнорідних сенсорів ймовірність того, що ціль буде виявлена хоча б одним із них, визначається як одиниця мінус ймовірність того, що ціль не буде виявлена жодним:

$$P_{total\_D} = 1 - \prod_{i=1}^{N}(1 - P_{ui}) = 1 - [(1 - P_{u1}) \cdot (1 - P_{u2}) \dots (1 - P_{uN})],$$

де P_{ui} — експериментально підтверджена ймовірність виявлення *i-м* засобом у заданих умовах.

Г.3. Математична модель розрахунку ймовірності нейтралізації повітряної цілі

Модель описує ефективність підсистеми активної протидії (РЕБ, вогневі засоби), що складається з *M* ешелонів або засобів.

Імовірність нейтралізації окремим *y*-м засобом (P_{uy}) визначається аналогічно до виявлення, але з урахуванням специфічних факторів протидії

(стійкість каналів управління БпЛА до завад, вразливість до кінетичного ураження):

$$P_{uy} = f(WC, t, L, T, M, PAM, C, D)$$

Розрахункова формула загальної ймовірності нейтралізації P_{total_N}:

$$P_{total\_N} = 1 - \prod_{j=1}^{M}\left(1 - P_{uj}\right) = 1 - [(1 - P_{u1}) \cdot (1 - P_{u2}) \dots (1 - P_{uM})]$$

Обмеження моделі: Розрахунок є валідним лише за умови, що час нейтралізації T_{neut} менший за час підльоту до критичної точки (T_{flight}).

Г.4. Інтегральна модель оцінки ризику (Risk Assessment Model)

Ризик ($R_{CU\ AS}$) розглядається як функція від ймовірності успішної атаки (P_{succ}) та масштабу наслідків (C).

1. **Ймовірність успішної атаки (P_{succ}):**

Атака вважається успішною, якщо система захисту не спрацювала. Ефективність системи захисту (P_{system}) є добутком ймовірностей успішного виявлення та успішної нейтралізації (подія виявлення є передумовою для нейтралізації):

$P_{system} = P_{total\_D} \times P_{total\_N}$

Відповідно, ймовірність успішної атаки (відмови систем=и):

$P_{succ} = 1 - P_{system} = 1 - (P_{total\_D} \times P_{total\_N})$

2. **Формула розрахунку ризику:**

$R_{CU\ AS} = [1 - (P_{total\_D} \times P_{total\_N}] \times C$

де C (Consequence) — коефіцієнт наслідків, що визначається відповідно до категорії ядерної установки (від 0 до 1, де 1 - катастрофічні наслідки з радіаційним викидом).

Г.5. Методика розрахунку необхідного обсягу вибірки для верифікації надійності обладнання

Для підтвердження заявлених виробником характеристик імовірності виявлення/нейтралізації (P_{ui}) необхідно проводити натурні випробування. Мінімальний розмір вибірки (n) для забезпечення статистичної достовірності результатів визначається за формулою:

$$n = \frac{N \cdot u^2 \cdot \sigma^2}{\Delta^2 (N-1) + u^2 \cdot \sigma^2},$$

де:

- N - обсяг генеральної сукупності (теоретична кількість можливих сценаріїв атак);
- u - квантиль нормального розподілу для заданого рівня довіри (наприклад, 1.96 для 95%);
- σ - середньоквадратичне відхилення результатів (попередня оцінка варіативності успіху);
- Δ - гранично допустима похибка результату (наприклад, 0.05 або 5%).

Г.6. Алгоритм оцінки кінетичної енергії падіння БпЛА

Для оцінки ризику вторинних наслідків (падіння збитого дрона на критичне обладнання) застосовується розрахунок кінетичної енергії удару (E_k):

$$E_k = \frac{1}{2} m v^2,$$

де:

- m - маса БпЛА (кг);
- v - швидкість падіння (м/с) у момент зіткнення з поверхнею.

Критерій прийнятності: Якщо $E_k > E_{crit}$ (межа стійкості будівельних конструкцій або корпусу обладнання), нейтралізація кінетичним способом над даною зоною заборонена, пріоритет надається засобам РЕБ або сіткометам.

ДОДАТОК Д ДОДАТКОВІ ІЛЮСТРАТИВНІ МАТЕРІАЛИ ТА ПРАКТИЧНІ КЕЙСИ (CASE STUDIES)

Д.1. Кейс №1: Аналіз вразливості ЗАЕС в умовах окупації та бойових дій

Цей кейс ілюструє невідповідність класичної моделі «Проєктної загрози» (DBT) умовам реальної війни, де ядерна установка стає об'єктом військового шантажу та майданчиком для розміщення військової техніки.

Рисунок Д.1 – Схема розміщення військової техніки поруч з ядерними реакторами на Запорізькій АЕС (ілюстрація порушення зон обмеженого доступу)

Події на Запорізькій АЕС демонструють відмову системи фізичного захисту на рівні «затримка» та «нейтралізація». Традиційні інженерні загородження не розраховані на протидію важкій бронетехніці. Це підтверджує необхідність переходу до запропонованої у Розділі 2 моделі інтеграції з силами оборони держави.

Д.2. Кейс №2: Характеристики помітності БпЛА типу «Shahed-136/Geran-2»

Ілюстрація проблеми виявлення малорозмірних цілей, яка була математично описана в Додатку Г.

Мала ЕПР у поєднанні з низькою висотою польоту та використанням композитних матеріалів робить такі об'єкти майже невидимими для застарілих РЛС, якими часто оснащувалися об'єкти критичної інфраструктури. Це обґрунтовує необхідність введення коефіцієнта P_{total_D} (ймовірність виявлення) у формулу ризику як критичного параметра.

Рисунок Д.2 – Порівняльна діаграма ефективної площі розсіювання (ЕПР/RCS) різних типів повітряних цілей

Д.3. Кейс №3: Наслідки кінетичного удару БпЛА по трансформаторному обладнанню

Ілюстрація важливості захисту розподільчих пристроїв для забезпечення власних потреб АЕС (проблема Blackout).

Рисунок Д.3 – Типові пошкодження високовольтного автотрансформатора внаслідок влучання дрона-камікадзе

Наслідки кінетичного удару по автотрансформатору: даний кейс підтверджує критичну вразливість зовнішніх енерговузлів АЕС та обґрунтовує необхідність включення ВРП до розрахункової моделі ризику R як об'єктів з високим рівнем наслідків C (див. Розділ 3.2).

Д.4. Кейс №4: Ешелонована система візуального та акустичного моніторингу

Приклад практичної реалізації запропонованого у дисертації підходу до використання альтернативних сенсорів.

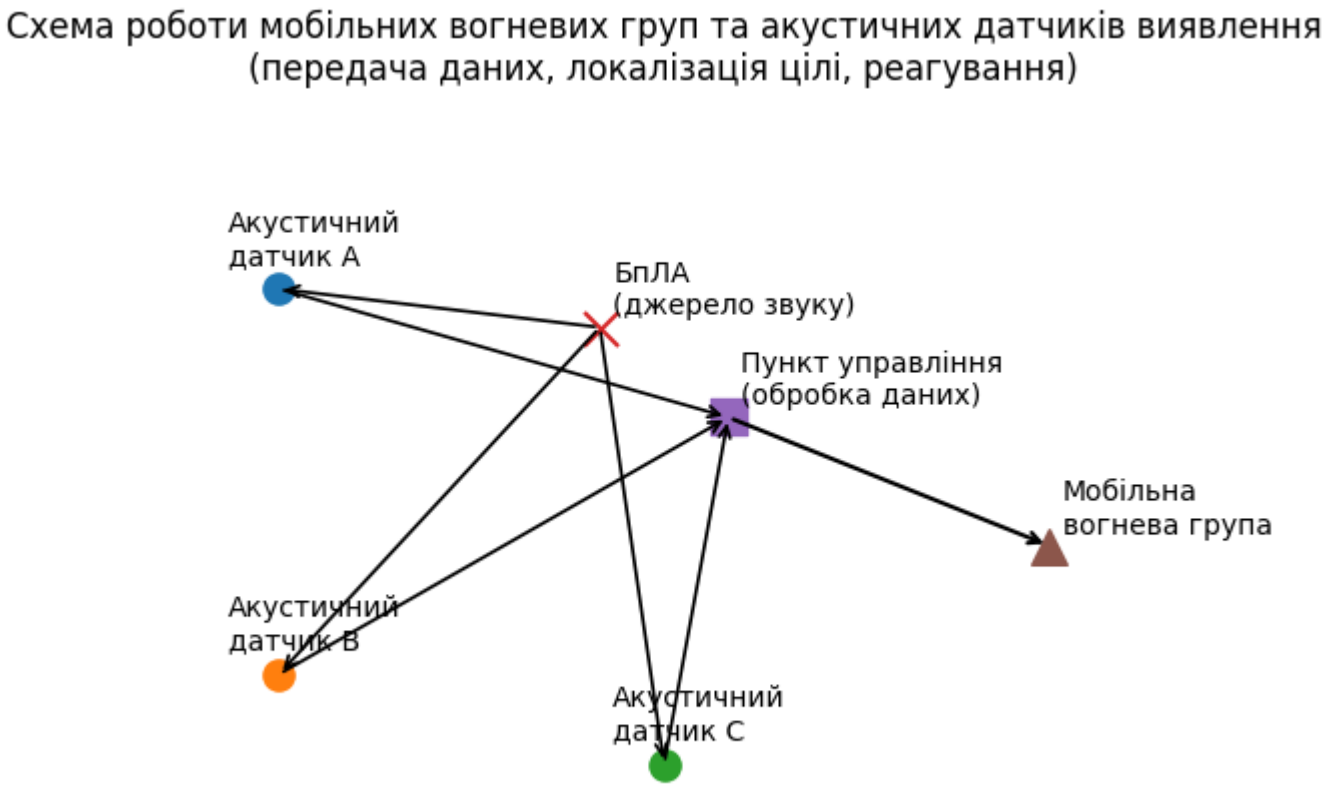

Рисунок Д.4 – Схема роботи мобільних вогневих груп та акустичних датчиків виявлення

Демонстрація того, як недорогі сенсори (мікрофони, прожектори) компенсують "сліпі зони" дорогих РЛС. Це візуалізує змінну N (кількість сенсорів) у формулі ймовірності виявлення з Додатка Г.