УДК 351.86:338.49 (043.2)
DOI: https://doi.org/10.32782/2786-8141/2024-6-10

Саврацький О.О.
аспірант кафедри кібербезпеки,
Національний університет «Одеська юридична академія»
ORCID: https://orcid.org/0009-0005-3396-4855
Alexander Savratsky
National University "Odesa Law Academy"

АДАПТАЦІЯ СИСТЕМИ УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДО СУЧАСНИХ БЕЗПЕКОВИХ ВИКЛИКІВ

ADAPTING THE CRITICAL INFRASTRUCTURE MANAGEMENT SYSTEM TO MODERN SECURITY CHALLENGES

Анотація. *Адаптація систем управління об'єктами критичної інфраструктури до сучасних безпекових викликів виступає не тільки як ключовий елемент національної безпеки, але й як важлива умова для забезпечення сталого розвитку суспільства в умовах глобалізації та зростаючої технологічної залежності. Ця стаття пропонує глибокий аналіз актуальних проблем і викликів, пов'язаних з управлінням критичною інфраструктурою, а також розробляє комплексні стратегії адаптації до змінювального безпекового ландшафту. В статті ретельно розглядається вплив сучасних загроз на функціонування об'єктів критичної інфраструктури, включаючи кібератаки, які можуть призвести до значних перебоїв в роботі енергетичних систем, транспортної інфраструктури, засобів зв'язку та інших важливих компонентів. Автори аналізують останні дослідження та публікації, висвітлюючи розробку методологій управління інформаційною безпекою, принципи проєктування автоматизованих систем управління, методи управління проєктними ризиками та підходи до тестування на проникнення. Особлива увага приділяється необхідності інтеграції технологічних, організаційних та правових інструментів для підвищення ефективності, безпеки та стійкості систем управління. В контексті цього, обговорюється важливість міжвідомчої співпраці, а також роль місцевих громад та державних органів в управлінні безпекою критичної інфраструктури. Автори наголошують на значенні забезпечення відповідності до міжнародних стандартів та норм, а також на необхідності постійного оновлення нормативно-правової бази з урахуванням динаміки зовнішнього середовища. Успішна адаптація систем управління критичною інфраструктурою до сучасних безпекових викликів вимагає глобального підходу, який охоплює не тільки технологічні аспекти, але й організаційні, правові, та навчальні ініціативи. Важливо створити умови для ефективної взаємодії між різними учасниками процесу управління, включаючи приватний сектор, урядові структури, наукові круги та громадськість. Така інтеграція дозволить не лише підвищити загальний рівень безпеки об'єктів критичної інфраструктури, але й забезпечити їхню готовність до швидкої адаптації до нових викликів та загроз, забезпечуючи тим самим безперебійне надання основних послуг та збереження стабільності у суспільстві.*

Ключові слова: *системи управління, об'єкти критичної інфраструктури, кібербезпека, ризики, кіберзагрози.*

Abstract. *Adaptation of critical infrastructure management systems to modern security challenges is not only a key element of national security, but also an important condition for ensuring sustainable development of society in the context of globalization and growing technological dependence. This article offers an in-depth analysis of current issues and challenges related to critical infrastructure management, and develops comprehensive strategies for adapting to the changing security landscape. The article thoroughly examines the impact of modern threats on the functioning of critical infrastructure, including cyberattacks that could lead to significant disruptions in the operation of energy systems, transportation infrastructure, communications, and other critical components. The authors analyze the latest research and publications, covering the development of information security management methodologies, principles of designing automated control systems, methods of project risk management, and approaches to penetration testing. Particular attention is paid to the need to integrate technological, organizational, and legal tools to improve the efficiency, security, and sustainability of management systems. In this context, the importance of interagency cooperation is discussed, as well as the role of local communities and government agencies in managing critical infrastructure security. The authors emphasize the importance of ensuring compliance with international standards and norms, as well as the need to constantly update the regulatory framework to reflect the dynamics of the external environment. Successful adaptation of critical infrastructure management systems to modern security challenges requires a global approach that covers not only technological aspects but also organizational, legal, and training initiatives. It is important to create conditions for effective interaction between various stakeholders in the management process, including the private sector, government agencies, academia, and the public. Such integration will not only increase the overall level of security of critical infrastructure facilities, but also ensure their readiness to quickly adapt to new challenges and threats, thereby ensuring the uninterrupted provision of essential services and maintaining stability in society.*

Keywords: *control systems, critical infrastructure facilities, cybersecurity, risks, cyber threats.*

Постановка проблеми. В останні роки увага експертного співтовариства усе частіше концентрується на об'єктах критичної інфраструктури, які є основою сучасної економіки. Ці системи є дуже вразливими до різноманітних потрясінь – від кліматичних небезпек до промислових аварій, терористичних і кібератак. Порушення роботи критично важливих систем та основних послуг, таких як телекомунікації, енерго- та водопостачання, транспортні та фінансові системи, може призвести до розривів в їх роботі з жахливими наслідками у вигляді екологічних, економічних та соціальних втрат. Таким чином, оборона об'єктів критич-

ної інфраструктури від загроз і небезпек, обумовлює необхідність створення системи управління яка була б орієнтована на забезпечення їх захисту з залученням широкого кола контрагентів: від місцевих громад до органів державної влади. Важливою складовою такої системи, з огляду на вище зазначене, є взаємодія з публічними регуляторами для забезпечення відповідності стандартам безпеки та ефективності. Відтак управління об'єктами критичної інфраструктури вимагає постійного адаптування до нових умов та викликів для забезпечення сталого та безпечного функціонування суспільства.

Наразі, управління об'єктами критичної інфраструктури регламентується численними нормативно-правовими актами, але всі вони переважно носять відомчий характер. Тому, для подальшої її розбудови необхідним є опрацювання та впровадження низки правових, організаційних, технологічних та інших механізмів.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення економічної стабільності для критичної інфраструктури, а також управління ризиками з орієнтацією на безпеку на стратегічному та тактичному рівнях управління у складних умовах сучасного глобального середовища є предметом дослідження багатьох науковців та практиків. Зокрема, Мохор В., Цуркан В. серед іншого присвячують свої роботи розгляду методології побудови систем управління інформаційною безпекою. Ящук В.І. концентрує увагу на принципах проєктування автоматизованих інформаційних систем управління об'єктами критичної інфраструктури. Комаров М.Ю., Гончар С.Ф. розглядають методику побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури. Павук І.В., Кобилкін Д.С. в своїх роботах аналізують питання формування концепції управління проєктними ризиками на об'єктах критичної інфраструктури. Мельничук О. концентрується на питаннях управління критичною інфраструктурою, розглядаючи модель та її впровадження. Питання тестування на проникнення як ефективний інструмент менеджменту кібербезпеки, розглядають в своїх працях Горбаченко С.А., Бойко В.Д.

Поряд з достатнім наробком за даною тематикою дослідження проблема адаптації системи управління об'єктами критичної інфраструктури до сучасних безпекових викликів залишається недостатньо розробленою та потребує додаткових обґрунтувань.

Мета статті полягає у визначенні особливостей управління об'єктами критичної інфраструктури, з акцентом на виявленні ключових викликів та стратегій, які можуть бути застосовані для підвищення їх ефективності, безпеки та стійкості.

Виклад основного матеріалу. Як на глобальному рівні, так і в межах окремих країн об'єкти критичної інфраструктури є життєво важливими складовими суспільних процесів, зокрема, й у економічній сфері. На рівні національної економіки до критичної інфраструктури відносяться такі сфери як енергетика, водопостачання, транспорт, зв'язок, охорона здоров'я комунальне господарство тощо. Тобто ті сфери, порушення роботи яких може викликати серйозні соціальні та економічні наслідки [1; 2]. Об'єктами критичної інфраструктури можуть бути як державні, так і приватні установи.

Доцільно виокремити декілька ключових аспектів, що характеризують об'єкти критичної інфраструктури (табл. 1).

З огляду на перелічені характеристики можна стверджувати, що розуміння та забезпечення безпеки критичної інфраструктури є ключовим елементом стратегії національної безпеки багатьох країн. З початком повномасштабного вторгнення розроблення ефективних стратегій захисту об'єктів критичної інфраструктури постає одним із найважливіших аспектів національної безпеки України. Насамперед, мова йде про створення комплексних систем безпеки, включаючи фізичний захист, кібербезпеку, а також розробку планів реагування на надзвичайні ситуації [4].

Ефективне управління критичною інфраструктурою передбачає залучення та координацію різних зацікавлених сторін, включаючи урядові агенції, приватний сектор та громадянське суспільство. Це дозволяє створити більш гнучкі та адаптивні системи управління, що здатні ефективно реагувати на змінні умови та нові загрози. Адже в сучасних умовах, забезпечення стійкості та безперебійності діяльності об'єктів критичної інфраструктури є не лише питанням пошуку відповідних технічних рішень, але й вимагає комплексного підходу, включаючи законодавчу підтримку, наукові дослідження, управлінські інновації та міжнародну співпрацю. Цей процес охоплює необхідні зміни та вдосконалення в різних аспектах, щоб система ефективно відповідала новим викликам та загрозам. Процес адаптації може включати в себе:

Таблиця 1 – Основні характеристики об'єктів критичної інфраструктури

№	Характеристика	Опис
1	Забезпечення важливих функцій	Об'єкти критичної інфраструктури надають послуги, без яких суспільство не може ефективно функціонувати: електроенергія, водопостачання, охорона здоров'я тощо.
2	Ризик для національної безпеки	Пошкодження або зрив роботи об'єктів критичної інфраструктури може мати серйозні наслідки на макрорівні, наприклад зменшення обороноздатності країни.
3	Уразливість в кіберсередовищі	Об'єкти критичної інфраструктури потребують високого рівня захисту не тільки від фізичних, а й від кібератак. Це включає в себе розробку та впровадження передових технологій безпеки, регулярне тестування систем на вразливості та підготовку до відновлення після можливих інцидентів.
4	Регулювання та відповідальність	Держава часто встановлює спеціальні правила та норми для регулювання діяльності об'єктів критичної інфраструктури, забезпечуючи їх надійність та безперебійність.
5	Міжнародна співпраця	У сучасному глобалізованому світі безпека об'єктів критичної інфраструктури вимагає міжнародної координації та співпраці, особливо в сферах, де інфраструктура перетинає національні кордони.

Джерело: складено за даними [3]

Рисунок 1 – Компоненти системи адаптації процесу управління об'єктами критичної інфраструктури до нових викликів і загроз

Джерело: розроблено автором на основі [5]

Адаптація системи управління до сучасних безпекових викликів допомагатиме забезпечити надійний захист об'єктів критичної інфраструктури в умовах турбулентності та постійних трансформацій.

Не можна забезпечити цілеспрямоване функціонування індивідуальних елементів інфраструктури, ігноруючи ключові управлінські принципи такі як планомірність, адаптивність, кваліфікованість, відкритість, прозорість, зворотній зв'язок та особиста відповідальність [6]. Адже вони розповсюджуються на всю систему керування критичною інфраструктурою, яка, на рівні країни, може бути представлена через агрегацію універсальних компонентів, необхідних для її роботи.

Іншим важливим завданням менеджменту об'єктів критичної інфраструктури є ефективне управління ризиками. Задля цього можна застосовувати декілька ефективних стратегій (табл. 2).

Основна мета в системі управління критичною інфраструктурою полягає у забезпеченні безпеки через керування процесами, самими об'єктами та зв'язками між ними. Досягнення цієї мети відбувається через виконання низки завдань (табл. 3).

Окремим безпековим викликом з точки зору управління об'єктами критичної інфраструктури є їхній захист від кібератак. Забезпечення ефективного кіберзахисту потребує не тільки сучасних технологічних рішень, а й відповідної управлінської складової. Адже основним джерелом загроз все частіше виступає «людський чинник». В цьому сенсі вагоме значення набуває така управлінська категорія як менеджмент кібербезпеки [8, с. 25]. Так, захист від кібератак становить значущий безпековий виклик для управління об'єктами критичної інфраструктури. Кіберзагрози можуть включати атаки на інформаційні системи, мережі та комп'ютерні системи, що управляють ключовими інфраструктурними об'єктами. Ці атаки можуть мати серйозні наслідки, такі як порушення роботи об'єктів, втрата конфіденційної інформації, або навіть загроза життю і безпеці громадян. Для вирішення цього виклику системи управління об'єктами критичної інфраструктури повинно вживати ряд заходів, вони наведені на рис. 2.

1. Кібербезпекові заходи: розробка та впровадження ефективних заходів кібербезпеки, таких як захист від несанкціонованого доступу, виявлення та відповідь на інциденти.

2. Моніторинг та виявлення: постійний моніторинг кіберактивності та вчасне виявлення потенційно небезпечних ситуацій.

3. Планування реагування: розробка імовірних сценаріїв кібератак і планування ефективного реагування на них.

Таблиця 2 – Стратегії управління ризиками об'єктів критичної інфраструктури

№	Стратегія	Опис
1	Інновації	Менеджмент об'єктів критичної інфраструктури має інвестувати в інновації, щоб підвищити ефективність процесів та операцій і зменшити ризики.
2	Співпраця	Менеджмент об'єктів критичної інфраструктури повинен співпрацювати з іншими підприємствами, урядовими структурами та громадськістю, щоб обмінюватися інформацією та ресурсами. Наприклад, локальні підприємства можуть співпрацювати з урядовими структурами для розробки планів реагування на надзвичайні ситуації.
3	Глобальна координація	Менеджмент об'єктів критичної інфраструктури повинен співпрацювати з іншими країнами, щоб забезпечити стійкість глобальної інфраструктури. Наприклад, для розробки спільних стандартів безпеки та обміну інформацією про наявні та можливі кібератаки.

Джерело: складено за даними [5]

Таблиця 3 – Основні завдання щодо забезпечення безпеки критичної інфраструктури

№	Завдання	Опис
1	Ідентифікація об’єктів критичної інфраструктури	Включає в себе визначення об'єктів, які відповідають заздалегідь узгодженим критеріям критичності.
2	Забезпечення захисту та стійкості об'єктів	Вимагає зусиль, ресурсів та уваги від усіх учасників управлінського процесу і включає різноманітні заходи для створення та впровадження планів захисту та стратегій розвитку кожного конкретного об’єкту.
3	Ефективність, перегляд та актуалізація стратегій розвитку об’єктів критичної інфраструктури на основі моніторингу	Передбачає заходи моніторингу системи управління та коригування планів захисту та розвитку об'єктів з урахуванням реальних змін у внутрішньому та зовнішньому середовищі.

Джерело: складено за даними [7]

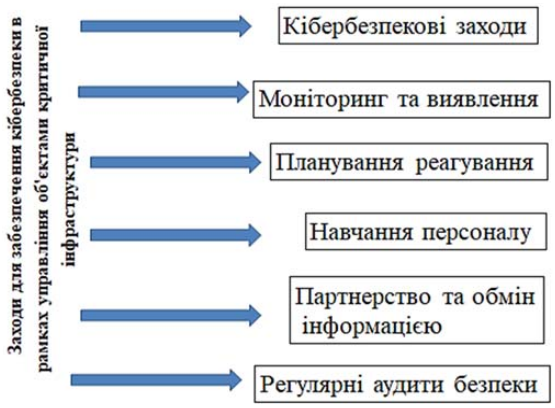

Рисунок 2 – Заходи забезпечення кібербезпеки в рамках процесу управління об’єктами критичної інфраструктури

Джерело: складено автором

4. Навчання персоналу: підвищення рівня обізнаності та навичок персоналу з питань кібербезпеки.

5. Партнерство та обмін інформацією: встановлення механізмів співпраці та обміну інформацією з іншими учасниками, включаючи галузі та державні органи, для об’єднання зусиль у протидії кіберзагрозам.

6. Регулярні аудити безпеки: проведення регулярних аудитів для визначення слабких місць та вдосконалення систем безпеки.

Врахування кібербезпекових аспектів у стратегічному та оперативному плануванні є ключовим елементом ефективного управління об’єктами критичної інфраструктури в умовах сучасних кіберзагроз.

На основі аналізу вищезазначених викликів і тенденцій можна сформулювати загальні рекомендації менеджменту різних рівнів для збільшення ефективності управління об’єктами критичної інфраструктури в умовах війни.

– розробити всеосяжний план управління ризиками, який враховує всі можливі загрози, включаючи кіберзагрози, технологічні зміни та політичні чинники;

– інвестувати ресурси в інновації, не тільки технологічні, а й управлінські, щоб підвищити ефективність, безпеку та стійкість;

– співпрацювати з іншими підприємствами, урядовими структурами та громадськістю, з метою обміну інформацією та ресурсами;

– на рівні держави координувати зусилля з іншими країнами для забезпечення стійкості глобальної інфраструктури.

Впровадження вказаних рекомендацій і стратегій дозволить підвищити ефективність, безпеку та стійкість об’єктів критичної інфраструктури України. У свою чергу для побудови ефективної системи кіберзахисту критичної інфраструктури в умовах війни важливими є не тільки технічні, а й організаційні та нормативно-правові аспекти, а управлінська діяльність за вказаним напрямом повинна спрямовуватися на запобігання ризикам, а не на ліквідацію негативного впливу.

Висновки. Об’єкти критичної інфраструктури відіграють важливу роль у національній безпеці та забезпечують безперебійне функціонування основних систем, таких як енергопостачання, транспорт, зв’язок, водопостачання та водовідведення. Одночасно, вони стикаються й з низкою ризиків, частина з яких пов’язана із функціонуванням кіберпростору. Системи повинні бути готовими до кіберзагроз та вміти швидко реагувати на них. Застосування передових технологій, навчання персоналу та співпраця між різними стейкхолдерами грають ключову роль у забезпеченні успішної адаптації систем управління до нинішніх викликів безпеки. Отже, наявна система управління має забезпечити підвищення ефективності, безпеки та стійкості підприємств критичної інфраструктури, а також сформувати комплекс заходів для управління ризиками.

Бібліографічний список:

1. Мохор В., Цуркан В. Методологія побудови систем управління інформаційною безпекою. *Захист інформації*. 2021. Том 23. № 4. С. 200–211.

2. Включення підприємств до переліку об’єктів критичної інфраструктури, 2022 URL: https://minagro.gov.ua/napryamki/kritichna-infrastruktura/vklyuchennya-pidpriyemstv-do-pereliku-obyektiv-kritichnoyi-infrastrukturi (дата звернення: 14.01.2024).

3. Ящук В.І. Принципи проектування автоматизованих інформаційних систем управління об’єктами критичної інфраструктури. URL: http://surl.li/pdfws (дата звернення: 14.01.2024).

4. Комаров М.Ю., Гончар С.Ф. Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури. *Моделювання та інформаційні технології*. 2017. Вип. 81. С. 12–19.

5. Мельничук О. Управління критичною інфраструктурою: модель та її впровадження. *Актуальні проблеми державного управління*. 2020. № 1(81). С. 64–74.

6. Павук І.В., Кобилкін Д.С. Особливості формування концепції управління проєктними ризиками на об'єктах критичної інфраструктури. *Інновінг сучасних трендів в менеджменті безпеки*. 2023. С. 59–60.

7. Мельничук О.В. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. Державне управління та місцеве самоврядування: зб. наук. праць. Дніпро : ДРІДУ НАДУ, 2019. Вип. 3(42). С. 13–27.

8. Горбаченко С.А., Бойко В.Д. Тестування на проникнення як ефективний інструмент менеджменту кібербезпеки. *Інформаційні технології та суспільство*. 2023. № 3. С. 23–29.

References:

1. Mokhor V., Tsurkan V. (2021) Metodolohiia pobudovy system upravlinnia informatsiinoiu bezpekoiu [Methodology for building information security management systems]. *Zakhyst informatsii – Information security*, vol. 23, no. 4, pp. 200–211.

2. Vkliuchennia pidpryiemstv do pereliku ob'iektiv krytychnoi infrastruktury [Inclusion of enterprises in the list of critical infrastructure facilities]. Available at: https://minagro.gov.ua/napryamki/kritichna-infrastruktura/vklyuchennya-pidpriyemstv-do-pereliku-obyektiv-kritichnoyi-infrastrukturi (accessed January 14, 2024).

3. Yashchuk V. I. Pryntsypy proektuvannia avtomatyzovanykh informatsiinykh system upravlinnia ob'iektamy krytychnoi infrastruktury [Principles of designing automated information systems for managing critical infrastructure facilities]. Available at: http://surl.li/pdfws (accessed January 14, 2024).

4. Komarov M. Y., Gonchar S. F. (2017) Metodyka pobudovy systemy upravlinnia informatsiinoiu bezpekoiu na ob'iektakh krytychnoi infrastruktury [Methodology for building an information security management system at critical infrastructure facilities]. *Modeliuvannia ta informatsiini tekhnolohii – Modeling and information technology*, vol. 81, pp. 12–19.

5. Melnychuk O. (2020) Upravlinnia krytychnoiu infrastrukturoiu: model ta yii vprovadzhennia [Critical infrastructure management: model and its implementation]. *Aktualni problemy derzhavnoho upravlinnia – Actual problems of public administration*, no. 1(81), pp. 64–74.

6. Pavuk I. V., Kobylkin D. S. (2023) Osoblyvosti formuvannia kontseptsii upravlinnia proiektnymy ryzykamy na ob'iektakh krytychnoi infrastruktury [Features of the formation of the concept of project risk management at critical infrastructure facilities]. *Innovinh suchasnykh trendiv v menedzhmenti bezpeky – Innovating modern trends in security management*, pp. 59–60.

7. Melnychuk O. V. (2019) Upravlinnia krytychnoiu infrastrukturoiu derzhavy: bazovi metody ta kryterii identyfikatsii ob'iektiv [Management of the critical infrastructure of the state: basic methods and criteria for identifying objects]. *Derzhavne upravlinnia ta mistseve samovriaduvannia: zb. nauk. prats – Public administration and local self-government: a collection of scientific works.* Dnipro: Dnipro state university. Vol. 3(42), pp. 13–27.

8. Gorbachenko S. A., Boyko V. D. (2023) Testuvannia na pronyknennia yak efektyvnyi instrument menedzhmentu kiberbezpeky [Penetration testing as an effective tool for cybersecurity management]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society,* no. 3, pp. 23–29.

Стаття надійшла до редакції 07.02.2024