

Вікторія МАСЛИК,

студентка кафедри менеджменту та бізнес-адміністрування
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: <https://orcid.org/0009-0007-6654-4149>

Науковий керівник: Наталія ФІЛІПЕНКО,

доктор юридичних наук, професор,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: <https://orcid.org/0000-0001-9469-3650>
e-mail: n.filipenko@khai.edu

DOI: <https://doi.org/10.32620/pls.2025.8.61>

МЕНЕДЖМЕНТ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК СКЛADOVA НАЦІОНАЛЬНОЇ СТІЙКОСТІ УКРАЇНИ

Анотація: у тезах досліджується роль менеджменту безпеки критичної інфраструктури (КІ) як ключового елементу забезпечення національної безпеки та стійкості України. Розглянуто сутність поняття критичної інфраструктури, її основні складові та значення для стабільного функціонування держави. Проаналізовано сучасні виклики, пов'язані з глобалізацією, цифровізацією та зростанням кількості гібридних і кіберзагроз, що безпосередньо впливають на енергетичну, транспортну, комунікаційну, фінансову та інші системи.

Особливу увагу приділено питанням інтеграції кібербезпеки у загальну систему менеджменту КІ, розвитку національних механізмів реагування на надзвичайні ситуації, міжвідомчій координації та міжнародному співробітництву у сфері захисту життєво важливих об'єктів. Наголошено на необхідності формування стійкої, адаптивної та технологічно розвиненої системи управління, здатної запобігати ризикам, оперативно реагувати на інциденти й забезпечувати швидке відновлення функціональності інфраструктури після кризових подій.

Зроблено висновок, що ефективний менеджмент безпеки критичної інфраструктури є запорукою національної стійкості, обороноздатності та сталого розвитку України в умовах зростання глобальних загроз.

Ключові слова: критична інфраструктура, національна безпека, менеджмент безпеки, кібербезпека, стійкість (resilience), управління ризиками, міжнародне співробітництво, національна стійкість, кризове реагування, сталий розвиток.

У сучасному світі питання забезпечення національної безпеки тісно пов'язане із стабільним функціонуванням критичної інфраструктури (далі – КІ). В умовах глобалізації, цифровізації та зростання кількості гібридних загроз саме критична інфраструктура стає основою життєздатності держави, адже її безперервна робота визначає стабільність економіки, соціальної сфери та обороноздатності країни. Будь-які порушення у функціонуванні енергетичних систем, транспорту, зв'язку чи фінансових установ можуть спричинити масштабні наслідки, що вплинуть на безпеку суспільства в цілому.

Менеджмент безпеки критичної інфраструктури передбачає комплекс організаційних, технічних, правових і стратегічних заходів, спрямованих на запобігання ризикам, своєчасне

реагування на загрози та забезпечення швидкого відновлення систем після кризових подій. Особливої актуальності це питання набуває для України, яка в умовах воєнних дій та посилення кіберзагроз змушена формувати ефективну політику захисту життєво важливих об'єктів. Отже, дослідження менеджменту безпеки критичної інфраструктури як складової національної стійкості є надзвичайно важливим, адже від його ефективності залежить не лише стабільність функціонування державних і приватних структур, а й здатність країни протистояти сучасним викликам та забезпечувати сталий розвиток у довгостроковій перспективі.

Насамперед, слід зазначити, що поняття "критична інфраструктура". Це система об'єктів і установ, що мають ключове значення для

стабільного функціонування суспільства та економіки держави. До неї входять підприємства продовольчої, транспортної, енергетичної, фінансової, хімічної, телекомунікаційної, інформаційно-технологічної, медичної сфер, а також комунальні служби [1]. Порушення роботи будь-якого з цих елементів може мати каскадний ефект, призводячи до серйозних соціальних, економічних та навіть політичних наслідків. Отже, забезпечення належного рівня захисту критичної інфраструктури є стратегічним завданням для кожної держави. Системний підхід до управління її безпекою дає змогу не лише мінімізувати ризики техногенних чи кібернетичних загроз, а й підвищити стійкість суспільства до кризових ситуацій. Ефективна координація між державними органами, приватним сектором та громадськістю сприяє створенню комплексної системи реагування, здатної швидко адаптуватися до нових викликів. Таким чином, розвиток та вдосконалення менеджменту безпеки критичної інфраструктури є необхідною умовою для підтримання національної безпеки та сталого розвитку країни.

Менеджмент безпеки КІ не обмежується лише фізичним захистом об'єктів. Він передбачає багатоаспектний підхід, що включає кібербезпеку, захист від природних катаклізмів, техногенних аварій та терористичних актів. З огляду на зростаючу кіберзагрозу, інтеграція кібербезпеки в загальну систему менеджменту КІ є критично важливою. За даними Світового економічного форуму, кібератаки на критичну інфраструктуру є одними з найнебезпечніших ризиків у глобальному масштабі [2]. Отже, сучасний підхід до менеджменту безпеки критичної інфраструктури має базуватися на принципах комплексності, превентивності та адаптивності. Лише поєднання технічних, організаційних і правових заходів дозволяє створити ефективну систему протидії загрозам будь-якого характеру. Важливим аспектом є також підготовка кваліфікованих фахівців, здатних оперативно реагувати на інциденти та впроваджувати сучасні технологічні рішення. Таким чином, інтеграція кібербезпеки в загальний менеджмент критичної інфраструктури забезпечує її стійкість, безперервність функціонування та захищеність держави в умовах зростаючих глобальних ризиків.

Національна система захисту критичної інфраструктури України є ключовим механізмом, що забезпечує стабільність та безпеку держави. Вона охоплює сукупність органів управління, сил і ресурсів центральних і місцевих органів виконавчої влади (а також військово-цивільних адміністрацій у разі їх створення), органів місцевого самоврядування та операторів критичної інфраструктури, які відповідають за розроблення й реалізацію державної політики у сфері захисту критичної інфраструктури. Це сприяє зміцненню стійкості критичної інфраструктури, що має надзвичайно важливе значення для стабільності та безпеки держави [3]. Отже,

підвищення стійкості критичної інфраструктури має стати одним із ключових напрямів державної політики у сфері національної безпеки. Реалізація цього підходу передбачає не лише запобігання інцидентам, а й створення ефективних механізмів управління ризиками та відновлення функціональності систем після кризових подій. Важливу роль у цьому процесі відіграє міжвідомча взаємодія, використання сучасних технологій моніторингу та прогнозування, а також міжнародне співробітництво у сфері безпеки КІ. Таким чином, формування стійкої та гнучкої системи управління критичною інфраструктурою є запорукою ефективного реагування на загрози та підтримання стабільності держави в умовах невизначеності.

Міжнародне співробітництво також відіграє ключову роль у менеджменті безпеки КІ. Оскільки багато загроз, таких як кібератаки або транскордонні терористичні акти, мають глобальний характер, співпраця з іншими країнами, обмін інформацією та досвідом є незамінними. Європейський Союз, наприклад, активно розробляє спільні стратегії та механізми захисту КІ своїх держав-членів, усвідомлюючи взаємозалежність національних інфраструктур [4]. Отже, розвиток міжнародного партнерства у сфері захисту критичної інфраструктури сприяє підвищенню глобальної безпеки та формуванню єдиного простору довіри між державами. Спільні ініціативи, стандарти та обмін найкращими практиками дозволяють більш ефективно протидіяти сучасним загрозам і забезпечувати стійкість життєво важливих систем. Участь України в міжнародних програмах та організаціях з безпеки КІ відкриває можливості для вдосконалення національної системи менеджменту, інтеграції у світові стандарти та зміцнення обороноздатності держави. Таким чином, міжнародна співпраця є не лише важливим чинником розвитку безпеки критичної інфраструктури, а й необхідною умовою забезпечення стабільності та сталого розвитку в глобальному вимірі. На завершення слід підкреслити, що менеджмент безпеки критичної інфраструктури є невід'ємною складовою національної стійкості та безпеки держави. В умовах постійного зростання кількості та складності загроз саме системний, інтегрований підхід до управління безпекою КІ забезпечує ефективне функціонування життєво важливих сфер суспільства. Поєднання технічних, організаційних, правових і міжнародних заходів дає змогу створити стійку, адаптивну та здатну до швидкого відновлення інфраструктуру. Розвиток національної системи менеджменту безпеки КІ повинен ґрунтуватися на сучасних технологіях, підготовці фахівців і тісній взаємодії між усіма суб'єктами безпеки. Таким чином, ефективне управління безпекою критичної інфраструктури є запорукою не лише стабільності держави, а й її спроможності успішно протистояти глобальним викликам та забезпечувати сталий розвиток у

майбутньому.

Висновок. Менеджмент безпеки критичної інфраструктури є ключовим чинником забезпечення національної безпеки, стійкості та розвитку держави. У сучасних умовах глобалізації, воєнних загроз і швидкого технологічного прогресу саме ефективне управління ризиками, своєчасне реагування на інциденти та здатність систем до відновлення визначають життєздатність країни. Україна, як держава, що перебуває у стані збройної агресії та кіберпротистояння, потребує комплексного, адаптивного підходу до захисту своїх життєво важливих об'єктів.

Розбудова національної системи менеджменту безпеки критичної інфраструктури має спиратися на інтеграцію кібербезпеки, правові та організаційні механізми, підготовку фахівців і міжнародну співпрацю. Такий підхід забезпечить не лише фізичну та інформаційну захищеність держави, а й підвищить її здатність до відновлення після кризових подій.

Отже, ефективне управління безпекою критичної інфраструктури є фундаментом національної стійкості, економічної стабільності та суспільного добробуту. Воно визначає не лише поточну безпеку країни, а й її спроможність розвиватися, зберігаючи незалежність і суверенітет у мінливому глобальному середовищі.

Бібліографічні посилання

1. Бронювання працівників критичної інфраструктури: зміни 2025 року | Школа бізнесу Нова Пошта. URL: <https://share.google/qXZQwgalgD3EJAiDH>
2. World Economic Forum. (2024). The Global Risks Report 2024.
3. Все, що ви повинні знати про об'єкти критичної інфраструктури в Україні. URL: <https://share.google/x0ZjlU9zAhiLzruXJ>
4. European Commission. (2022). Proposal for a Directive on the resilience of critical entities.

V. Maslyk

Critical infrastructure security management as a component of Ukraine's national resilience.

Abstract: The theses explore the role of critical infrastructure (CI) security management as a key element in ensuring Ukraine's national security and resilience. The concept of critical infrastructure, its main components, and its importance for the stable functioning of the state are examined. The study analyzes current challenges related to globalization, digitalization, and the growing number of hybrid and cyber threats that directly affect energy, transport, communication, financial, and other systems.

Particular attention is paid to the integration of cybersecurity into the overall CI management system, the development of national mechanisms for emergency response, interagency coordination, and international cooperation in protecting vital assets. The need to establish a resilient, adaptive, and technologically advanced management system capable of preventing risks, responding quickly to incidents, and ensuring the rapid recovery of infrastructure functionality after crises is emphasized.

It is concluded that effective critical infrastructure security management is a cornerstone of Ukraine's national resilience, defense capability, and sustainable development in the face of increasing global threats.

Keywords: critical infrastructure, national security, security management, cybersecurity, resilience, risk management, international cooperation, national resilience, crisis response, sustainable development.

Зразок для цитування:

Маслик В. Менеджмент безпеки критичної інфраструктури як складова національної стійкості України. Пропілеї права та безпеки, 2025. №8. С. 240-242. DOI: <https://doi.org/10.32620/pls.2025.8.61>.