Коба О. В.,
кандидат педагогічних наук, старший дослідник, доцент кафедри забезпечення державної безпеки, Київський інститут Національної гвардії України
(*м. Київ, України*)

ВПЛИВ СУЧАСНИХ ТЕХНОЛОГІЙ НА ПРОПУСКНИЙ РЕЖИМ У ФІЗИЧНІЙ ЯДЕРНІЙ БЕЗПЕЦІ: ПРАКТИКА ПІДРОЗДІЛІВ НГУ

Забезпечення фізичної ядерної безпеки є одним із ключових завдань національної безпеки України, особливо в умовах повномасштабної збройної агресії. Пропускний режим на об'єктах ядерної інфраструктури є критично важливим елементом захисту від несанкціонованого доступу, диверсій та терористичних загроз. Сучасні технології, зокрема біометричні системи, автоматизовані комплекси контролю доступу, безпілотні системи спостереження та штучний інтелект, кардинально змінюють підходи до організації пропускного режиму[6, 7]. Метою цієї роботи є аналіз впливу сучасних технологій на систему пропускного режиму у сфері фізичної ядерної безпеки та дослідження практики їх застосування підрозділами Національної гвардії України (далі-НГУ) [4, 5].

Актуальність теми. Умови воєнного стану суттєво посилюють вимоги до пропускного режиму на ядерних об'єктах. Зростає необхідність у багаторівневій системі захисту, яка включає не лише фізичну охорону, а й кіберзахист, автоматизований моніторинг та аналітику даних у режимі реального часу. Використання технологій розпізнавання облич, систем відеоаналітики та безпілотних літальних апаратів дає змогу підвищити ефективність охорони об'єктів критичної інфраструктури. Водночас, у 2024-2025 рр. спостерігається зростання ризиків, пов'язаних з AI, таких як вразливість до кібератак чи помилки в розпізнаванні, що вимагає балансованого підходу[7, 8].

Практика підрозділів НГУ та інших структур, що забезпечують охорону ядерних об'єктів, впроваджують сучасні комплекси контролю доступу, системи відеоспостереження з аналітикою на основі штучного інтелекту, мобільні сканери документів, а також технології радіаційного моніторингу. В умовах воєнного стану такі системи дають змогу оперативно реагувати на потенційні загрози та знижувати людський фактор при ухваленні рішень. Не обмежуючись НГУ, подібні технології застосовуються Державною інспекцією ядерного регулювання України (далі-ДІЯРУ) для інспекцій та моніторингу, де AI використовується для аналізу даних з датчиків радіації, а біометрія – для верифікації персоналу на АЕС. Наприклад, у 2024 р. Міністерство енергетики інтегрувало AI-дрони для патрулювання периметрів, що підвищило ефективність на 30-40% за даними звітів. Міжнародний досвід (наприклад, США через NRC) показує, що комбінація AI з біометрією знижує час реакції на

загрози, але вимагає захисту від хакерських атак, як у випадках з українськими дронами в обороні [6, 7, 8].

Окремим напрямом діяльності стала протидія безпілотним літальним апаратам (далі-БПЛА) та баражуючим боєприпасам типу «Шахед». Для цього застосовуються мобільні комплекси радіоелектронної боротьби (далі-РЕБ), системи акустичної та тепловізійної детекції дронів, а також засоби активного придушення каналів управління. У поєднанні з технологіями радіаційного моніторингу та автоматизованими системами управління силами охорони це дозволяє забезпечити комплексний підхід до захисту ядерних об'єктів і значно зменшити вплив людського фактора при ухваленні рішень [5, 9].

Правовий аспект. Використання сучасних технологій регламентується Законом України «Про використання ядерної енергії та радіаційну безпеку»[2], Законом України «Про правовий режим воєнного стану»[3], Закон України «Про Національну гвардію України» [4], та іншими нормативно-правовими актами.

Водночас практика не лише НГУ, а й ДІЯРУ та інших структур потребує оновлення підзаконної бази для легітимізації застосування новітніх технологій, зокрема біометрії та систем штучного інтелекту, у сфері охорони ядерних об'єктів. У 2025 р. Україна підписала Рамкову конвенцію Ради Європи про штучний інтелект, права людини, демократію та верховенство права, яка встановлює стандарти для етичного використання AI, включаючи заборони на певні біометричні системи (наприклад, розпізнавання емоцій) у критичних сферах [10]. Це узгоджується з проєктом Закону № 8153 про захист персональних даних, що адаптує GDPR до AI-контексту, забороняючи масове біометричне сканування без згоди [11]. Міністерство цифрової трансформації опублікувало Білу книгу з регуляції AI, орієнтовану на гармонізацію з EU AI Act, де високоризикові системи (як у ядерній безпеці) вимагають обов'язкової сертифікації. За рекомендаціями IAEA, регуляторний фреймворк повинен враховувати ризики AI, такі як ядерні загрози від автономних систем, і включати міжнародну технічну допомогу для оновлення норм. Прогалини в чинній базі, наприклад, відсутність конкретних правил для AI в пропускному режимі, можуть бути заповнені через прийняття спеціального Закону про регуляцію AI-технологій, як запропоновано в 2024 р [12, 13].

Сучасні технології суттєво змінюють підходи до забезпечення пропускного режиму у фізичній ядерній безпеці. Досвід підрозділів НГУ свідчить про ефективність впровадження автоматизованих систем контролю, біометричних технологій та інтелектуальних систем відео спостереження [5]. Для підвищення ефективності охорони ядерних об'єктів необхідно оновити нормативно-правову базу [10, 11, 13], забезпечити належний рівень фінансування та продовжувати інтеграцію сучасних технологій у практику охорони об'єктів критичної інфраструктури [6, 7, 8, 9].

Список використаних джерел:

1. Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» : за станом на 19 жовт. 2000 р. № 2064-III // Відомості Верховної Ради України. – 2001. – № 1. – Ст. 1.

2. Закон України «Про використання ядерної енергії та радіаційну безпеку» : за станом на 8 лют. 1995 р. № 39/95-ВР // Відомості Верховної Ради України. – 1995. – № 12. – Ст. 81.

3. Закон України «Про правовий режим воєнного стану» : за станом на 12 трав. 2015 р. № 389-VIII // Відомості Верховної Ради України. – 2015. – № 28. – Ст. 250.

4. Закон України «Про Національну гвардію України» : за станом на 13 бер. 2014 р. № 876-VII // Відомості Верховної Ради України. – 2014. – № 17. – Ст. 594.

5. Наказ Міністерства внутрішніх справ України від 03.07.2014 № 625 «Про затвердження Положення про військові частини і підрозділи з охорони важливих державних об'єктів та спеціальних вантажів НГУ» [Електронний ресурс] // Офіційний вебпортал МВС України. – Режим доступу: https://zakon.rada.gov.ua/go/z0830-14.

6. Штучний інтелект у ядерній безпеці [Електронний ресурс] // Офіційний сайт Комісії ядерного регулювання США (NRC). – 2025. – Режим доступу: https://www.nrc.gov/ai.html.

7. Штучний інтелект та ядерна зброя: здоровий глузд у розумінні витрат і переваг / Texas National Security Review. – 2025. – Т. 8, № 3. – С. 45–67. – Режим доступу: https://tnsr.org/2025/06/artificial-intelligence-and-nuclear-weapons-a-commonsense-approach-to-understanding-costs-and-benefits/.

8. Інформаційний бюлетень: Просування зусиль Міністерства внутрішньої безпеки щодо зниження ризиків на перетині штучного інтелекту та хімічних, біологічних, радіологічних і ядерних загроз [Електронний ресурс] // Офіційний сайт DHS. – Режим доступу: https://www.dhs.gov/publication/fact-sheet-and-report-dhs-advances-efforts-reduce-risks-intersection-artificial.

9. Огляд новин ядерної безпеки та оновлення для членів, травень 2025 р. / Stimson Center. – Вашингтон, 2025. – 32 с. – Режим доступу: https://www.stimson.org/2025/nuclear-security-news-and-member-updates-roundup-may-2025/.

10. Безпечний ШІ для мільйонів українців: Україна підписала Рамкову конвенцію Ради Європи про штучний інтелект, права людини, демократію та верховенство права [Електронний ресурс] // Офіційний вебпортал Кабінету Міністрів України. – 2025. – Режим доступу: https://www.kmu.gov.ua/en/news/bezpechnyi-shi-dlia-milioniv-ukraintsiv-ukraina-pidpysala-ramkovu-konventsiiu-pro-shtuchnyi-intelekt-ta-prava-liudyny.

11. Захист персональних даних та ШІ: Проєкт Закону № 8153, GDPR та EU AI Act у контексті технологій штучного інтелекту / Dnistrianskyi Center for Law

and Policy. – Київ, 2022. – 28 с. – Режим доступу: https://dc.org.ua/en/news/zahyst-personalnyh-danyh-i-shi-zakonoproekt-8153-gdpr-ta-zakon-es-pro-shi-u-konteksti-tehnologiy-shtuchnogo-intelektu.

12. Регулювання штучного інтелекту / Ukrainian Law Firms. – Київ, 2025. – С. 112–125. – Режим доступу: https://ukrainianlawfirms.com/reviews/ai-regulation/.

13. Біла книга з регулювання штучного інтелекту в Україні [Електронний ресурс] / Міністерство цифрової трансформації України. – Київ, 2024. – 56 с. – Режим доступу: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%91%D1%96%D0%BB%D0%B0_%D0%BA%D0%BD%D0%B8%D0%B3%D0%B0_%D0%B7_%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%A8%D0%86_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96_%D0%90%D0%9D%D0%93%D0%9B.pdf.