## **Олександр ГУК**

доктор філософії

Національний університет оборони України, м.Київ

[0000-0002-0311-7162](http://orcid.org/0000-0002-0311-7162)

## **Рустам МУРАСОВ**

кандидат технічних наук

Національний університет оборони України, м.Київ

0000-0003-0800-2062

## **Сергій ФАРАОН**

доктор філософії

Національний університет оборони України, м.Київ

## [0000-0002-5500-7352](http://orcid.org/0000-0002-5500-7352)

## **Ігор ТОЛМАЧОВ**

 Національний університет оборони України, м.Київ

[0009-0002-9970-0383](http://orcid.org/0009-0002-9970-0383)

**СТРАТЕГІЇ КІБЕРБЕЗПЕКИ ДЛЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ**

Захист критичної інфраструктури від кібератак став одним з найбільш важливих викликів, які стоять перед сучасними інформаційно-комунікаційними системами, що забезпечують функціонування критичної інфраструктури. Зміни в сучасному цифровому світі обумовлюють застосування нових підходів до кіберзахисту об’єктів критичної інфраструктури, так як кібератаки на важливі сектори: енергетика, зв'язок та охорона здоров'я, логістика, банківська справа, загрожують цивільному населенню, збільшують напругу і руйнують економіку [1, 2].

Необхідним також є міжнародна співпраця та врегулювання міжнародних правових норм з метою захисту критичної інфраструктури від кіберзлочинців та кібертерорізму. Важливо розробляти та впроваджувати ефективні правові механізми для кримінального покарання кіберзлочинців та врегулювання кібердіяльності. Крім того, міжнародне співробітництво дозволяє обмінюватися інформацією про кіберзагрози та кращі практики кібербезпеки з іншими країнами, що є ефективним інструментом для підвищення кіберзахисту.

Постійна зміна природи кіберзагроз є одним з основних викликів. Кібератаки на критичну інфраструктуру можуть мати різноманітні форми, включаючи кібершпигунство, кібертероризм, кіберсаботаж та інші. Отже, розробка адаптивних та гнучких стратегій кібербезпеки є надзвичайно важливою [3].

Існування паралелей між кібертехнологіями та іншими галузями з подвійним призначенням, такими як ядерні, біологічні, космічні та інші, які мають як корисний, так і руйнівний потенціал обумовлює створення нових підходів до захисту об’єктів критичної інфраструктури з метою своєчасного реагування на загрози та виклики, що виникають [4].

Важливим аспектом є необхідність розробки та впровадження інноваційних технологій для захисту критичної інфраструктури [5]. Це може включати в себе використання штучного інтелекту, машинного навчання, блокчейн технологій та інших передових засобів. Такі технології дозволяють ефективно виявляти та запобігати кіберзагрозам, а також оперативно реагувати на кіберінциденти.

Розробка та впровадження стратегій та реалізація кібербезпеки з метою захисту критичної інфраструктури. Такий підхід може включати в себе:

Моніторинг та виявлення: розробка систем, які вчасно виявляють аномальну активність та потенційні загрози;

Шифрування та аутентифікація: застосування сучасних методів шифрування та аутентифікації для захисту комунікацій та доступу до систем;

Резервне копіювання та відновлення: регулярне створення резервних копій даних та можливість швидкого відновлення після інциденту.

Таким чином, подальшою метою досліджень щодо забезпечення захисту критичної інфраструктури від кібератак є розроблення комплекснох стратегій, які будуть включати в собі окремі напрямки щодо моніторингу, шифрування та резервного копіювання інформації, що надасть нові спроможності та перспективи для захисту критичної інфраструктури. Також впровадження адаптованих нормативно-правових механізмів надасть нові можливості суб’єктам та об’єктам кібербезпеки більш ефективно виконувати свої функції в умовах кібератак.

**Література:**

1. Закон України “Про критичну інфраструктуру”. Закон від 2023 року № 5, ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (Дата доступу: 08.03.2024).
2. Постанова Кабінету Міністрів України від 28 квітня 2023 року № 415 “Про затвердження порядку ведення реєстру об'єктів критичної інфраструктури, включення таких об'єктів до реєстру, доступу та надання інформації з нього”. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text (Дата доступу: 08.03.2024).
3. Указ Президента України № 447/2021 “Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України””. URL: https://www.president.gov.ua/documents/4472021-40013 (Дата доступу: 08.03.2024).
4. Мурасов Р. К. Метод оцінювання ризиків для об'єктів критичної інфраструктури в умовах бойових дій з урахуванням їх деструктивно-кумулятивного потенціалу // Journal of Scientific Papers "Social Development and Security". – 2023. – Т. 13, № 1. – DOI: 10.33445/sds.2023.13.1.13.
5. Машталір В. В., Гук О. М., Толмачов І. В., Фараон С. І. Прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення з урахуванням його еволюції // Сучасні інформаційні технології у сфері безпеки та оборони. – Київ: Національний університет оборони України, 2023. – Вип. 48, № 3. – С. 147-156. – DOI: 10.33099/2311-7249/2023-48-3-147-156.