Костянтин СПОРИШЕВ,
доктор наук з державного управління, доцент,
заступник начальника інституту підготовки
керівних кадрів з наукової роботи
Національної академії
Національної гвардії України,
м. Харків, Україна
ORCID: https://orcid.org/0000-0003-4737-9698
e-mail: spor_kos@ukr.net

Євген КАЗАНЦЕВ,
ад'юнкт докторантури та ад'юнктури
Національної академії
Національної гвардії України,
м. Харків, Україна
ORCID: https://orcid.org/0009-0001-2199-0563
e-mail: kazanzevyvgen@gmail.com

DOI: https://doi.org/10.32620/pls.2025.8.74

ПІДХОДИ ДО ВІДНОВЛЕННЯ ЕЛЕМЕНТІВ СИСТЕМИ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ПОСТКОНФЛІКТНИЙ ПЕРІОД

Анотація: *Досліджено сучасні підходи до відновлення системи захисту об'єктів критичної інфраструктури України у постконфліктний період. Проаналізовано основні виклики, серед яких дефіцит ресурсів, кіберзагрози, фрагментарність управління та потреба в інтеграції сектору безпеки й оборони. Обґрунтовано принципи резильєнтності, цифрової інтеграції та випереджувального управління ризиками. Визначено ключову роль сил безпеки у відновленні, кіберзахисті, аналітичному супроводі та формуванні нової культури національної безпеки.*

Ключові слова: *державна безпека, критична інфраструктура, сили безпеки України, постконфліктний період.*

У сучасних умовах тривалої збройної агресії проти України питання відновлення та забезпечення надійного функціонування системи захисту об'єктів критичної інфраструктури набуває стратегічного значення. Знищення або виведення з ладу енергетичних, транспортних, інформаційно-комунікаційних, водогосподарських, оборонно-промислових і медичних об'єктів суттєво знижує рівень національної безпеки, ускладнює гуманітарну ситуацію, перешкоджає ефективному управлінню силами оборони та цивільним сектором. Постконфліктний період вимагає переходу від реактивної моделі реагування на загрози до проактивної – орієнтованої на стійкість, кіберзахист, технологічне переоснащення та комплексну інтеграцію систем раннього виявлення ризиків [1-5].

Україна має унікальний досвід протидії багатовимірним загрозам у сфері критичної інфраструктури – від масованих кібератак до ракетних і дронових ударів по енергетичних об'єктах [2, 3]. Тому розроблення підходів до відновлення та модернізації елементів системи її захисту є не лише внутрішньою потребою, а й внеском у формування європейської архітектури безпеки.

Постконфліктний етап характеризується високим рівнем деструкції енергетичних мереж, транспортних коридорів, логістичних вузлів, об'єктів водо- та теплопостачання. Порушено єдність управлінських і технічних ланцюгів, спостерігається фрагментарність у системі управління безпекою об'єктів критичної інфраструктури. Серед головних викликів:

- Дефіцит ресурсів і персоналу, особливо в галузях енергетики, зв'язку та логістики;
- Застарілість нормативно-правової бази, що не враховує реалії гібридних і високотехнологічних загроз;
- Нестача координації між цивільними та військовими структурами у питаннях моніторингу, обміну інформацією та реагування;
- Кібератаки на системи управління технологічними процесами (SCADA), що створюють ризик каскадних відмов;
- Низький рівень резервування та децентралізації управління, що робить об'єкти вразливими до комплексних атак;
- Недостатня інтеграція сектору безпеки й оборони у процеси відбудови критичної інфраструктури.

Концептуальні підходи до відновлення. Система відновлення елементів захисту критичної інфраструктури має базуватися на принципах резильєнтності (стійкості), інтероперабельності, цифрової інтеграції та випереджувального управління ризиками. Доцільно виділити три взаємопов'язані напрями [4, 5]:

1. Організаційно-управлінський – створення єдиного національного координаційного центру з відновлення об'єктів критичної інфраструктури, підпорядкованого Раді національної безпеки і оборони України. Його функції мають включати стратегічне планування, узгодження дій між силовими структурами, приватними операторами та міжнародними партнерами, а також формування державного реєстру стану елементів критичної інфраструктури.

2. Технологічно-аналітичний – розроблення інформаційно-аналітичних платформ моніторингу стану об'єктів критичної інфраструктури з використанням штучного інтелекту, супутникового спостереження, геоінформаційних систем, безпілотних технологій і блокчейн-рішень для фіксації інцидентів. Такі системи мають забезпечити швидке виявлення аномалій, прогнозування наслідків пошкоджень та оптимізацію рішень щодо відновлення.

3. Оборонно-безпековий – інтеграція військових інженерних і кіберпідрозділів у процеси оцінки технічного стану, розмінування, створення тимчасових енергетичних або логістичних рішень. У цьому контексті важливо розвивати спільні навчання та доктринальні підходи між Збройними Силами України, Національною гвардією, Службою безпеки України, Держспецзв'язку, ДСНС і Національною поліцією.

Сектор безпеки і оборони відіграє ключову роль у забезпеченні фізичного, кібернетичного й інформаційного захисту об'єктів критичної інфраструктури. Його функції у постконфліктний період можна згрупувати за такими напрямами [1]:

1. Інженерно-технічний захист – участь у будівництві та укріпленні елементів критичної інфраструктури (енергетичних підстанцій, вузлів зв'язку, транспортних об'єктів). Використання військових підрозділів інженерного профілю дозволяє скоротити строки відновлення, забезпечити захист робіт від диверсій.

2. Оперативно-аналітична діяльність – формування системи обміну даними між військовими та цивільними структурами. Використання розвідувальних та аналітичних ресурсів сектору оборони сприяє прогнозуванню потенційних атак на інфраструктуру та завчасному реагуванню.

3. Кіберзахист і протидія інформаційним загрозам — розбудова національної мережі кіберрезерву, спільне патрулювання цифрових просторів, підготовка фахівців з кібероборони. У співпраці з приватним ІТ-сектором доцільно створити кіберцентри при регіональних військових адміністраціях.

4. Забезпечення громадського порядку і протидія диверсіям – Національна поліція та Національна гвардія повинні забезпечити охорону критичних об'єктів, охорону гуманітарних і логістичних коридорів, а також участь у ліквідації наслідків надзвичайних ситуацій.

5. Міжнародна взаємодія — залучення досвіду НАТО, ЄС та партнерських країн щодо побудови національних систем захисту критичної інфраструктури, зокрема у сферах кібербезпеки, інцидент-менеджменту та стратегічних комунікацій.

Необхідним є оновлення Закону України «Про критичну інфраструктуру» з урахуванням досвіду воєнного періоду та постконфліктних умов [6]. Доцільно запровадити:

- стандарти оцінки рівня стійкості об'єктів;
- механізм спільного управління ризиками для державних і приватних операторів;
- процедури залучення сил оборони до тимчасового управління об'єктами у кризових ситуаціях;
- обов'язкову сертифікацію систем кіберзахисту;
- державні програми підтримки інноваційних рішень для безпеки ОКІ (зокрема технологій автономного енергозабезпечення, резервного зв'язку, моніторингу стану споруд).

Сучасні тенденції вказують на необхідність переходу до інтегрованих ситуаційних центрів на національному та регіональному рівнях, які функціонують у режимі реального часу, забезпечуючи обмін даними між силовими, енергетичними та комунальними структурами. Ключовим завданням таких центрів є виявлення вразливостей, оцінка ризиків та координація рішень щодо відновлення. Для цього потрібні спільні бази даних, захищені канали зв'язку та алгоритми автоматизованого аналізу ситуацій.

Значну роль у цьому процесі відіграє розвиток аналітичних спроможностей сектору безпеки – впровадження систем підтримки прийняття рішень, побудованих на основі машинного навчання, які дозволяють оперативно визначати пріоритети відновлення, прогнозувати наслідки пошкоджень та ефективно розподіляти ресурси [7].

Відновлення системи захисту критичної інфраструктури неможливе без професійної підготовки персоналу. Необхідно створити єдину програму безпеково-технічної освіти, що охоплює питання кібербезпеки, кризового менеджменту, інженерного захисту та аналізу ризиків. Важливо передбачити участь у таких програмах не лише фахівців державного сектору, а й представників приватних операторів критичних послуг.

Сектор безпеки і оборони може стати базою для формування мобільних груп реагування, що здійснюватимуть оцінку пошкоджень, оперативне відновлення зв'язку, електропостачання або логістичних маршрутів у надзвичайних умовах.

Майбутня модель системи захисту критичної інфраструктури України повинна бути:

• інтелектуальною (використання ШІ, IoT, великих даних);

• розподіленою (мінімізація залежності від централізованих вузлів);

• енергоавтономною (впровадження локальних джерел генерації);

• синхронізованою із системою національної безпеки;

• адаптивною до нових загроз, включно з кіберфізичними, радіоелектронними та інформаційно-психологічними впливами.

Відновлення системи захисту об'єктів критичної інфраструктури у постконфліктний період є комплексним завданням, що вимагає злагодженої взаємодії сектору безпеки і оборони, органів державного управління, науково-технічної спільноти та приватного бізнесу. Роль сектору безпеки полягає не лише у фізичному чи кіберзахисті, але й у стратегічному плануванні, аналітичному супроводі, технологічній модернізації та формуванні нової культури безпеки.

Інтеграція воєнного досвіду у систему цивільного захисту, побудова мережі стійких регіональних центрів управління, розвиток інноваційних технологій моніторингу та прогнозування ризиків – усе це є запорукою формування стійкої, сучасної та ефективної системи захисту критичної інфраструктури України, здатної забезпечити національну безпеку у довгостроковій перспективі.

Бібліографічні посилання

1. Bielai, S., & Lavrov, I. (2023). Theoretical Foundations of the Formation of the Protection System of Critical Infrastructure Facilities of Ukraine. Honor and Law, (2), 85. С. 5-11. DOI: https://doi.org/10.33405/2078-7480/2023/2/85/282518

2. Yefimenko, I., Sakovskyi, A., & Bilozorov, Y. (2023). Protection of Critical Infrastructure as a Component of Ukraine's National Security. Law Journal of the National Academy of Internal Affairs, 13(2). С. 74-85. DOI: https://doi.org/10.56215/naia-chasopis/2.2023.74

3. Georgescu, A. (2025). A Critical Infrastructure Protection Perspective on the Conflict in Ukraine: Recommendations for a Resilient Post-war Ukraine. In N. S. (Ed.), Ukraine's Journey to Recovery, Reform and Post-War Reconstruction (pp. 271-285). Springer. DOI: https://doi.org/10.1007/978-3-031-66434-2_19

4. "Resilience of Critical Infrastructures: Review and Analysis of Current Approaches." (2025). Finance of Ukraine, № 6, с. 83-100. URL: https://doi.org/10.33763/finukr2025.06.083.

5. Berezutskyi, V., & Tokhtamysh, T. (2024). Risks of critical infrastructures during war. Law & Innovation Society. DOI: https://doi.org/10.37772/2309-9275-2024-2(23)-5.

6. Закон України «Про критичну інфраструктуру та її захист». Відомості ВР, 2022, № 19. URL: https://ips.ligazakon.net/document/JI04668A?an=3 (дата звернення: 25.10.25).

7. Бєлай С.В., Споришев К.О. Системи підтримки прийняття рішень у державному управлінні силами безпеки України. Актуальні питання у сучасній науці. Державне управління. 2024. № 2 (20). С. 320–329.

K. Sporyshev, Y. Kazanzev

Approaches to restoration of elements of the critical infrastructure protection system in the post-conflict period.

Abstract: The article examines modern approaches to restoring Ukraine's critical infrastructure protection system in the post-conflict period. The main challenges are analyzed, including resource shortages, cyber threats, fragmented management, and the need for integration of the security and defense sector. The principles of resilience, digital integration, and proactive risk management are substantiated. The key role of security forces in recovery, cyber defense, analytical support, and the development of a new national security culture is emphasized.

Keywords: state security, critical infrastructure, security forces of Ukraine, post-conflict period.

Зразок для цитування:

Споришев К., Казанцев Є. Підходи до відновлення елементів системи захисту об'єктів критичної інфраструктури у постконфліктний період. Пропілеї права та безпеки, 2025. №8. С. 283-285. DOI: https://doi.org/10.32620/pls.2025.8.74.