УДК 351.86:327.56

ORCID ID: https://orcid.org/0000-0002-0303-7453
Білоус С. П., Черкаський національний університет імені Богдана Хмельницького

ORCID ID: https://orcid.org/0000-0002-0335-3077
Самойленко Л. Я., Черкаський національний університет імені Богдана Хмельницького

ORCID ID: https://orcid.org/0009-0003-7903-9687
Бандунко Л. М., Черкаський національний університет імені Богдана Хмельницького

ІННОВАЦІЙНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ

Стаття присвячена дослідженню інноваційних підходів до забезпечення національної безпеки на основі міжнародного досвіду. Актуальність теми обумовлена сучасними глобальними викликами, зокрема кіберзагрозами, гібридними війнами та необхідністю захисту критичної інфраструктури. У дослідженні розглянуто передові технології, такі як штучний інтелект, аналіз великих даних, блокчейн, безпілотні системи, та їх застосування у сфері безпеки. Проаналізовано досвід провідних країн світу — США, Ізраїлю, Китаю, — що активно впроваджують інноваційні стратегії для нейтралізації загроз. США є одним із найбільш інноваційних лідерів у галузі кібербезпеки та застосування штучного інтелекту (ШІ) для прогнозування загроз. Окрім того, США активно розробляють безпілотні літальні апарати, які застосовуються для моніторингу та захисту критичної інфраструктури, а також для розвідувальних місій. Ізраїль є світовим лідером у розробці програмного забезпечення для кіберзахисту, і багато ізраїльських компаній працюють над створенням передових рішень для захисту державних та приватних мереж. Важливо зазначити, що завдяки тісній співпраці між урядом та приватним сектором, Ізраїль створив ефективну екосистему захисту від загроз. На основі цього запропоновано рекомендації щодо адаптації успішних практик до українських реалій з метою розробки ефективної національної стратегії безпеки. Китай активно впроваджує штучний інтелект (ШІ) та технології розпізнавання обличчя для забезпечення громадської безпеки. У поєднанні з жорстким державним контролем та регуляціями, ці технологічні рішення допомагають Китаю здійснювати ефективне управління національною безпекою та забезпечувати стабільність всередині країни. Визначено, що для України важливим є не лише вивчення та адаптація цих інноваційних підходів, але й активне залучення до міжнародної співпраці у сфері безпеки, що дозволить отримати доступ до передових технологій, знань та практик.

***Ключові слова**: національна безпека, державне управління, загрози, ризики, антикризове управління, міжнародний досвід*

Актуальність теми. Актуальність дослідження теми зумовлена зростаючою складністю та динамікою сучасних загроз, які виходять за рамки традиційних безпекових викликів. У сучасному глобалізованому світі питання національної безпеки охоплюють не лише військові аспекти, але й економічну стабільність, кібербезпеку, захист критичної інфраструктури, інформаційну безпеку та стійкість до гібридних загроз. Це вимагає нових підходів та рішень, які базуються на інтеграції передових технологій, цифровізації та ефективної міждержавної співпраці.

Сучасні світові тенденції демонструють активне застосування інноваційних технологій, таких як штучний інтелект, аналіз великих даних, блокчейн, безпілотні системи та інтернет речей, у забезпеченні національної безпеки. Провідні країни світу розробляють і впроваджують новітні

стратегії, що дозволяють швидко реагувати на загрози, прогнозувати їх розвиток та мінімізувати можливі ризики. З огляду на це, вивчення міжнародного досвіду впровадження інноваційних підходів до безпеки є вкрай важливим для розробки ефективної національної стратегії України, що дозволить не лише підвищити рівень захищеності держави, але й зміцнити її позиції у міжнародному безпековому середовищі.

Дослідження актуальне й тим, що інтеграція новітніх технологій у безпековий сектор відкриває можливості для зміцнення потенціалу обороноздатності держави, підвищення ефективності управління кризовими ситуаціями та оптимізації роботи державних структур. Таким чином, аналіз міжнародного досвіду, його адаптація та впровадження в українських реаліях сприятиме розвитку комплексної та стійкої системи національної безпеки, здатної протистояти сучасним викликам.

Метою статті є вивчення та систематизація інноваційних підходів до забезпечення національної безпеки на основі міжнародного досвіду, а також визначення перспектив їх впровадження в українській практиці.

Огляд наявних досліджень і публікацій. свідчить про значний інтерес українських та зарубіжних науковців до тематики інноваційних підходів у забезпеченні національної безпеки. Основну увагу дослідники приділяють питанням впровадження новітніх технологій, розвитку кібербезпеки, створенню систем реагування на гібридні загрози, а також оптимізації державного управління у цій сфері.

Серед українських науковців варто відзначити роботи О. Литвиненка, який у своїх дослідженнях акцентує увагу на необхідності комплексного підходу до захисту критичної інфраструктури та ролі сучасних інформаційних технологій у забезпеченні національної безпеки. Він підкреслює важливість розвитку національної стратегії кібербезпеки, яка б враховувала найкращі міжнародні практики та адаптувала їх до українських реалій [1, 2].

Іншою вагомою постаттю є О. Воронін, який досліджує аспекти кібербезпеки та інформаційної безпеки, наголошуючи на важливості створення національної екосистеми захисту від кіберзагроз. У своїх працях О. Воронін аналізує міжнародний досвід щодо формування кіберкоманд та співпраці держави з приватним сектором у сфері безпеки [3].

Дослідження І. Романенко зосереджені на адаптації інноваційних технологій у сфері управління кризовими ситуаціями. Вона досліджує роль штучного інтелекту, аналізу великих даних та безпілотних систем у процесі прогнозування загроз і прийняття рішень під час кризових ситуацій. Її роботи підкреслюють важливість оперативності та точності у реагуванні на загрози, що стає можливим завдяки впровадженню сучасних технологічних рішень [4].

Значний внесок у розвиток теоретичних основ інноваційних підходів до забезпечення національної безпеки зробив також В. Горбулін, який досліджує питання гібридної війни та асиметричних загроз. У своїх працях він акцентує на необхідності інтеграції багатокомпонентних систем безпеки, що включають як традиційні оборонні заходи, так і новітні технологічні інструменти [5].

Таким чином, роботи українських науковців охоплюють широкий спектр питань, пов’язаних з інноваційними підходами до забезпечення національної безпеки, зокрема кібербезпеку, управління кризовими ситуаціями, захист критичної інфраструктури та аналіз гібридних загроз. Вивчення та адаптація міжнародного досвіду, що здійснюється у їхніх дослідженнях, є важливим кроком для підвищення ефективності української системи національної безпеки.

Виклад основного матеріалу. Українські науковці пропонують різноманітні визначення національної безпеки, кожне з яких відображає певний аспект цього багатогранного поняття. Проаналізуємо декілька з них:

О. Литвиненко визначає національну безпеку як: «комплексну систему заходів, спрямованих на захист життєво важливих інтересів держави, суспільства та особистості від зовнішніх і внутрішніх загроз» [1]. Він підкреслює важливість створення умов для стійкого розвитку держави, забезпечення її суверенітету, територіальної цілісності та незалежності. Його підхід акцентує на багатошаровості безпеки, де враховуються як традиційні військові аспекти, так і політичні, економічні та інформаційні компоненти.

В. Горбулін розглядає національну безпеку як: «здатність держави ефективно протидіяти всім видам загроз і викликів, зберігаючи свою політичну, економічну, соціальну та культурну цілісність» [5]. Його визначення зосереджене на понятті стійкості та здатності держави адаптуватися до нових загроз, включаючи гібридні та асиметричні виклики, що є особливо актуальним у контексті сучасної

глобальної нестабільності.

І. Романенко пропонує розглядати національну безпеку через призму соціального благополуччя, вказуючи на те, що вона полягає в захисті населення та забезпеченні стабільного розвитку суспільства. Її підхід підкреслює роль держави у створенні умов для безпечного та стійкого розвитку громадян, де економічна та соціальна стабільність стають ключовими елементами системи національної безпеки [4].

О. Воронін вказує на багатовимірність національної безпеки, охоплюючи у своєму визначенні як фізичну захищеність країни, так і захист її інформаційного простору, економічної стабільності та екологічного балансу. Він стверджує, що сучасні загрози вимагають інтегрованого підходу, де традиційні та нетрадиційні форми безпеки поєднуються для забезпечення комплексного захисту національних інтересів [3].

Таким чином, українські науковці сходяться на думці, що національна безпека є багатокомпонентною категорією, яка охоплює широкий спектр сфер: від військової оборони до інформаційного та соціально-економічного захисту. Кожне з цих визначень підкреслює різні аспекти цієї складної системи, що відповідає сучасним умовам глобальних викликів та загроз.

Питання інноваційних підходів до забезпечення національної безпеки є надзвичайно актуальним у сучасному світі, де швидкі технологічні зміни, глобалізація та гібридні загрози створюють нові виклики для держав. Традиційні методи захисту, орієнтовані на військову силу та дипломатію, більше не здатні повністю гарантувати національну безпеку. Сучасні реалії вимагають інтеграції новітніх технологій, а також використання креативних та адаптивних стратегій, що дозволяють державам реагувати на загрози ефективніше та швидше.

Одним із ключових елементів інноваційних підходів до забезпечення національної безпеки є використання передових технологій, таких як штучний інтелект (ШІ), аналіз великих даних (Big Data), блокчейн, безпілотні літальні апарати (БПЛА), інтернет речей (IoT), кібербезпека та квантові обчислення. Країни, що активно впроваджують ці технології, можуть значно підвищити свою спроможність до виявлення, запобігання та нейтралізації різних загроз [6]. Наприклад штучний інтелект використовується для прогнозування загроз, аналізу великих масивів даних та автоматизації процесів виявлення кіберзагроз. Це дозволяє значно скоротити час реагування на атаки та знижує можливість людської помилки. Блокчейн забезпечує прозорість та захист від маніпуляцій даними, що особливо важливо у контексті захисту критичної інфраструктури, фінансових операцій та безпеки в електронному урядуванні. Безпілотні системи застосовуються для моніторингу кордонів, проведення розвідувальних операцій, а також для забезпечення безпеки критичних об’єктів у важкодоступних районах [7].

Провідні країни світу активно застосовують новітні технології для підвищення національної безпеки. США, Ізраїль та Китай є провідними державами, що активно застосовують інноваційні технології для забезпечення національної безпеки, кожна з яких розробляє та впроваджує свої підходи до вирішення сучасних загроз.

США є одним із найбільш інноваційних лідерів у галузі кібербезпеки та застосування штучного інтелекту (ШІ) для прогнозування загроз. Американські інвестиції в національну безпеку включають розвиток передових автоматизованих систем, здатних ефективно ідентифікувати та нейтралізувати кіберзагрози. Пентагон виділяє значні ресурси на створення розвідки на основі великих даних, що допомагає виявляти патерни поведінки та попереджати потенційні атаки. Окрім того, США активно розробляють безпілотні літальні апарати, які застосовуються для моніторингу та захисту критичної інфраструктури, а також для розвідувальних місій. Важливою складовою національної безпеки стали спеціальні кібервійська, які забезпечують постійний моніторинг кіберпростору, виявлення загроз та захист від можливих атак. Це дозволяє США підтримувати високий рівень кіберстійкості та оперативно реагувати на небезпеки, пов'язані з кіберзлочинністю та кібертероризмом [8].

Ізраїль має успішний досвід застосування інноваційних технологій для захисту національної безпеки, особливо у сфері кібербезпеки та використання безпілотних літальних апаратів. Країна є світовим лідером у розробці програмного забезпечення для кіберзахисту, і багато ізраїльських компаній працюють над створенням передових рішень для захисту державних та приватних мереж. Ізраїльські безпілотники відомі своєю технологічною досконалістю, і вони використовуються як для оборонних, так і для розвідувальних цілей. Важливо зазначити, що завдяки тісній співпраці між урядом та приватним сектором, Ізраїль створив ефективну екосистему захисту від загроз. Країна також є одним із провідних експортерів технологій у сфері безпеки, що сприяє розвитку глобальних стандартів кібербезпеки та інтеграції інноваційних технологій у різних країнах світу [9].

Китай активно впроваджує штучний інтелект (ШІ) та технології розпізнавання обличчя для забезпечення громадської безпеки. Такі системи дозволяють китайському уряду здійснювати моніторинг за масовими зібраннями, відстежувати активність громадян та запобігати потенційним заворушенням. Аналітика великих даних у поєднанні зі штучним інтелектом дозволяє підвищити ефективність боротьби з тероризмом та злочинністю, оскільки вона дозволяє швидко і точно обробляти інформацію з багатьох джерел. Окрім того, Китай активно інвестує у розвиток власних технологій кіберзахисту, що є частиною ширшої стратегії національної безпеки, спрямованої на захист критичної інфраструктури, військових об'єктів та інформаційних ресурсів країни. У поєднанні з жорстким державним контролем та регуляціями, ці технологічні рішення допомагають Китаю здійснювати ефективне управління національною безпекою та забезпечувати стабільність всередині країни [10].

Таким чином, ці три країни демонструють різні підходи до використання інноваційних технологій у забезпеченні національної безпеки, зокрема в сферах кіберзахисту, штучного інтелекту, аналітики великих даних та безпілотних технологій. Кожна з них має свої унікальні переваги та специфіку, що може стати основою для подальшого впровадження подібних рішень в інших країнах.

Україна знаходиться в особливо складних умовах через необхідність протистояння військовій агресії, кіберзагрозам та гібридним викликам. Серед ключових напрямів, які потребують особливої уваги, виділяють розвиток кібербезпеки, інтеграцію цифрових технологій в управління кризовими ситуаціями та посилення співпраці між державою та приватним сектором. Кожен із цих напрямів має потенціал для забезпечення стійкості та захищеності країни від нових типів загроз.

Розвиток кібербезпеки є однією з пріоритетних сфер у забезпеченні національної безпеки України. Сучасні кіберзагрози стають дедалі складнішими, що вимагає розробки потужної стратегії кіберзахисту, яка охоплюватиме не лише традиційні підходи до безпеки, а й інноваційні рішення на основі штучного інтелекту (ШІ). Впровадження систем ШІ дозволяє аналізувати великі обсяги даних у режимі реального часу, виявляти аномалії в мережевому трафіку та прогнозувати потенційні атаки ще до того, як вони стануть загрозою. Це дає можливість знижувати ризики кібератак та оперативно реагувати на них. Окрім того, Україні необхідно активно співпрацювати з міжнародними партнерами, аби отримати доступ до найкращих технологічних рішень і практик у сфері кібербезпеки. Це може включати як навчальні програми та обмін досвідом, так і інтеграцію передових західних технологій у національні системи безпеки. Успішні приклади співпраці у сфері кібербезпеки між державою та приватними технологічними компаніями вже існують у багатьох країнах, і Україна може скористатися їхнім досвідом для побудови власної стратегії захисту [11].

Інтеграція цифрових технологій в управління кризовими ситуаціями є ще одним важливим напрямом, що сприяє підвищенню національної безпеки. Використання ШІ та аналітики великих даних дозволяє швидше та ефективніше реагувати на надзвичайні ситуації, забезпечуючи своєчасне надання допомоги постраждалим і зниження втрат. Важливо впроваджувати системи моніторингу та попередження про можливі катастрофи, які здатні збирати інформацію з різних джерел і прогнозувати розвиток подій на основі аналізу даних. Такі системи можуть передбачати природні катастрофи, техногенні аварії чи інші види кризових ситуацій, надаючи інформацію для швидкого реагування. Наприклад, у випадку пожежі або повені автоматизовані алгоритми можуть визначити оптимальні маршрути для евакуації та координації рятувальних служб. Також важливою є розробка національних платформ, які об’єднуватимуть дані з різних державних та приватних джерел для оперативного аналізу та реагування на загрози. Подібні технології вже успішно впроваджуються у багатьох країнах, де завдяки системам ШІ вдається знижувати економічні втрати від стихійних лих і катастроф [12].

Посилення співпраці між державою та приватним сектором має ключове значення для ефективного впровадження інновацій у сфері безпеки. Розвиток нових технологій часто залежить від приватних компаній, що спеціалізуються на розробці безпекових рішень, тому держава має активно залучати їх до спільних проєктів. Це може включати створення сприятливих умов для діяльності технологічних стартапів, які працюють у сфері кібербезпеки, розробки безпілотних систем, аналізу даних та штучного інтелекту. Для цього важливо запроваджувати спеціальні програми підтримки таких стартапів, надавати податкові пільги та стимулювати інвестиції в розробку інноваційних технологій. Співпраця з приватним сектором також дозволяє державі отримати доступ до передових розробок і використовувати їх для підвищення рівня національної безпеки. Такі партнерства можуть включати участь у науково-дослідницьких проєктах, створення центрів інновацій, де урядові установи та технологічні компанії працюватимуть разом над розробкою рішень для забезпечення

безпеки країни [13].

Висновки. Отже, впровадження інноваційних підходів до забезпечення національної безпеки потребує комплексного підходу, що включає розвиток кібербезпеки, інтеграцію сучасних технологій в управління кризовими ситуаціями та активну співпрацю між державою і приватним сектором. Україна має значний потенціал для розвитку цих напрямів, і досвід інших країн може стати важливим джерелом для створення ефективної національної системи безпеки.

Сучасні загрози національній безпеці включають гібридні атаки, які поєднують військові, економічні, інформаційні та кібернетичні елементи. У цьому контексті інноваційні підходи повинні враховувати необхідність протидії дезінформації, забезпечення інформаційної безпеки та створення систем стійкості до гібридних загроз [14].

Застосування аналітики великих даних дозволяє прогнозувати інформаційні атаки, розпізнавати фальшиві новини та швидко реагувати на спроби маніпуляції громадською думкою. Цей підхід активно використовується у США та країнах ЄС, де створюються спеціальні підрозділи для боротьби з дезінформацією, а також розробляються стандарти інформаційної стійкості.

Бібліографічний список:

1. Литвиненко О.М. Комплексний підхід до захисту критичної інфраструктури як основа національної безпеки: виклики та перспективи. *Збірник наукових праць Національного інституту стратегічних досліджень*. 2021. № 2. С. 12–22.

2. Литвиненко О.М. Інформаційні війни та стратегічні комунікації у контексті національної безпеки: сучасні виклики та рішення. *Український журнал інформаційної безпеки*. 2023. № 3. С. 34–41.

3. Воронін О.А. Кібербезпека та інформаційна безпека: створення національної екосистеми захисту від кіберзагроз. *Український журнал інформаційної безпеки*. 2023. № 1. С. 29–38.

4. Романенко І.О. Штучний інтелект і аналіз великих даних у кризовому управлінні: перспективи впровадження. *Журнал кризового управління та безпеки*. 2022. № 2. С. 62–71.

5. Горбулін В.П. Гібридна війна та асиметричні загрози: виклики для національної безпеки. *Стратегічні пріоритети*. 2021. № 3. С. 15–26.

6. Український інститут стратегічних досліджень. Інноваційні технології в системі забезпечення національної безпеки: аналіз міжнародного досвіду та рекомендації для України. Аналітичний звіт. Київ: УІСД, 2021. 47 с.

7. Романенко І.О. Безпілотні системи у процесі прогнозування загроз та управління кризовими ситуаціями. *Технології управління безпекою*. 2023. № 1. С. 89–98.

8. Cybersecurity & Infrastructure Security Agency. Strategic Plan 2021–2025: Building Resilient Systems for National Security. Washington D.C.: CISA, 2021. 56 p.

9. Гуменюк О.В., Василенко М.С. Сучасні інформаційно-комунікаційні технології в забезпеченні національної безпеки: зарубіжний досвід та українські перспективи. *Науковий вісник Національної академії внутрішніх справ*. 2022. № 3. С. 52–60.

10. Brown J. Smith A. The Role of Artificial Intelligence in National Security: Current Trends and Future Directions. *Journal of Security Studies*. 2021. Vol. 12, No. 4. Pp. 233–245.

11. Литвиненко О. М. Національна стратегія кібербезпеки: адаптація міжнародного досвіду до українських реалій. *Вісник Київського національного університету імені Тараса Шевченка*. 2022. № 4. С. 75–84.

12. Горбулін В.П. Інтеграція багатокомпонентних систем безпеки: сучасні технологічні інструменти та традиційні оборонні заходи. *Науковий вісник Національного університету оборони України*. 2022. № 5. С. 34–45.

13. Воронін О.А. Співпраця держави з приватним сектором у сфері кібербезпеки: міжнародний досвід та українські реалії. *Інформаційні технології та безпека*. 2021. № 3. С. 41–50.

14. Ковальчук І.П. Протидія гібридним загрозам: інноваційні підходи до забезпечення національної безпеки в Україні. *Вісник Київського національного університету імені Тараса Шевченка*. 2023. № 2. С. 98–105.

References:

1. Lytvynenko, O.M. (2021), “A comprehensive approach to the protection of critical infrastructure as the basis of national security: challenges and prospects”, *Zbirnyk naukovykh prats Natsionalnoho instytutu stratehichnykh doslidzhen*, no 2, pp. 12–22.

2. Lytvynenko, O.M. (2023), “Information warfare and strategic communications in the context of national security: contemporary challenges and solutions”, *Ukrayinskyy zhurnal informatsiynoyi bezpeky*, no 3, pp. 34–41.

3. Voronin, O.A. (2023), “Cyber security and information security: creating a national cyber threat protection

ecosystem", *Ukrayinskyy zhurnal informatsiynoyi bezpeky*, no 1, pp. 29–38.

4. Romanenko, I.O. (2022), "Artificial intelligence and big data analysis in crisis management: prospects for implementation", *Zhurnal kryzovoho upravlinnya ta bezpeky*, no 2, pp. 62–71.

5. Horbulin, V.P. (2021), "Hybrid warfare and asymmetric threats: challenges for national security", *Stratehichni priorytety*, no 3, pp. 15–26.

6. Ukrayinskyy instytut stratehichnykh doslidzhen (2021), "Innovative technologies in the national security system: analysis of international experience and recommendations for Ukraine", Analitychnyy zvit, Kyyiv: UISD.

7. Romanenko, I.O. (2023), "Unmanned systems in the process of forecasting threats and managing crisis situations", *Tekhnolohiyi upravlinnya bezpekoyu*, no 1, pp. 89–98.

8. Cybersecurity & Infrastructure Security Agency (2021), "Strategic Plan 2021–2025: Building Resilient Systems for National Security", Washington D.C.: CISA.

9. Humenyuk, O.V., and Vasylenko, M.S. (2022), "Modern information and communication technologies in ensuring national security: foreign experience and Ukrainian perspectives", *Naukovyy visnyk Natsionalnoyi akademiyi vnutrishnikh sprav*, no 3, pp. 52–60.

10. Brown, J., and Smith, A. (2021), "The Role of Artificial Intelligence in National Security: Current Trends and Future Directions", *Journal of Security Studies*, Vol. 12, no. 4, pp. 233–245.

11. Lytvynenko, O. M. (2022), "National cyber security strategy: adaptation of international experience to Ukrainian realities", *Visnyk Kyyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*, no 4, pp. 75–84.

12. Horbulin, V.P. (2022), "Integration of multi-component security systems: modern technological tools and traditional defensive measures", *Naukovyy visnyk Natsionalnoho universytetu oborony Ukrayiny*, no 5, pp. 34–45.

13. Voronin, O.A. (2021), "State cooperation with the private sector in the field of cyber security: international experience and Ukrainian realities", *Informatsiyni tekhnolohiyi ta bezpeka*, no 3, pp. 41–50.

14. Kovalchuk, I.P. (2023), "Countering hybrid threats: innovative approaches to ensuring national security in Ukraine", *Visnyk Kyyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*, no 2, pp. 98–105.

Bilous S., Samoilenko L., Bandunko L. Innovative approaches to ensuring national security: international experience and perspectives of implementation

The article highlights the increasing complexity of modern threats, extending beyond traditional military challenges to include economic stability, cybersecurity, critical infrastructure protection, and resilience to hybrid threats. The growing interconnectivity and digitalization of the global environment necessitate new security strategies that leverage advanced technologies and international cooperation. This study emphasizes the significance of integrating innovative technological solutions such as artificial intelligence (AI), big data analytics, blockchain, unmanned systems, and the Internet of Things (IoT) into national security frameworks. Leading nations worldwide, including the United States, Israel, and China, have been at the forefront of developing and implementing these advanced strategies, enabling them to predict, mitigate, and respond to diverse security threats more effectively. The article provides a comprehensive analysis of international best practices in deploying innovative security measures. It focuses on how advanced technologies enhance threat detection, crisis management, and the protection of critical infrastructure. For instance, AI's role in threat prediction and the automation of cybersecurity measures, the use of blockchain for data transparency and protection, and the deployment of unmanned systems for border surveillance and infrastructure security are explored in detail. The adaptation of these approaches in the Ukrainian context is essential for developing a robust national security strategy that can withstand contemporary global challenges. Ukrainian researchers have also been actively exploring the application of these technologies to improve national defense capabilities. The article reviews the contributions of scholars such as O. Lytvynenko, O. Voronin, and I. Romanenko, who have analyzed various aspects of cybersecurity, crisis management, and hybrid threats. The integration of international experiences, adapted to local conditions, is seen as a crucial step toward enhancing Ukraine's national security framework, ensuring its readiness to address emerging challenges effectively. The study concludes that adopting an innovative, multi-dimensional approach to security, which incorporates traditional defense mechanisms and modern technological tools, is key to building a comprehensive and resilient national security system.

Keywords: *national security, public administration, threats, risks, anti-crisis management, international experience*