



Теорія і методика професійної освіти

УДК: 004.8:623.459

DOI <https://doi.org/10.5281/zenodo.20756065>

## АНАЛІЗ НАСЛІДКІВ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ СТРИМУВАННЯ ХІМІЧНИХ, БІОЛОГІЧНИХ, РАДІОЛОГІЧНИХ ТА ЯДЕРНИХ (ХБРЯ) РИЗИКІВ

**Абрамов Костянтин Анатолійович,**

старший викладач, Національний юридичний університет імені Ярослава

Мудрого, ORCID: 0009-0003-1625-3432

**Прийнято: 15.05.2026 | Опубліковано: 30.05.2026**

***Анотація.** У статті досліджено наслідки інтеграції технологій штучного інтелекту у систему стримування та протидії хімічним, біологічним, радіологічним та ядерним (ХБРЯ) загрозам в умовах якісної трансформації глобального безпекового середовища. Проаналізовано концептуальну рамку застосування штучного інтелекту, машинного навчання та автономних систем прийняття рішень у безпековому контексті, зокрема розмежовано таксономію ШІ-застосувань у ХБРЯ-домені: предиктивну аналітику, комп'ютерний зір, обробку природної мови для розвідки відкритих джерел та автономну робототехніку для дезактивації. Розкрито ландшафт ХБРЯ-загроз у 2020-х роках із акцентом на російсько-українську війну, зокрема хімічні інциденти на лінії зіткнення (підтверджені звітом ОЗХЗ щодо агента CS на Дніпропетровщині), радіаційні ризики навколо Запорізької АЕС (руйнування станцій моніторингу у тридцятикілометровій зоні) та біобезпекові виклики в умовах зруйнованої інфраструктури. Систематизовано емпіричні дані щодо ефективності ШІ-систем детекції хімічних агентів із точністю 96–99*



відсотків, радіонуклідної ідентифікації понад 95 відсотків та біосурвеїлансу на основі розвідки відкритих джерел, зокрема досвід системи EPIWATCH в Україні. Обґрунтовано, що ефективність ШІ-детекції є умовною та залежить від якості даних, інтероперабельної архітектури й підготовленості персоналу, а в бойових умовах лабораторні показники неминуче знижуються. Досліджено етико-правовий вимір інтеграції через призму концепції значущого людського контролю, шести принципів відповідального використання ШІ НАТО та ризиків подвійного використання генеративних моделей, зокрема випадок генерації нервово-паралітичного агента VX моделлю MegaSyn. Проаналізовано український контекст, включно з нормативною базою ДСНС, досвідом систем EPIWATCH та SaveEcoBot, перспективами адаптації до Плану дій ЄС із ХБРЯ-безпеки та стандартів НАТО. Сформульовано поетапну стратегію інтеграції ШІ у національну систему ХБРЯ-стримування з урахуванням обмежених ресурсів та умов збройного конфлікту. Авторська позиція полягає в необхідності агресивного розгортання ШІ в аналітичних та детекційних функціях за збереження людського нагляду над усіма критичними рішеннями у ХБРЯ-домені.

**Ключові слова:** штучний інтелект, ХБРЯ-загрози, глобальна безпека, стримування, біосурвеїланс, радіаційний моніторинг, значущий людський контроль, подвійне використання

## ANALYSIS OF THE CONSEQUENCES OF ARTIFICIAL INTELLIGENCE INTEGRATION FOR CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR (CBRN) RISK DETERRENCE

*Abramov Kostiantyn Anatoliiovych,*

*Senior Lecturer, Yaroslav Mudryi National Law University,*

*ORCID: 0009-0003-1625-3432*



***Abstract.** The article examines the consequences of integrating artificial intelligence technologies into the system of deterrence and countering chemical, biological, radiological and nuclear (CBRN) threats amid a qualitative transformation of the global security environment. The conceptual framework for applying artificial intelligence, machine learning and autonomous decision-making systems in the security context is analysed, with a taxonomy of AI applications in the CBRN domain delineated: predictive analytics, computer vision, natural language processing for open-source intelligence and autonomous robotics for decontamination. The CBRN threat landscape of the 2020s is explored with emphasis on the Russo-Ukrainian war, including chemical incidents along the front line (confirmed by the OPCW report on CS agent in Dnipropetrovsk region), radiation risks around the Zaporizhzhia Nuclear Power Plant (destruction of monitoring stations within the thirty-kilometre zone) and biosecurity challenges amid destroyed infrastructure. Empirical data on the effectiveness of AI detection systems for chemical agents with accuracy of 96–99 percent, radionuclide identification above 95 percent and biosurveillance based on open-source intelligence are systematised, including the EPIWATCH system experience in Ukraine. It is substantiated that the effectiveness of AI detection is conditional and depends on data quality, interoperable architecture and personnel readiness, while laboratory performance inevitably declines under combat conditions. The ethical and legal dimension of integration is studied through the prism of the meaningful human control concept, NATO six principles of responsible AI use and dual-use risks of generative models, notably the MegaSyn case of VX nerve agent generation. The Ukrainian context is analysed, including the SESU regulatory framework, experience of EPIWATCH and SaveEcoBot systems, and prospects for adaptation to the EU CBRN Action Plan and NATO standards. A phased strategy for AI integration into the national CBRN deterrence system is formulated taking resource constraints and armed conflict conditions into account. The author argues for aggressive AI deployment in analytical and detection functions while preserving human oversight over all critical decisions in the CBRN domain.*

**Keywords:** *artificial intelligence, CBRN threats, global security, deterrence, biosurveillance, radiation monitoring, meaningful human control, dual use*

**Постановка проблеми.** Ландшафт хімічних, біологічних, радіологічних та ядерних загроз у 2020-х роках зазнав якісної трансформації, і російсько-українська війна стала його найгострішим проявом, бо саме вона водночас актуалізувала всі чотири компоненти ХБРЯ-спектру на території однієї держави. Хімічний вимір перестав бути гіпотетичним: за результатами технічного візиту ОЗХЗ підтвердила наявність сльозогінного агента CS у зразках із окопу на Дніпропетровщині, а генеральний директор організації наголосив, що всі 193 держави-учасниці Конвенції про хімічну зброю зобов'язалися ніколи не застосовувати таку зброю [1]. Сполучені Штати окремо констатували застосування рф хлорпікрину (задушливого агента часів Першої світової війни) проти українських військ, кваліфікувавши це як порушення Конвенції [2]. Радіологічно-ядерний вимір уособлює Запорізька атомна електростанція, де внаслідок обстрілів чотири з чотирнадцяти довоєнних станцій радіаційного моніторингу у тридцятикілометровій зоні стали недоступними, а 27 червня 2024 року була знищена станція за шістнадцять кілометрів на південний захід від майданчика [3]. Біологічний вимір актуалізувала пандемія COVID-19 як стрес-тест біобезпеки, а зруйнована інфраструктура додала ризиків спалахів інфекцій, і одночасність цих загроз, ускладнена активними бойовими діями, не має аналогів у новітній історії.

Якщо припустити, що традиційні механізми стримування здатні абсорбувати таку кількість одночасних загроз, емпіричні дані швидко спростовують це припущення. Формальний епідеміологічний нагляд в Україні після лютого 2022 року фактично припинився для більшості інфекційних хвороб, мережі радіаційного моніторингу зазнали руйнувань, а верифікація хімічних інцидентів на лінії зіткнення потребує тижнів міжнародних інспекцій. Інтеграція технологій штучного інтелекту (ШІ) у систему ХБРЯ-стримування здатна



компенсувати інституційні розриви, оскільки алгоритмічна обробка даних не потребує фізичної присутності інспекторів і працює у режимі реального часу. Звіт Міністерства внутрішньої безпеки США 2024 року фіксує, що впровадження ШІ у запобігання, виявлення, реагування та пом'якшення наслідків здатне забезпечити суттєві або емерджентні переваги, зокрема в атрибуції підозрюваних біологічних чи хімічних атак [4]. Водночас та сама технологія залишається онтологічно двоїстою: в міру наближення генеративних моделей до експертного рівня зростає ризик їх зловживання для конструювання ХБРЯ-зброї, але паралельно сектор ШІ стає партнером у зниженні цих ризиків [5]. Двоїстість захисного й наступального потенціалу ШІ означає, що жодна оцінка ефективності не може бути відірвана від оцінки ризику, а стримування охоплює не лише технічну спроможність виявити загрозу, а й управлінську здатність утримати баланс між швидкістю машини та відповідальністю людини, і саме ця телеологічна напруга є предметом подальшого аналізу.

**Аналіз останніх досліджень і публікацій.** Застосування машинного навчання у ХБРЯ-захисті системно досліджено в оглядовій роботі журналу *Heliyon* (2024), де проаналізовано п'ять функціональних областей (від планування розташування сенсорів до підтримки рішень) і запропоновано класифікаційну рамку, яка систематизує підходи, що до цього існували розрізнено [6]. Технології ідентифікації хімічних агентів досліджувалися із застосуванням гіперспектрального зображення, де експериментально підтверджено зниження хибнопозитивних спрацювань приблизно у сто разів і досягнення ймовірності виявлення 96 відсотків порівняно з 90 відсотками класичного підходу [7]. Дослідження 2025 року підтвердило подальше зростання точності: модель на основі газової хроматографії з кварцово-підсиленою фотоакустичною спектроскопією досягла 97 відсотків за довірчого інтервалу 95,5 відсотків і 99 відсотків за інтервалу 99,7 відсотків [8]. Систематичний огляд застосувань МН до гамма-спектроскопії на детекторах NaI(Tl) засвідчив, що глибокі моделі перевершують традиційний аналіз із точністю ідентифікації



радіонуклідів понад 95 відсотків навіть за складних умов екранування та низької статистики рахунку [9], а безпілотні платформи з інтегрованими сцинтиляційними сенсорами CLYC уможливають картографування дози без опромінення персоналу [10].

Біосурвеїланс як напрям отримав два комплементарних дослідження, що утворюють змістовну полярність: ретроспективний аналіз стічних вод Барселони виявив SARS-CoV-2 за 41 день до офіційного першого випадку, охопивши близько 2,7 мільйона мешканців [11], тоді як систематичний огляд у *Frontiers in Public Health* застерігає, що попри вищі метрики чутливості ШІ-моделей впровадження органами громадського здоров'я залишається низьким через брак довіри, проблеми інтерпретованості та упередженість тренувальних даних [12]. ШІ-система EPIWATCH при моніторингу інфекційних спалахів в Україні зафіксувала різке зростання повідомлень щодо холери, ботулізму, туберкульозу після лютого 2022 року, яких офіційні джерела не реєстрували [13], а огляд у тому ж журналі аналізує конвергенцію ШІ, CRISPR та синтетичної біології для протидії біобезпековим загрозам, акцентуючи як захисний потенціал, так і ризики подвійного використання [14]. Глибоке навчання суттєво прискорило моделювання атмосферної дисперсії: нейромережа навчається за 4,4 секунди та видає прогноз за 8 мілісекунд, зберігаючи прийнятну точність порівняно з обчислювально-гідродинамічними моделями [15], що скорочує розрив між детекцією та евакуацією з годин до секунд.

Етичний вимір автономності розкрито через призму летальних автономних систем зброї та міжнародного гуманітарного права, де обґрунтовано необхідність збереження значущого людського контролю над рішеннями про застосування сили [16]. Дослідження в *Nature Machine Intelligence* емпірично підтвердило загрозу подвійного використання: інвертування цільової функції моделі MegaSyn згенерувало 40 000 молекул, включно з нервово-паралітичним агентом VX [17], а відповіддю стала розробка методів оцінки двоїстих спроможностей біологічних ШІ-моделей до їх розгортання [18]. Робототехніку



реагування на ядерні аварії систематизовано в огляді досвіду Фукусіми, де зафіксовано як переваги безпілотних платформ, так і системні обмеження (запізнення у тижні, вихід з ладу, потреба в унікальній конструкції) [19]. Біобезпекову систему України проаналізовано у Health Security, де констатовано її зміцнення за підтримки міжнародних партнерів [20], а вітчизняні дослідження у журналах «Економічний простір» [21], «Ядерна та радіаційна безпека» [22] та Information Technology [23] засвідчують формування внутрішньої експертної бази, хоча й за відсутності системного впровадження.

**Виділення невирішених частин загальної проблеми.** Аналіз наукової літератури засвідчує, що переважна більшість досліджень ефективності ШІ-систем у ХБРЯ-доміні зосереджена на лабораторних або синтетичних наборах даних, тоді як екстраполяція отриманих показників точності на реальні бойові умови (з нестабільним фоном, екрануванням і деградованими сенсорами) залишається недостатньо обґрунтованою. Системного дослідження інтеграції ШІ у ХБРЯ-стримування саме в українському контексті, який поєднує радіаційні, хімічні та біологічні загрози одночасно, фактично не проведено. Етико-правовий аналіз автономності ШІ-рішень у ХБРЯ-сфері переважно здійснюється в абстрактних рамках летальних автономних систем зброї, тоді як специфіка цивільного захисту (де ціна помилки вимірюється не лише життями, а й екологічними катастрофами тривалістю в десятиліття) потребує окремого опрацювання. Нарешті, відсутня поетапна стратегія інтеграції ШІ у ХБРЯ-стримування для країн з обмеженими ресурсами в умовах збройного конфлікту, що робить наявні рекомендації розвинених країн лише частково застосовними.

**Формулювання цілей статті.** Метою статті є комплексний аналіз наслідків інтеграції штучного інтелекту для стримування ХБРЯ-ризиків, що охоплює технологічний, етико-правовий та управлінський виміри з акцентом на український контекст. Для досягнення мети передбачається систематизувати концептуальну рамку застосування ШІ у ХБРЯ-доміні, оцінити вимірну ефективність ШІ-систем детекції та моніторингу за різними типами загроз,



проаналізувати етико-правові обмеження автономності ШІ-рішень через призму значущого людського контролю, дослідити ризики подвійного використання генеративних моделей і сформулювати поетапну стратегію інтеграції ШІ у національну систему ХБРЯ-стримування.

**Виклад основного матеріалу.** Концептуальна рамка інтеграції ШІ у безпековий простір потребує чіткого розмежування трьох понять, які в публічному дискурсі часто змішують, хоча кожне з них породжує якісно різні наслідки для стримування. Під штучним інтелектом розуміють широкий клас систем, що імітують когнітивні функції людини; машинне навчання є його підмножиною, де алгоритм виводить закономірності з даних без явного програмування; автономні системи прийняття рішень додають здатність діяти у фізичному світі без втручання оператора. Якщо перші два рівні залишаються інструментами аналітика, третій набуває суб'єктності у прийнятті рішень, і саме на цьому рівні виникають найгостріші етичні та правові колізії. Дослідники визначають автономну систему ХБРЯ-захисту як спроможність незалежно виявляти, ідентифікувати чи нейтралізувати загрозу, спираючись на сенсори, робототехніку та алгоритми, утримуючи бійця на безпечній відстані [6]. Таксономія застосувань ШІ охоплює предиктивну аналітику, комп'ютерний зір для аналізу супутникових знімків, обробку природної мови для розвідки відкритих джерел та автономну робототехніку для дезактивації, і кожен із цих напрямів змінює парадигму від реактивної схеми «виявив і відреагував» до проактивного запобігання, коли система прогнозує інцидент до його настання.

Визначивши категоріальний апарат, видається обґрунтованим перейти до оцінки вимірної ефективності ШІ-детекції, яка, за поширеним уявленням, є абсолютною характеристикою технології, проте емпіричні дані спростовують цю лінійну інтерпретацію. Точність 96–99 відсотків для хімічних агентів [7; 8] та понад 95 відсотків для радіонуклідної ідентифікації [9] здобувається переважно на синтетичних або лабораторних наборах даних, а в польових умовах війни (з нестабільним фоном, екрануванням і деградованими сенсорами) показники

неминуче знижуються. Безпілотні платформи з інтегрованими сцинтиляційними сенсорами справді дозволяють картографувати дозу без опромінення персоналу [10], проте їхня робота залежить від погодних умов, завад радіоелектронної боротьби та доступності захищених каналів зв'язку, що в зоні бойових дій не гарантовано. Ефективність ШІ-систем є, відтак, не абсолютною, а умовною: вона реалізується лише за наявності якісних даних, інтегрованої архітектури та підготовленого персоналу, і без цих передумов висока лабораторна точність перетворюється на оманливу впевненість, небезпечнішу за відверту відсутність даних, бо створює ілюзію контролю.

### Таблиця 1

#### Порівняльна характеристика ефективності ШІ-систем детекції за типами ХБРЯ-загроз

| Домен загрози           | Метод ШІ-детекції   | Лабораторна точність  | Польові обмеження  |
|-------------------------|---|---|--|
| Хімічний                | Гіперспектральне зображення з неймережевою класифікацією; GC-QEPAS із моделлю машинного навчання для імітаторів БОР | 96 % ймовірності виявлення при зниженні хибнопозитивних у ~100 разів (гіперспектр.); 97–99 % (GC-QEPAS, CI 95,5–99,7 %)                           | Забруднення оптики димом і пилом, потреба калібрування під суміші агентів; метеозалежність розсіювання   |
| Біологічний             | OSINT-аналітика EPIWATCH (NLP + ML на медіа-потоках); моніторинг стічних вод із ML-кластеризацією                   | Випередження формального нагляду на 41 день (wastewater, Барселона); виявлення спалахів холери, ботулізму, ТБ в Україні, не зафіксованих офіційно | Низька довіра органів охорони здоров'я до ШІ-прогнозів; упередженість тренувальних даних; неповне покриття сільських районів і прифронтових зон; залежність від інтернет-зв'язку |
| Радіологічний / ядерний | Гамма-спектроскопія NaI(Tl) з глибокими неймережами; БПЛА з CLYC-детекторами (гамма + нейтрони)                     | > 95 % ідентифікації радіонуклідів за екранування та низького рахунку   | РЕБ-завади БПЛА, обмежений час польоту, деградація сенсорів за високих накопичених доз; руйнування стаціонарних станцій (4 із 14 у зоні ЗАЕС)                                    |

*Джерело: складено автором на основі [7–13]*

Біосурвеїланс ілюструє прірву між лабораторним потенціалом і реальним впровадженням з особливою наочністю, і якщо поставити питання онтологічно,



то проблема полягає не у відсутності технології, а у відсутності інституційної довіри до неї. Ретроспективний аналіз стічних вод Барселони виявив SARS-CoV-2 за сорок один день до офіційного першого випадку, охопивши близько 2,7 мільйона мешканців [11], що означає понад місяць форвардного сигналу для системи охорони здоров'я. Однак систематичний огляд застерігає: попри вищі метрики чутливості та точності ШІ-моделей порівняно з базовими підходами впровадження органами громадського здоров'я залишається низьким через брак довіри, проблеми інтерпретованості та упередженість тренувальних даних [12]. Український досвід підтверджує закономірність із трагічною наочністю: ШІ-система EPIWATCH зафіксувала різке зростання повідомлень щодо холери (з нуля до 157), ботулізму (з 22 до 122), туберкульозу (з 11 до 75) після лютого 2022 року, тоді як формальний нагляд загрози не реєстрував [13]. Досвід EPIWATCH дає підстави для формулювання парадоксу впровадження: ШІ найбільш цінний саме там, де інституційні системи руйнуються, проте саме в цих умовах його інтеграція є найскладнішою через брак інфраструктури, кадрів та фінансування, і розв'язання цього парадоксу потребує не технологічних, а насамперед організаційних та політичних рішень.

Описана діагностична спроможність залишається лише першою ланкою ланцюга стримування; швидкість прийняття рішень після детекції визначає темпоральний вимір, де ШІ дає найвідчутнішу перевагу. Моделювання розповсюдження хмари забруднення традиційно спиралося на гаусові, лагранжеві та обчислювально-гідродинамічні моделі, точні, але повільні, і нейромережа з двома прихованими шарами, що навчається за 4,4 секунди й видає прогноз за 8 мілісекунд [15], скорочує розрив між детекцією та евакуацією з годин до секунд. Координація міжвідомчого реагування за участю ДСНС, Збройних Сил України та міжнародних місій потребує саме такої оперативності, позаяк кожна хвилина затримки у визначенні напрямку руху хмари може коштувати сотень додаткових постраждалих. Роботизовані платформи забезпечують роботу в зонах зараження, і досвід Фукусіми надав конкретні



уроки, що водночас охолоджують надмірний оптимізм: роботи стартували із запізненням у тижні, багато з них виходили з ладу через радіацію, а кожне завдання вимагало унікальної конструкції [19]. Перенесення цього досвіду на українські реалії означає, що інвестиції у ШІ-реагування мають супроводжуватися інвестиціями у стійкість, ремонтпридатність і навчання операторів, і ілюзія миттєвої роботизованої панацеї є не менш небезпечною, ніж відсутність роботів узагалі.

Описана інституційна архітектура стримування становить технологічну рамку, проте без етико-правового виміру вона залишається неповною, бо питання допустимої автономності визначає саму природу людино-машинної взаємодії у критичних ситуаціях. Поняття значущого людського контролю, яке з 2014 року обговорюється у межах Конвенції про конкретні види звичайної зброї, залишається центральним для оцінки допустимості ШІ-рішень, позаяк машина не здатна відстежувати вимоги міжнародного гуманітарного права (розрізнення, пропорційність, воєнну необхідність) [16]. Для ХБРЯ-домену розмежування летальних автономних систем і систем підтримки рішень є визначальним: перші у критичних функціях лишаються етично неприйнятними, другі допустимі за умови людського нагляду, і питання відповідальності за хибні спрацювання чи пропуск загрози залишається юридично невирішеним. НАТО у Стратегії ШІ 2021 року закріпило шість принципів відповідального використання (законність, відповідальність і підзвітність, простежуваність, надійність, керованість, пом'якшення упередженості) [24], а переглянута Стратегія 2024 року додала увагу до генеративного ШІ та протидії зловмисному застосуванню [25]. Видається обґрунтованим стверджувати, що ці принципи утворюють необхідну, але недостатню умову: без механізму примусового виконання вони залишаються деклараціями доброї волі.

Ризик зловживання генеративними моделями перетворює стримування на двостороннє завдання з одночасною захисною й наступальною динамікою, і саме ця дуальність формує найглибший філософський виклик інтеграції ШІ. Модель

MegaSyn для пошуку ліків після інвертування цільової функції менш ніж за шість годин обчислень на звичайному персональному комп'ютері згенерувала 40 000 молекул, включно з нервово-паралітичним агентом VX та новими сполуками з прогнозованою вищою токсичністю [17]. Наукова спільнота відповідає розробкою методів оцінки двоїстих спроможностей біологічних ШІ-моделей до їх розгортання, спираючись на десятиліття досвіду управління ризиками подвійного використання в науках про життя [18], а конвергенція ШІ, CRISPR та синтетичної біології посилює як захисний потенціал, так і загрози [14]. Висновок із аналізу двоїстого потенціалу є дискомфортним, проте неунікним: інтеграція ШІ у стримування ХБРЯ-загроз одночасно знижує одні ризики й підвищує інші, і збалансоване управління має визнавати обидві динаміки, не вдаючись ані до технологічного оптимізму, ані до технофобії, а натомість формуючи інституційні запобіжники, здатні тримати технологію в межах суспільно прийняттого ризику.

Український контекст робить абстрактні дилеми двоїстого використання болісно конкретними і водночас створює унікальне вікно можливостей, адже масив ХБРЯ-даних воєнного часу, яким Україна вже володіє, не має аналогів у жодній іншій країні. Нормативною основою захисту слугують Кодекс цивільного захисту та Єдина державна система цивільного захисту, керована ДСНС, проте рівень інтеграції ШІ-технологій у національну систему залишається початковим і фрагментарним, а біобезпекову систему Україна зміцнила за підтримки міжнародних партнерів на тлі російської дезінформації [20]. Бібліометричний аналіз підтверджує усвідомлення проблеми академічною спільнотою: штучний інтелект і цивільний захист виокремлюються як тематичні вузли [21], огляд ШІ в ядерній енергетиці окреслює перспективні напрями моніторингу та прогнозування [22], а українські науковці досліджують нейромережеві методи прогнозування надзвичайних ситуацій [23].

Таблиця 2

## Етапи інтеграції ШІ у національну систему ХБРЯ-стримування України

| Параметр          | Етап 1: програмні рішення (6–12 міс.)  | Етап 2: архітектура даних (2–4 роки)   | Етап 3: робототехніка (5+ років)  |
|-------------------|--|--|---|
| Ключові дії       | Розгортання OSINT-аналітики (EPIWATCH, SaveEcoBot) на наявних сенсорних мережах; створення єдиної платформи збору ХБРЯ-даних | Інтероперабельна база даних, сумісна з IAEA IRMIS; ML-прискорення моделей дисперсії для ДСНС; сертифікація за принципами ШІ НАТО | Модульні роботизовані платформи для дезактивації з урахуванням уроків Фукусіми                                |
| Ресурси           | Мінімальні: відкрите ПЗ, хмарна інфраструктура, існуючий персонал ДСНС   | Середні: ліцензування, інтеграція з міжнародними системами, навчання 200+ операторів   | Високі: НДДКР, серійне виробництво або імпорт, полігонні випробування   |
| Бенчмарк переходу | Стабільне функціонування єдиної бази ХБРЯ-даних із покриттям щонайменше 80 % території                                       | Польова точність детекції > 90 %; успішне проходження аудиту НАТО  | Визначається безпековою ситуацією та ресурсною спроможністю   |
| Ризики            | Фрагментарність даних, відсутність єдиного формату   | Кіберзагрози інтегрованим системам; бюрократичні бар'єри сертифікації; залежність від донорського фінансування                   | Неготовність промислової бази; етичні застереження щодо автономності рішень; невизначеність правового статусу |

*Джерело: розроблено автором*

Євроінтеграція задає нормативний і ресурсний каркас для побудови національної стратегії, без якого поетапний план залишається академічною вправою. Адаптація до Плану дій ЄС із ХБРЯ-безпеки та механізму rescEU (зі стратегічним запасом захисного спорядження, засобів детекції та медичних контрзаходів) відкриває доступ до фінансування й технологій, яких бракує національній системі [26], а стандарти НАТО та принципи відповідального використання ШІ задають технічні й етичні орієнтири [24; 25]. Трьохетапний підхід дозволяє отримувати віддачу від ШІ-інвестицій уже на першому кроці, не чекаючи повної розбудови інфраструктури, і водночас нарощувати спроможності відповідно до інституційної зрілості та доступних коштів. Якщо



припустити, що Україна послідовно реалізує всі три етапи, за горизонтом п'яти-семи років країна зможе перетворити трагічний досвід війни на джерело глобальної експертизи у галузі ШІ-інтегрованого ХБРЯ-стримування, і цей потенціал є, можливо, єдиним позитивним наслідком випробувань, через які вона проходить.

**Висновки.** Проведений аналіз засвідчує, що інтеграція штучного інтелекту у систему стримування ХБРЯ-ризиків є не питанням вибору, а об'єктивною необхідністю, зумовленою якісною трансформацією загроз. Хімічні інциденти на лінії зіткнення, радіаційні ризики навколо Запорізької АЕС та зруйнована біобезпекова інфраструктура формують комплексний виклик, відповіді на який традиційні системи моніторингу та реагування вже не спроможні.

Ефективність ШІ-систем є реальною та вимірною: точність ідентифікації хімічних агентів сягає 96–99 відсотків, радіонуклідної ідентифікації перевищує 95 відсотків, а прискорення моделювання атмосферної дисперсії скорочує час прогнозу з годин до мілісекунд. Водночас показники є умовними та залежать від якості даних, інтероперабельної архітектури й підготовленості персоналу, що в бойових умовах не гарантовано.

Авторська позиція полягає у необхідності агресивного розгортання ШІ в аналітичних і детекційних функціях (де ціна помилки вимірюється хибною тривоною) та водночас вкрай стриманого підходу до автономних рішень (де ціна помилки є незворотною). Концепція значущого людського контролю має бути покладена в основу будь-якої системи ШІ-підтримки рішень у ХБРЯ-домени, а летальні автономні рішення у критичних функціях залишаються етично неприйнятними.

Ризик подвійного використання генеративних моделей (здатність генерувати молекули бойових отруйних речовин за лічені години обчислень) робить стримування двостороннім завданням: технологія, яка захищає, водночас здатна озброювати. Збалансоване управління має визнавати обидві динаміки,



впроваджуючи скринінг моделей до їх розгортання та законодавчо закріплюючи відповідальність за зловживання.

Україна перебуває у парадоксальному становищі: вона має найбагатший у світі сучасний масив ХБРЯ-даних воєнного часу, проте найслабші ресурси для його алгоритмічної обробки. Стратегічним пріоритетом має стати не імітація дорогих автономних платформ провідних армій, а розбудова дешевих, стійких, людиноцентричних систем підтримки рішень, інтегрованих із сенсорними мережами та міжнародними базами даних.

Поетапна стратегія (від низькоресурсних програмних рішень на наявних мережах через інтероперабельну архітектуру даних до автономної робототехніки) дозволяє отримувати віддачу від інвестицій уже на першому кроці та нарощувати спроможності відповідно до інституційної зрілості. Адаптація до стандартів ЄС та НАТО забезпечує доступ до ресурсів і задає етичні орієнтири.

Стимування ХБРЯ-ризиків у XXI столітті визначатиметься не тим, наскільки автономними є машини, а тим, наскільки розумно суспільство утримує над ними контроль. Саме в цій площині технологічна спроможність перетинається з правовою відповідальністю, а ефективність алгоритмів перевіряється етичною зрілістю тих, хто їх розгортає.

### **Список використаних джерел**

1. Organisation for the Prohibition of Chemical Weapons. Report of the OPCW Technical Assistance Visit to Ukraine (TAV/04/24). The Hague, 2024. URL: <https://www.opcw.org/media-centre/news/2024/11/opcw-issues-report-its-technical-assistance-visit-ukraine-following>

2. U.S. Accuses Russia of Chemical Weapons Use in Ukraine. Arms Control Today. 2024. URL: <https://www.armscontrol.org/act/2024-06/news/us-accuses-russia-chemical-weapons-use-ukraine>

3. IAEA concern at damage to Zaporizhzhia radiation monitoring station. World Nuclear News. 2024. URL: <https://world-nuclear-news.org/Articles/IAEA-concern-at-damage-to-Zaporizhzhia-radiation-m>
4. Report on the Impact of AI on Chemical, Biological, Radiological, and Nuclear Threats. U.S. Department of Homeland Security. 2024. URL: [https://www.dhs.gov/sites/default/files/2024-06/24\\_0620\\_cwmd-dhs-cbrn-ai-eo-report-04262024-public-release.pdf](https://www.dhs.gov/sites/default/files/2024-06/24_0620_cwmd-dhs-cbrn-ai-eo-report-04262024-public-release.pdf)
5. Harnessing AI to Move from Threat to Threat Reduction. Stimson Center. 2025. URL: <https://www.stimson.org/2026/harnessing-ai-to-move-from-threat-to-threat-reduction/>
6. Machine learning-based decision support framework for CBRN protection. *Heliyon*. 2024. Vol. 10, No. 4. e25745. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10884456/>
7. Hyperspectral imaging for chemicals identification: a human-inspired machine learning approach. *Scientific Reports*. 2022. Vol. 12. 17389. DOI: <https://doi.org/10.1038/s41598-022-22468-7>
8. Liberatore N., Felizzato G., Mengali S., Viola R., Romolo F. S. A novel signal processing approach enabled by machine learning for the detection and identification of chemical warfare agent simulants using a GC-QEPAS system. *Forensic Sciences Research*. 2025. Vol. 10, No. 3. owaf002. DOI: <https://doi.org/10.1093/fsr/owaf002>
9. Machine learning application in NaI(Tl) gamma-ray spectroscopy for radionuclide identification: a systematic review. *Radiation Medicine and Protection*. 2025. DOI: <https://doi.org/10.1016/j.radmp.2025.09.009>
10. Barzilov A., Kazemeini M. Unmanned Aerial System Integrated Sensor for Remote Gamma and Neutron Monitoring. *Sensors*. 2020. Vol. 20, No. 19. 5529. DOI: <https://doi.org/10.3390/s20195529>
11. Chavarria-Miró G., Anfruns-Estrada E., Martínez-Velázquez A. et al. Time evolution of SARS-CoV-2 in wastewater during the first pandemic wave of COVID-

19. *Applied and Environmental Microbiology*. 2021. Vol. 87, No. 21. e00425-21. DOI: <https://doi.org/10.1128/AEM.00425-21>

12. Artificial intelligence in early warning systems for infectious disease surveillance: a systematic review. *Frontiers in Public Health*. 2025. Vol. 13. 1609615. DOI: <https://doi.org/10.3389/fpubh.2025.1609615>

13. Kannan A., Chen R., Akhtar Z., Sutton B., Quigley A., Morris M. J., MacIntyre C. R. Use of Open-Source Epidemic Intelligence for Infectious Disease Outbreaks, Ukraine, 2022. *Emerging Infectious Diseases*. 2024. Vol. 30, No. 9. P. 1771–1779. DOI: <https://doi.org/10.3201/eid3009.240082>

14. From pandemics to preparedness: harnessing AI, CRISPR, and synthetic biology to counter biosecurity threats. *Frontiers in Public Health*. 2025. Vol. 13. 1711344. DOI: <https://doi.org/10.3389/fpubh.2025.1711344>

15. Mendil M., Leirens S., Armand P., Duchenne C. Hazardous atmospheric dispersion in urban areas: a Deep Learning approach for emergency pollution forecast. *Environmental Modelling & Software*. 2022. Vol. 152. 105338. DOI: <https://doi.org/10.1016/j.envsoft.2022.105338>

16. Amoroso D., Tamburrini G. Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues. *Current Robotics Reports*. 2020. Vol. 1. P. 187–194. DOI: <https://doi.org/10.1007/s43154-020-00024-3>

17. Urbina F., Lentzos F., Invernizzi C., Ekins S. Dual use of artificial-intelligence-powered drug discovery. *Nature Machine Intelligence*. 2022. Vol. 4, No. 3. P. 189–191. DOI: <https://doi.org/10.1038/s42256-022-00465-9>

18. Dual-use capabilities of concern of biological AI models. *PLOS ONE*. 2025. Vol. 20, No. 5. e0303266. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12061118/>

19. The Use of Robots to Respond to Nuclear Accidents: Applying the Lessons of the Past to the Fukushima Daiichi Nuclear Power Station. *Annual Review of Control, Robotics, and Autonomous Systems*. 2021. Vol. 4. P. 681–710. DOI: <https://doi.org/10.1146/annurev-control-071420-100248>



20. Understanding Biosafety and Biosecurity in Ukraine. *Health Security*. 2022. Vol. 20, No. 5. DOI: <https://doi.org/10.1089/hs.2022.0095>
21. Кубатко О. В., Озімс С. Ч., Вороненко В. І., Коноваленко І. С. Штучний інтелект для підвищення ефективності бізнесу та цивільного захисту. *Економічний простір*. 2024. № 190. С. 141–147. DOI: <https://doi.org/10.32782/2224-6282/190-27>
22. Golyonko O., Ulych I., Ogir O., Dybach O. Штучний інтелект у ядерній енергетиці: огляд перспективних напрямів та особливості застосування. *Ядерна та радіаційна безпека*. 2025. № 2(106). С. 66–79. DOI: [https://doi.org/10.32918/nrs.2025.2\(106\).07](https://doi.org/10.32918/nrs.2025.2(106).07)
23. Методи прогнозування для вивчення та попередження надзвичайних природних явищ. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2023. № 4. DOI: <https://doi.org/10.32782/IT/2023-4-2>
24. Summary of the NATO Artificial Intelligence Strategy. North Atlantic Treaty Organization. 2021. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy>
25. Summary of NATO's Revised Artificial Intelligence Strategy. North Atlantic Treaty Organization. 2024. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
26. European Commission. EU strategic reserves for CBRN emergencies (rescEU). 2022. URL: <https://reliefweb.int/report/world/eu-develops-strategic-reserves-chemical-biological-and-radio-nuclear-emergencies>