СЕКЦІЯ V.
МЕНЕДЖМЕНТ, ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

ІННОВАЦІЙНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Магомедов Андрій Омарович
ORCID ID: 0000-0001-5919-2340
кандидат історичних наук,
здобувач кафедри історії та культури України
Університет Григорія Сковороди в Переяславі, Україна

Зростаючі загрози та ризики, що виникають у безпековій сфері для об’єктів інфраструктури, їх захисту від військових атак, тероризму та природних катастроф, вимагають інноваційних підходів для ефективного захисту і сталого функціонування цих об'єктів. У рамках дослідження зосереджено увагу на вивченні інноваційних підходів та методів, які дозволяють підвищити рівень безпеки об'єктів критичної інфраструктури.

Основним завданням даного дослідження є аналіз і оцінка сукупності технологій, стратегій та підходів, які застосовуються для захисту об’єктів критичної інфраструктури від потенційних загроз. Зосереджуючись на інноваційних рішеннях, розглядаються новаторські технологічні розробки, методи аналізу та прогнозування загроз, а також ефективні стратегії взаємодії з владними структурами та галузевими партнерами у сфері захисту об’єктів критичної інфраструктури [1].

Аналізу можливостей застосування штучного інтелекту та машинного навчання для виявлення та прогнозування ризиків для об'єктів критичної інфраструктури з урахуванням періодичних загроз ракетних обстрілів об’єктів критичної інфраструктури України російською федерацією може бути представлений у вигляді наступного алгоритму – рис. 1

Гібридні підходи до забезпечення безпеки об'єктів критичної інфраструктури в умовах ракетних обстрілів російської федерації викликають увагу науковців до пошуку шляхів мінімізації їх наслідків. Сучасна геополітична обстановка відзначається зростаючою нестабільністю та загрозами для критичної інфраструктури, зокрема з боку російської федерації, не тільки для України, а і для інших країн світу, що зумовлює необхідність розробки інтегрованих підходів до її захисту.

Архітектура управління критичною інфраструктурою базується на ідеях саморегулювання, що відображає політику, орієнтовану на рекомендації, стандартизацію та участь стейкхолдерів у процесах управління безпековими факторами. Обов'язковість законодавства та регулятивних механізмів використовується як основний інструмент, в усіх секторах, у тому числі включаючи сферу ядерного регулювання. Додатковим підходом можна вважати залучення

Рис. 1 **Аналізу можливостей застосування штучного інтелекту та машинного навчання для виявлення та прогнозування потенційних загроз безпеці критичних об'єктів інфраструктури**

** Джерело: розроблено автором на основі аналізу джерел [2-3]*

стейкхолдерів та співпрацю з ними у безпекових питаннях. На практиці, країни часто поєднують елементи обох підходів і можуть визначатися як переважно «добровільні» або «обов'язкові» [4].

Одним із ключових аспектів гібридного підходу є розвиток інтегрованих систем моніторингу та реагування, які мають здатність вчасно виявляти загрози ракетних обстрілів та автоматично активувати заходи захисту, базуючись на сучасних технологіях сенсорів, включаючи радари, супутникові системи та системи виявлення ракет. Крім того, до гібридного підходу також входить розробка стратегій захисту, що

передбачає вивчення потенційних сценаріїв ракетних обстрілів, оцінку можливих наслідків та розробку відповідних заходів забезпечення безпеки [5, 6]. Базовим елементом захисту критичної інфраструктури є сучасні системи ПВО, які мають можливості захищати та забезпечувати безперебійну роботу об’єктів критичної інфраструктури.

Важливо також враховувати вплив політичних та дипломатичних чинників на гібридний підхід до безпеки. Ефективне управління кризовими ситуаціями, співпраця з міжнародними партнерами та використання дипломатичних каналів можуть вирішально вплинути на успішність заходів забезпечення безпеки критичної інфраструктури України.

Узагальнюючи, підходи до забезпечення безпеки об'єктів критичної інфраструктури в умовах ракетних обстрілів російською федерацією вимагають інтеграції різних методів та стратегій. Вони базуються на комплексному аналізі загроз, впровадженні інтегрованих систем моніторингу та реагування, застосуванні кіберзахисту та врахування політичних та дипломатичних аспектів. Тільки цілісний підхід може забезпечити ефективний захист критичної інфраструктури в умовах сучасних геополітичних викликів.

Список використаних джерел:

1. Онищенко С.В., Маслій О.А., Дрібна А.В. Оцінювання фінансово-економічної безпеки підприємства критичної інфраструктури. *Вісник Хмельницького національного університету. Серія «Економічні науки».* 2022, № 6. Т. 1. С. 249-258. https://doi.org/10.31891/2307-5740-2022-312-6(1)-38
2. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3. С. 62-76. URL: http://nbuv.gov.ua/UJRN/spa_2016_3_10
3. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз. URL: https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html
4. Boiarynova K., Melnychuk V. Formation of the human capital development mechanism of machine-building enterprises on the basis of digitalization. *Ekonomichnyy analiz*. Issue 33, 2023, №. 2. Pp. 175-184.
5. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. *Державне управління: удосконалення та розвиток*. 2022. № 1. URL: http://www.dy.nayka.com.ua/pdf/1_2022/40.pdf
6. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення: монографія/ Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. Львів: Сполом, 2020. 418 с