Багрій Г. А.
кандидат психологічних наук, доцент,
доцент кафедри іноземних мов,
Національна академія Державної прикордонної служби
України імені Богдана Хмельницького, Україна
orcid.org/0000-0003-0928-2940

Роль цифрових технологій у забезпеченні безпеки критичної *інфраструктури України*

Анотація. *У тезах досліджено особливості протидії дезінформації та маніпуляціям у кіберпросторі. Розглянуто роль цифрових технологій, штучного інтелекту та інформаційної стійкості у забезпеченні інформаційної безпеки держави.*

Ключові слова: *дезінформація, кіберпростір, інформаційна безпека, цифрові технології, штучний інтелект, маніпуляції, інформаційна стійкість.*

Hanna Bahrii
Ph.D. in Psychology, Assistant Professor,
National Academy of the State Border Guard Service of Ukraine
named after Bohdan Khmelnytskyi
E-mail: bahrii_82@ukr.net
orcid.org/0000-0003-0928-2940

The role of digital technologies in ensuring the security of Ukraine's critical infrastructure

Abstract. *The theses examine the features of countering disinformation and manipulation in cyberspace. The role of digital technologies, artificial intelligence, and information resilience in ensuring the state's information security is analyzed.*

Keywords: *disinformation, cyberspace, information security, digital technologies, artificial intelligence, manipulation, information resilience.*

Швидкий розвиток цифрових технологій у поєднанні зі зростаючою складністю сучасних загроз суттєво впливає на підходи до забезпечення безпеки критичної інфраструктури в Україні. В умовах гібридної війни, кібератак та зростаючої залежності від цифрових систем захист об'єктів критичної інфраструктури стає пріоритетом для системи національної безпеки.

Цифрові технології більше не є лише допоміжними інструментами, а становлять основу сучасних механізмів безпеки. Їх інтеграція в системи захисту інфраструктури визначає стійкість, адаптивність і безперервність функціонування життєво важливих сервісів в умовах кризи та невизначеності.

Безпека критичної інфраструктури є складною, багаторівневою системою, що охоплює фізичний захист, кібербезпеку, інформаційну стійкість та скоординовані механізми реагування. Сучасна парадигма передбачає

інтеграцію цифрових технологій, таких як штучний інтелект, аналітика великих даних, хмарні обчислення та автоматизовані системи моніторингу. Ці технології забезпечують виявлення загроз у режимі реального часу, прогнозний аналіз та швидке ухвалення рішень. Наприклад, інтелектуальні системи моніторингу можуть аналізувати великі обсяги даних з енергетичних мереж або транспортних систем, виявляючи аномалії, що можуть свідчити про кібервтручання або технічні збої. Це змінює підхід від реактивного до проактивного управління безпекою [1].

Міжнародний досвід свідчить, що розвинені країни покладаються на стандартизовані підходи та інтегровані цифрові рішення для захисту критичної інфраструктури. Зокрема, використання рамкових моделей кібербезпеки, моделей оцінки ризиків та протоколів реагування на інциденти забезпечує системний підхід до захисту інфраструктури. Ключовим елементом є впровадження систем безперервного моніторингу у поєднанні з автоматизованими механізмами реагування. Наприклад, сучасні платформи безпеки можуть автоматично ізолювати скомпрометовані сегменти мережі або активувати резервні системи, мінімізуючи можливі збитки. Роль фахівців також змінюється, оскільки вони повинні поєднувати технічні знання з аналітичним мисленням і здатністю працювати в умовах швидких змін [2].

Аналіз сучасного стану захисту критичної інфраструктури в Україні свідчить як про значний прогрес, так і про наявність певних проблем. З одного боку, Україна набула унікального досвіду протидії кіберзагрозам і забезпечення функціонування інфраструктури в умовах збройного конфлікту. Це включає захист енергетичних систем, мереж зв’язку та транспортної логістики як від фізичних, так і від кіберзагроз. З іншого боку, залишаються проблеми, пов’язані з фрагментацією цифрових рішень, недостатньою координацією між установами та нерівномірним рівнем впровадження технологій у різних секторах. У деяких випадках застарілі системи обмежують ефективність сучасних заходів безпеки [3].

Впровадження передових цифрових технологій пов’язане як з об’єктивними, так і з суб’єктивними труднощами. До об’єктивних обмежень належать обмежені фінансові ресурси, недостатній рівень технічного забезпечення та необхідність масштабної модернізації інфраструктурних систем. Суб’єктивні виклики включають опір організаційним змінам, нестачу кваліфікованого персоналу та потребу у формуванні нової культури безпеки, орієнтованої на інновації та адаптивність. Крім того, інтеграція міжнародного досвіду потребує ретельної адаптації до національних умов, оскільки пряме копіювання іноземних моделей без урахування місцевої специфіки може знижувати їх ефективність.

У цьому контексті розвиток безпеки критичної інфраструктури в Україні має ґрунтуватися на синергетичному підході, що поєднує міжнародні стандарти

з національним досвідом. Перспективним напрямом є впровадження цифрових платформ управління ризиками, які інтегрують дані з різних секторів у єдину систему. Наприклад, використання технологій штучного інтелекту дозволяє прогнозувати можливі сценарії атак та розробляти превентивні заходи. Ще одним важливим напрямом є створення кіберполігонів для підготовки фахівців, де моделюються реальні загрози та відпрацьовуються механізми реагування [4].

Цифровізація процесів безпеки відкриває нові можливості для підвищення ефективності захисту інфраструктури. Використання аналітики даних, машинного навчання та автоматизованих систем управління дозволяє постійно вдосконалювати механізми безпеки. Наприклад, аналіз інцидентів за допомогою цифрових інструментів дає змогу детально оцінити вразливості та розробити більш стійкі системи. Це сприяє формуванню культури безперервного навчання та вдосконалення в секторі безпеки.

Перспективи розвитку безпеки критичної інфраструктури в Україні тісно пов'язані зі створенням інтегрованої цифрової екосистеми, здатної реагувати на сучасні загрози. Поєднання інноваційних технологій із практичним досвідом підвищить стійкість інфраструктурних систем та забезпечить їх безперебійну роботу навіть в екстремальних умовах. Зокрема, посилення співпраці з міжнародними партнерами та узгодження з глобальними стандартами сприятиме підвищенню сумісності та колективної безпеки.

Отже, роль цифрових технологій у забезпеченні безпеки критичної інфраструктури стає дедалі більш визначальною. Їх ефективне впровадження потребує комплексного підходу, що включає технологічні інновації, інституційний розвиток та формування сучасної культури безпеки. Це створить необхідні умови для зміцнення національної стійкості та забезпечення стабільного функціонування критичної інфраструктури в умовах сучасних викликів.

Список використаних джерел

1. Ящук В. І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави // Цифрові технології у відновленні економіки та інфраструктури України : матеріали І Міжнар. Наук.-практ. Конф. – Київ, 2024. URL: https://sci.ldubgd.edu.ua/bitstream.pdf
2. Цифрові технології у відновленні економіки та інфраструктури України : матеріали І Міжнар. Наук.-практ. Конф. – Київ, 2024. – URL: https://yydorogyy.kiev.ua/blog.pdf
3. Сенюк О. П., Лапка О. Я. Роль цифрових технологій у забезпеченні інформаційної безпеки в умовах воєнного стану // Наукові праці Національної академії внутрішніх справ. – 2024. – URL:

https://elar.navs.edu.ua/server/api/core/bitstreams/782c2fe0-0483-4a5b-bfd2-16c03374ba60/content

4. Помаза Т., Тарадуда О. Держава і суспільство: сучасні виклики та пошук рішень : збірник матеріалів ІІІ Всеукр. Наук.-теорет. Конф. (16 травня 2024 р.). – Київ : Київський фаховий коледж туризму та готельного господарства, 2024. – URL: https://repositsc.nuczu.edu.ua/bitstream.pdf