УДК 624.01

Аналіз засобів захисту критичної інфраструктури під час агресії з боку РФ

Ліла Є.І., НУЗЦ України
НК – Афанасенко К.А., к.т.н., доцент, НУЦЗ України

Критична інфраструктура є невід'ємною складовою національної безпеки України, оскільки забезпечує життєво важливі функції держави, зокрема енергопостачання, транспорт, зв'язок, водопостачання тощо. В умовах агресії з боку РФ особливу актуальність набули загрози з боку ракетних ударів, безпілотних літальних апаратів (БПЛА), балістичних ракет та інших засобів ведення війни. Це вимагає розробки та реалізації ефективних інженерних заходів захисту, визначених у постанові Кабінету міністрів України від 4 серпня 2023 р. № 818 «Розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури»

Актуальність і важливість цієї теми є надзвичайно високою в сучасних умовах, оскільки критична інфраструктура, що включає енергетичні, транспортні, комунікаційні та інші стратегічні об'єкти, є основою функціонування держави. Її уразливість у разі нападів, техногенних чи природних катастроф може мати катастрофічні наслідки для національної безпеки та економічної стабільності країни. Особливо це стосується України, де критична інфраструктура перебуває під постійною загрозою з боку агресії РФ, включаючи ракетні удари, БПЛА, диверсії та кіберзагрози. Водночас актуальність цього питання визначається не лише зовнішніми ризиками, а й внутрішніми викликами, такими як нестабільність енергетичних мереж, потреба у зміцненні кіберзахисту та адаптація до технологічних змін. У цьому контексті захист критичної інфраструктури — це не лише охорона фізичних об'єктів, а й створення стійкої та інтегрованої системи, що забезпечить безперервне функціонування найважливіших галузей, попри можливі атаки чи інші зовнішні впливи.

Таким чином, існує необхідність аналізу можливості створення та використання захисту населення та інженерних споруд від обстрілів.

До фізичного захисту належить:

1. Укріплення будівель та споруд за допомогою спеціальних інженерних конструкцій, посилених залізобетоном, металевими екранами та енерго-поглинаючими матеріалами.
2. Захист від авіаційних та ракетних ударів шляхом створення підземних сховищ, маскування об'єктів, розсіювання критичних елементів інфраструктури.
3. Периметрова безпека, що включає встановлення контрольно-пропускних пунктів, інтелектуальних систем моніторингу території, датчиків руху та протидронових сіток.
4. Протипожежні заходи, що передбачають автоматизовані системи пожежогасіння, використання негорючих матеріалів та сенсорних систем контролю температури.

Протидія повітряним загрозам включає в себе (рис. 1):

1. Системи протиповітряної оборони, зокрема мобільні зенітно-ракетні комплекси, ракетно-артилерійські системи малої та середньої дальності.
2. Радіолокаційні системи раннього попередження для моніторингу повітряного простору та виявлення загроз.
3. Протиповітряні пастки та хибні цілі, що знижують ймовірність влучання ракет по реальних об'єктах критичної інфраструктури.

Технологічні засоби включають (рис. 1):

1. Резервні джерела енергопостачання, зокрема автономні електростанції, системи генерації енергії на основі відновлюваних джерел.
2. Автоматизовані системи керування, що зменшують залежність від людського фактора у кризових ситуаціях.

3. Системи моніторингу та аналізу загроз із використанням штучного інтелекту для прогнозування атак.

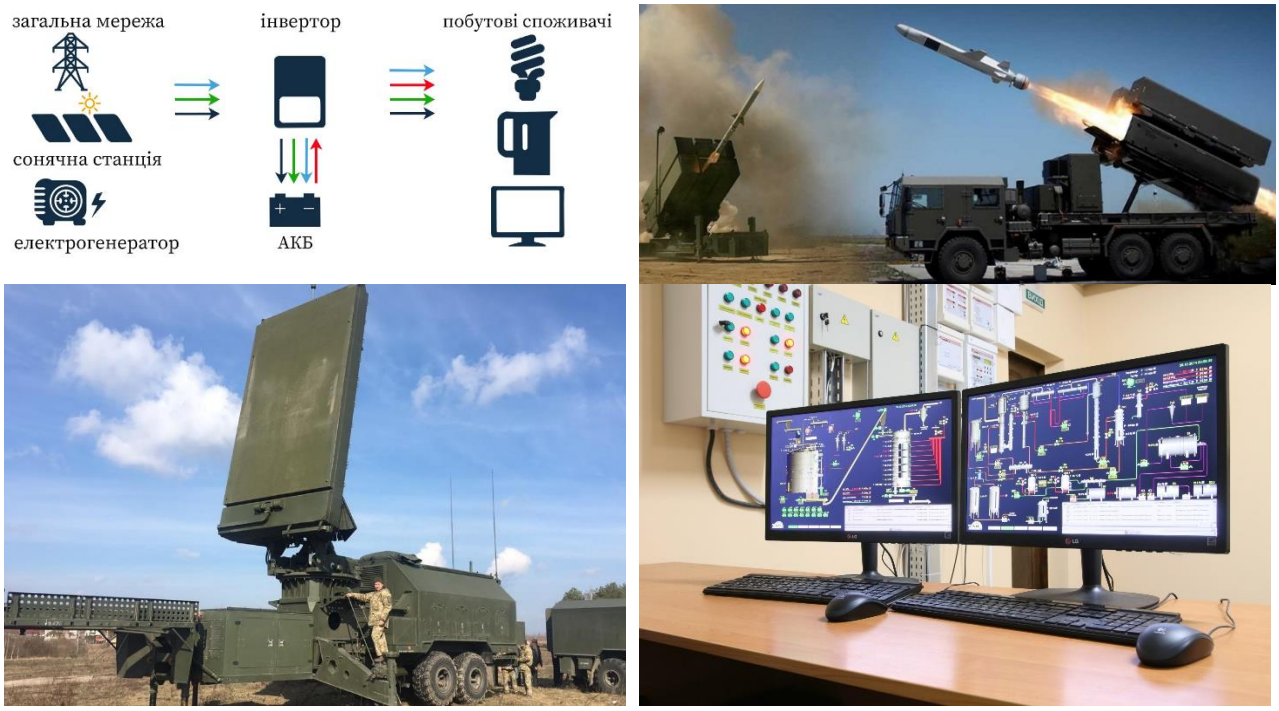

Рисунок 1. Засоби захисту критичної інфраструктури

Успішні міжнародні рішення:

1. **Ізраїль**: Система "Залізний купол" ефективно захищає країну від ракетних атак, забезпечуючи високу ймовірність перехоплення загроз. Крім того, активно використовуються підземні сховища для персоналу та критичних енергетичних об'єктів.
2. **США**: Велика увага приділяється кібербезпеці, включаючи багаторівневі системи захисту енергетичних мереж. У сфері фізичного захисту використовуються високотехнологічні датчики для моніторингу та раннього виявлення загроз.
3. **Німеччина та Франція**: Розвиток підземної інфраструктури та інвестиції у створення альтернативних джерел енергії дозволяють забезпечити безперебійну роботу об'єктів навіть у разі атак.

Порівняння з Україною: Україна активно впроваджує заходи захисту критичної інфраструктури, проте має обмежений ресурсний потенціал у порівнянні з розвиненими країнами. Значні виклики пов’язані з необхідністю модернізації систем ППО та кіберзахисту. Завдяки міжнародній підтримці та впровадженню передових рішень ситуація поступово покращується.

Для забезпечення захисту необхідно:

- Продовжувати розвиток та модернізацію систем ППО.
- Інвестувати в заходи кібербезпеки та захист інформаційних систем.
- Використовувати міжнародний досвід для створення ефективних систем моніторингу та реагування.
- Впроваджувати автономні енергетичні системи та альтернативні джерела енергії.

Висновки: Інженерний захист критичної інфраструктури України має базуватися на комплексному підході, що охоплює фізичну безпеку, протиповітряний захист, кібербезпеку та технологічні рішення. Впровадження передових технологій, зокрема автоматизованих систем управління та засобів кіберзахисту, є критично важливим для забезпечення стійкості держави. Досвід інших країн демонструє ефективність інтегрованих систем оборони, які слід адаптувати до українських реалій.