

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

За сучасних геополітичних умов захист об'єктів критичної інфраструктури (ОКІ) набуває вирішального значення. Гібридні загрози, які об'єднують у собі кібератаки, фізичні диверсії, інформаційно-психологічні операції та економічний тиск, створюють серйозні ризики для ключових секторів, таких як енергетика, водопостачання, транспорт та телекомунікації [1]. Звичайні методи безпеки, орієнтовані на окремі типи загроз, сьогодні є недостатніми. Це зумовлює необхідність переходу до інтегрованого підходу, заснованого на концепції стійкості систем [4].

Метою дослідження є аналіз сучасних підходів до забезпечення безпеки об'єктів критичної інфраструктури та визначення найефективніших стратегій протидії гібридним викликам.

Основні аспекти захисту:

1. Кібер-фізична конвергенція: Сучасні об'єкти критичної інфраструктури дедалі більше залежать від цифрових систем, таких як SCADA. Гібридні атаки часто розпочинаються із кіберпроникнення з метою дезорганізації керування, а потім переходять до фізичного впливу. Захист має бути багаторівневим: поєднання кібербезпеки (зокрема, антивірусних систем) із фізичним зміцненням об'єктів є ключовим фактором стійкості.

2. Моніторинг із використанням штучного інтелекту: Штучний інтелект дозволяє реально часу аналізувати потенційні ризики та виявляти аномалії в роботі систем. Інтелектуальні сенсори здатні фіксувати незвичні коливання в енергомережах або порушення каналів зв'язку ще до виникнення аварійних ситуацій. Впровадження прогностичної аналітики дає змогу моделювати сценарії ймовірних атак і заздалегідь готувати контрзаходи. Прогностичні моделі AI допомагають виявляти приховані зв'язки між дрібними інцидентами, які можуть бути частиною підготовки до масштабної атаки.

3. Стійкість (Resilience) як пріоритетна стратегія: Повна запобіжна протидія загрозам неможлива, тому основна увага приділяється здатності системи швидко відновлюватися після збоїв. Для цього важливо створювати резервні потужності, децентралізувати енергетичні та комунікаційні системи, а також розробляти протоколи оперативного реагування. Це включає впровадження мобільних генеруючих потужностей та автономних вузлів зв'язку. [2].

4. Державно-приватне партнерство: Більшість об'єктів критичної інфраструктури знаходиться у приватній власності, однак їхній вихід із ладу може загрожувати національній безпеці. Тому лише постійний обмін інформацією про можливі загрози між державними структурами і приватними підприємствами забезпечить дієву систему захисту. Важливим елементом є створення спільних центрів аналізу загроз та координації дій у кризових ситуаціях [3].

5. Нормативно-правове регулювання та стандартизація: Ефективний захист неможливий без чіткої законодавчої бази, що визначає критерії віднесення об'єктів до критичних та встановлює вимоги до їх безпеки [2]. Це включає імплементацію міжнародних стандартів захисту інформації та фізичної безпеки, адаптованих до умов гібридної війни [1].

Отже, для ефективного захисту критичної інфраструктури в умовах гібридної війни необхідний перехід від реактивного підходу до проактивного управління ризиками. Важливим є впровадження інтелектуальних моніторингових систем та удосконалення нормативно-правової бази. Це вимагає створення єдиного координаційного центру, який би об'єднував зусилля військових, кіберфахівців та приватних операторів інфраструктури. Тільки системний та багаторівневий контроль забезпечить стабільну роботу ключових об'єктів інфраструктури, підтримуючи безпеку держави та громадян у кризових ситуаціях.

Список літератури

1. **Про** критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20> (дата звернення: 02.04.2026).
2. **Про** затвердження Порядку визначення об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р. № 944.
3. **Горбулін В. П.** Як перемогти Росію у війні майбутнього. Київ : **Брайт Букс**, 2020. 256 с.
4. **Магда Є. В.** Гібридна війна: вижити і перемогти. Харків : **Віват**, 2015. 304 с.