УДК 351.86:004.056

КОМПЛЕКСНИЙ ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КОМБІНОВАНИХ АТАК (ФІЗИЧНИХ І КІБЕРНЕТИЧНИХ)

Рудешко Ірина Вікторівна,
старший викладач
Хусаінов Олексій Васильович
Студент
Національний університет цивільного захисту України,
м. Черкаси, Україна
rudeshko_iryna@nuczu.edu.ua
khusainov.oleksii_2022b@nuczu.edu.ua

Анотація. У статті досліджено теоретичні та практичні аспекти забезпечення комплексного захисту об'єктів критичної інфраструктури (ОКІ) від комбінованих атак, що поєднують фізичні та кібернетичні впливи. Проаналізовано сучасні загрози, особливості кіберфізичних атак, їх наслідки для функціонування державних систем. Розглянуто принципи побудови інтегрованої системи захисту, а також визначено ключові напрями вдосконалення безпеки ОКІ в умовах воєнного стану.

Ключові слова: критична інфраструктура, кібербезпека, кіберфізичні атаки, комбіновані загрози, захист інформації, національна безпека.

Вступ. Критична інфраструктура є основою функціонування держави, економіки та суспільства. Порушення її роботи може призвести до значних соціальних, економічних та екологічних наслідків. У сучасних умовах особливу загрозу становлять **комбіновані атаки**, які поєднують фізичні руйнування з кібернетичними впливами.

Зростання рівня цифровізації ОКІ призводить до підвищення вразливості до кіберзагроз. Як зазначають дослідники, сучасні атаки дедалі частіше мають

комплексний характер і спрямовані на досягнення максимального деструктивного ефекту [5, с. 12].

Особливо актуальною ця проблема є для України в умовах воєнного стану, коли об’єкти критичної інфраструктури стають пріоритетними цілями противника [4, с. 45].

Мета дослідження. Метою статті є комплексний аналіз загроз об’єктам критичної інфраструктури в умовах комбінованих (кіберфізичних) атак та обґрунтування ефективних підходів до побудови інтегрованої системи їх захисту.

Матеріали і методи. У процесі дослідження використано сукупність загальнонаукових і спеціальних методів, що забезпечили досягнення поставленої мети.

До основних методів належать:

- **аналіз і синтез** – для узагальнення наукових підходів до захисту критичної інфраструктури та формування цілісного уявлення про комбіновані загрози;
- **системний підхід** – для розгляду об’єктів критичної інфраструктури як складних кіберфізичних систем;
- **порівняльний аналіз** – для дослідження міжнародного досвіду захисту ОКІ [7, с. 8];
- **метод класифікації** – для систематизації загроз (фізичних, кібернетичних та комбінованих);
- **метод моделювання** – для формування узагальненої моделі комплексного захисту;
- **експертний аналіз** – для оцінювання ефективності запропонованих заходів.

Матеріалами дослідження є:

- наукові публікації з питань кібербезпеки та захисту критичної інфраструктури;
- нормативно-правові акти України у сфері національної безпеки;

- аналітичні звіти щодо кіберзагроз та кіберінцидентів.

Застосування зазначених методів дозволило комплексно дослідити проблему та сформувати практичні рекомендації щодо підвищення рівня захисту ОКІ.

Результати та обговорення. У результаті проведеного дослідження встановлено, що сучасні загрози об’єктам критичної інфраструктури мають комплексний характер і поєднують фізичні та кібернетичні компоненти. Це зумовлює необхідність переходу від фрагментарного до інтегрованого підходу в забезпеченні безпеки.

Виявлено, що комбіновані атаки створюють значно більший деструктивний ефект порівняно з окремими видами впливу, оскільки реалізується так званий синергетичний ефект [5, с. 14]. Зокрема, одночасне втручання в інформаційні системи управління та фізичне пошкодження об’єкта призводить до втрати контролю над технологічними процесами.

Проведений аналіз дозволив визначити ключові вразливості ОКІ:

- недостатній рівень інтеграції фізичного та кіберзахисту;
- застарілі системи управління;
- відсутність належного моніторингу загроз;
- недостатня підготовка персоналу [2, с. 28].

На основі узагальнення отриманих результатів обґрунтовано доцільність впровадження комплексної системи захисту, яка включає:

1. **Інтеграцію фізичних та кібернетичних систем безпеки**, що дозволяє забезпечити оперативне реагування на комбіновані атаки.
2. **Багаторівневу систему захисту**, яка передбачає наявність декількох рубежів безпеки.
3. **Розвиток систем моніторингу та прогнозування загроз**, що дає змогу виявляти атаки на ранніх етапах.
4. **Підвищення кваліфікації персоналу**, що є критично важливим фактором ефективного реагування.

Особливу увагу приділено умовам воєнного стану, які суттєво ускладнюють функціонування ОКІ. Встановлено, що в таких умовах пріоритетними є:

- резервування критичних систем;
- забезпечення автономності функціонування;
- швидке відновлення після атак [4, с. 50].

Обговорення результатів показало, що ефективний захист можливий лише за умови поєднання організаційних, інженерних та кібербезпекових заходів. При цьому важливу роль відіграє державна політика у сфері захисту критичної інфраструктури та міжнародне співробітництво.

Таким чином, результати дослідження підтверджують необхідність переходу до проактивної моделі безпеки, що базується на управлінні ризиками та постійному вдосконаленні систем захисту.

Висновки. У результаті проведеного дослідження встановлено, що сучасні об’єкти критичної інфраструктури функціонують як складні кіберфізичні системи, вразливі до багатовекторних впливів. Найбільшу небезпеку становлять комбіновані атаки, які поєднують фізичне ураження об’єктів із кібернетичним втручанням у системи управління, що призводить до значного підсилення негативних наслідків та ускладнює процес реагування [5, с. 14].

Доведено, що традиційні підходи до захисту, які передбачають роздільне функціонування фізичних та інформаційних систем безпеки, є недостатньо ефективними в умовах сучасних загроз. Необхідним є впровадження інтегрованої моделі захисту, що забезпечує узгоджене функціонування всіх складових безпеки.

У ході дослідження визначено, що ключовими загрозами для ОКІ є:

- фізичні руйнування об’єктів інфраструктури;
- кібернетичні атаки на інформаційні системи;
- комбіновані кіберфізичні впливи, які мають синергетичний характер [7, с. 5].

Встановлено, що найбільш ефективною є багаторівнева система захисту, яка включає організаційні, інженерно-технічні, кібербезпекові та інформаційно-аналітичні заходи. Такий підхід дозволяє мінімізувати ризики, своєчасно виявляти загрози та забезпечувати швидке реагування на інциденти.

Особливу увагу приділено умовам воєнного стану, в яких функціонування критичної інфраструктури супроводжується підвищеним рівнем небезпеки. Визначено, що в таких умовах пріоритетними напрямами захисту є:

- резервування критичних систем і ресурсів;
- створення автономних джерел функціонування;
- підвищення стійкості до зовнішніх впливів;
- забезпечення швидкого відновлення після атак [4, с. 50].

У процесі дослідження доведено, що важливим елементом забезпечення безпеки є впровадження сучасних технологій, зокрема:

- систем моніторингу та виявлення загроз;
- технологій штучного інтелекту для аналізу кіберінцидентів;
- засобів криптографічного захисту інформації;
- автоматизованих систем управління безпекою.

Окремо встановлено, що значну роль у забезпеченні захисту ОКІ відіграє людський фактор. Недостатній рівень підготовки персоналу може суттєво знизити ефективність навіть найсучасніших систем безпеки [6, с. 18]. У зв’язку з цим необхідним є постійне навчання та підвищення кваліфікації фахівців.

Також підтверджено, що ефективний захист критичної інфраструктури неможливий без належного нормативно-правового забезпечення та міжнародного співробітництва. Використання кращих світових практик дозволяє підвищити рівень стійкості національної інфраструктури до сучасних загроз.

Узагальнюючи результати дослідження, можна сформулювати такі практичні рекомендації:

1. Впровадження інтегрованих систем захисту ОКІ.

2. Розвиток національної системи кібербезпеки.
3. Підвищення рівня підготовки персоналу.
4. Використання сучасних технологій аналізу загроз.
5. Розширення міжнародного співробітництва.

Таким чином, комплексний захист об’єктів критичної інфраструктури є одним із ключових чинників забезпечення національної безпеки держави. Його ефективність визначається здатністю системи безпеки адаптуватися до нових викликів, протидіяти комбінованим атакам та забезпечувати безперервність функціонування критично важливих об’єктів.

Перспективами подальших досліджень є розробка інтелектуальних систем управління безпекою, удосконалення методів прогнозування загроз та впровадження інноваційних технологій захисту ОКІ.

Список літератури

1. Делембовський М. В., Ткаченко В. О., Мельник Д. І. Захист критичної інфраструктури України від кібератак. *Grail of Science*. 2024. № 32. С. 12–18.
2. Мурасов Р. К., Фараон С. І., Гук О. М. Кібербезпека критичної інфраструктури: оцінювання та управління ризиками кібератак. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2025. № 1 (43). С. 30–37.
3. Давидюк А. В. Кіберзахист та кібероборона критичної інфраструктури. У: *Матеріали міжнародної науково-практичної конференції*. Київ, 2022. С. 7–12.
4. Мануїлов Я. С. Забезпечення кібербезпеки об’єктів критичної інфраструктури в умовах кібервійни. *Інформація і право*. 2023. № 3 (46). С. 45–53.
5. Ільєнко А. О., Телющенко В. М., Дубчак О. В. Сучасні кіберзагрози критичної інфраструктури України та світу. *Кібербезпека: освіта, наука, техніка*. 2023. № 2 (18). С. 10–17.

6. Комісарова Н. О., Крутіков П. Д. Система кіберзахисту об’єктів критичної інфраструктури в умовах війни. *Науковий вісник*. 2024. № 1. С. 12–19.
7. Гончук А. А. Кіберзагрози та захист критичної інфраструктури: зарубіжний досвід. Харків: ХНУВС, 2025. 24 с.
8. Філліппова В. В., Гаврись А. П., Камрацька О. І. Комплексний захист об’єктів критичної інфраструктури України в умовах військового конфлікту. Львів: ЛДУ БЖД, 2025. 36 с.
9 Рудешко І.В., Халепа Ю.В., Романюк В.В. Міжнародний досвід захисту критичної інфраструктури та можливості його адаптації. *INNOVATIONS OF MODERN SCIENCE AND EDUCATION:* матеріали Міжнар. наук.-практ. конф., м. Ванкувер, 23-24 квітня. 2026 р. Канада, 2016.