УДК 614.8:351.862

МІЖНАРОДНИЙ ДОСВІД ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА МОЖЛИВОСТІ ЙОГО АДАПТАЦІЇ

Рудешко Ірина Вікторівна,
старший викладач
Халепа Юліана Володимирівна,
Романюк Владислав Васильович
Студенти
Національний університет цивільного захисту України,
м. Черкаси, Україна
rudeshko_iryna@nuczu.edu.ua
khalepa.iuliana_2022b@nuczu.edu.ua
Romaniuk.Vladyslav_2022@chipb.org.in

Анатація. У статті здійснено комплексний аналіз міжнародного досвіду забезпечення захисту критичної інфраструктури в умовах зростання сучасних загроз, зокрема терористичних актів, кіберінцидентів, техногенних аварій та наслідків воєнних конфліктів. Досліджено підходи провідних держав світу до формування системи захисту об’єктів критичної інфраструктури, зокрема у країнах Європейського Союзу, США та інших розвинених державах, із акцентом на нормативно-правове регулювання, організаційні механізми управління, міжвідомчу координацію та впровадження сучасних технологій безпеки.

Особливу увагу приділено аналізу принципів стійкості, безперервності функціонування та відновлюваності критичної інфраструктури, а також ролі державних органів, приватного сектору та міжнародного співробітництва у забезпеченні належного рівня її захисту.

На основі узагальнення міжнародного досвіду визначено ключові напрями його адаптації до умов України, з урахуванням сучасних безпекових

викликів, зокрема в умовах воєнного стану. Обґрунтовано необхідність удосконалення національної системи захисту критичної інфраструктури шляхом гармонізації законодавства з міжнародними стандартами, підвищення ефективності діяльності органів державної влади, розвитку державно-приватного партнерства та впровадження інноваційних технологій захисту.
Ключові слова: критична інфраструктура, міжнародний досвід, захист, стійкість, безпека, ризики, державне управління, адаптація, ДСНС, воєнний стан.

Критична інфраструктура є основою функціонування держави, забезпечуючи життєво важливі потреби населення, економіки та національної безпеки. До неї належать об’єкти енергетики, транспорту, водопостачання, зв’язку, охорони здоров’я та інші системи, від яких залежить стабільність суспільства.

В умовах сучасних викликів, зокрема збройної агресії проти України, суттєво зростає рівень загроз для об’єктів критичної інфраструктури. Систематичні атаки на енергетичні об’єкти, використання безпілотних літальних апаратів, кібернапади та диверсії підтверджують необхідність вдосконалення системи їх захисту.

Одним із ефективних шляхів вирішення цієї проблеми є впровадження передового міжнародного досвіду, адаптованого до національних умов.

Питання захисту критичної інфраструктури розглядаються у працях зарубіжних та вітчизняних науковців, а також у міжнародних нормативних документах. У країнах Європейського Союзу ключовим документом є Директива (EU) 2022/2557, яка встановлює вимоги до забезпечення стійкості критичних суб’єктів [1, с. 5].

У США система захисту ОКІ базується на стратегічних документах Агентства з кібербезпеки та безпеки інфраструктури (CISA), що визначають основні напрями розвитку безпеки інфраструктури [2, с. 7].

В Україні правові засади функціонування системи захисту критичної інфраструктури визначені Законом України «Про критичну інфраструктуру» [5, с. 3], однак практична реалізація потребує подальшого вдосконалення.

Метою статті є поглиблений аналіз міжнародного досвіду захисту критичної інфраструктури та визначення ефективних шляхів його адаптації в Україні.

Сучасна концепція захисту критичної інфраструктури базується на понятті **стійкості (resilience)**, що передбачає здатність системи:

- протистояти загрозам;
- адаптуватися до змін;
- швидко відновлювати функціонування після пошкодження.

На відміну від традиційного підходу, який орієнтований переважно на фізичний захист, сучасні концепції передбачають комплексне поєднання:

- інженерного захисту;
- організаційних заходів;
- інформаційної безпеки;
- управління ризиками.

Такий підхід дозволяє підвищити загальну ефективність системи захисту [4, с. 6].

Європейський Союз реалізує комплексну політику у сфері захисту критичної інфраструктури, що охоплює всі ключові сектори економіки.

Основні елементи європейського підходу:

- ризик-орієнтоване управління – проведення регулярних оцінок загроз;
- секторальний підхід – визначення критичних галузей;
- міждержавна координація;
- обов’язковість звітності про інциденти.

Директива (EU) 2022/2557 встановлює вимоги до:

- визначення критичних суб’єктів;
- розробки планів безпеки;

- впровадження заходів захисту;
- проведення навчань [1, с. 8].

Особливу увагу приділено захисту від гібридних загроз, які поєднують фізичні та кібернетичні атаки.

У США система захисту критичної інфраструктури є однією з найбільш розвинених у світі. Вона базується на принципах:

- партнерства держави та бізнесу;
- децентралізованого управління;
- пріоритету кібербезпеки.

Ключові особливості:

- поділ інфраструктури на 16 секторів;
- створення центрів обміну інформацією (ISACs);
- застосування сучасних стандартів безпеки;
- активне використання аналітичних систем.

Важливою складовою є впровадження концепції **“zero trust”**, яка передбачає постійну перевірку доступу до систем [2, с. 11].

У таблиці 1 надано порівняльний аналіз світового досвіду щодо захисту о’єктів критичної інфраструктури.

Таблиця 1

Порівняльний аналіз міжнародного досвіду

Критерій	ЄС	США	Можливості для України
Основний підхід	Стійкість	Управління ризиками	Комбінований підхід
Організація	Централізована координація	Децентралізована система	Посилення координації
Кібербезпека	Інтегрована	Пріоритетна	Розвиток кіберзахисту
Партнерство	Обмежене	Розвинене	Розширення співпраці
Реагування	Координація на рівні ЄС	Секторальне управління	Вдосконалення взаємодії

На сьогодні для України характерні наступні загрози: ракетні та дронові удари, диверсії, кібернапади, техногенні аварії.

Особливістю є їх **комбінований характер**, що ускладнює захист і потребує комплексного підходу.

Адаптація міжнародного досвіду для України має проходити за наступними напрямками:

Нормативно-правове забезпечення

- гармонізація законодавства з нормами ЄС;
- впровадження стандартів оцінки ризиків;
- визначення відповідальності суб'єктів.

Інженерний захист

- укріплення будівель;
- створення захисних споруд;
- використання бар'єрних систем;
- впровадження систем протидії БпЛА.

Кібербезпека

- захист автоматизованих систем управління;
- створення центрів моніторингу;
- впровадження сучасних стандартів безпеки.

Організаційні заходи

- розвиток міжвідомчої взаємодії;
- проведення навчань;
- створення систем реагування.

Роль ДСНС України

ДСНС є ключовим елементом системи захисту ОКІ та виконує такі функції:

- реагування на надзвичайні ситуації;
- проведення рятувальних робіт;
- оцінка наслідків ураження;
- участь у плануванні заходів захисту.

Висновки. Міжнародний досвід свідчить, що ефективний захист критичної інфраструктури можливий лише за умов комплексного підходу, який включає інженерні, організаційні та інформаційні заходи. Для України важливим є впровадження ризик-орієнтованої моделі, розвиток міжвідомчої взаємодії та адаптація європейських стандартів. Особливу роль у цьому процесі відіграє ДСНС України. Адаптація міжнародного досвіду дозволить підвищити стійкість критичної інфраструктури та забезпечити національну безпеку.

Список літератури

1. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. – Brussels, 2022. – 45 p.
2. Cybersecurity and Infrastructure Security Agency (CISA). CISA Strategic Plan 2025–2026. – Washington, 2024. – 30 p.
3. Council of the European Union. Critical Infrastructure Blueprint. – Brussels, 2024. – 12 p.
4. European Commission. Critical Infrastructure Resilience in the EU. – Brussels, 2023. – 20 p.
5. Закон України «Про критичну інфраструктуру». – Київ, 2021. – 18 с.