УДК 004.8:004.056:004.7
DOI https://doi.org/10.32782/2663-5941/2026.1.2/45

***Супрун О.М.***
https://orcid.org/0000-0002-1196-5655
Державний університет «Київський авіаційний інститут»

***Кравчук Я.Я.***
https://orcid.org/0009-0006-1593-9995

***Бабкова Н.О.***
https://orcid.org/0000-0002-6947-0401
Державний університет «Київський авіаційний інститут»

# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ РОЗПОДІЛЕНИХ МЕРЕЖЕВИХ ІНФРАСТРУКТУР

*Актуальність дослідження зумовлена стрімким зростанням складності розподілених мережевих інфраструктур, активним використанням хмарних і периферійних обчислень, а також ескалацією сучасних кіберзагроз, що характеризуються високою динамічністю, багатовекторністю та здатністю обходити традиційні механізми захисту. За таких умов класичні підходи до кібербезпеки, які ґрунтуються на статичних правилах і сигнатурному аналізі, виявляються недостатньо ефективними, що актуалізує потребу в інтелектуалізації систем безпеки.*

*Метою статті є наукове обґрунтування доцільності та визначення практично орієнтованих напрямів використання штучного інтелекту для підвищення рівня безпеки розподілених мережевих інфраструктур в умовах зростання складності та інтенсивності сучасних кіберзагроз.*

*Методологічне підґрунтя дослідження становлять системний аналіз архітектур розподілених мереж, узагальнення сучасних підходів до гарантування кібербезпеки, порівняльний аналіз методів штучного інтелекту, а також логічне моделювання процесів виявлення загроз і управління інцидентами безпеки. У статті застосовано методи абстрагування, узагальнення та аналітичного синтезу, що дало змогу комплексно оцінити можливості й обмеження інтелектуальних систем захисту.*

*У результаті дослідження встановлено, що використання штучного інтелекту забезпечує інтеграцію аналітичних, детекційних і управлінських функцій у єдиний контур безпеки розподілених мереж. Доведено, що інтелектуальні механізми дають змогу здійснювати проактивне виявлення загроз, кореляцію інцидентів і пріоритизацію ризиків з урахуванням критичності ресурсів і сервісів. Виявлено ключові науково-практичні проблеми застосування штучного інтелекту, що пов'язані з якістю та нестаціонарністю даних, масштабованістю рішень, інтерпретованістю моделей і вразливістю інтелектуальних систем до нових типів атак.*

*У висновках обґрунтовано, що ефективне впровадження штучного інтелекту в системи безпеки розподілених мереж можливе за умови поєднання інтелектуальних засобів із традиційними механізмами захисту, забезпечення керованості даних і збереження експертного контролю над управлінськими рішеннями.*

*Перспективи подальших досліджень пов'язані з розробленням інтерпретованих і стійких до маніпуляцій моделей штучного інтелекту, створенням адаптивних механізмів управління політиками безпеки та формуванням методик комплексного оцінювання ефективності інтелектуальних систем захисту в реальних розподілених мережевих середовищах.*

***Ключові слова:*** *кіберстійкість, управління кіберризиками, інтелектуальні системи захисту, виявлення вторгнень, адаптивні механізми безпеки, розподілені обчислення, управління інцидентами.*

**Постановка проблеми.** Стрімка цифровізація суспільних і виробничих процесів зумовила широке впровадження розподілених мережевих інфраструктур, які є підґрунтям функціонування критично важливих інформаційних систем у сферах державного управління, фінансів, промис-

© Супрун О.М., Кравчук Я.Я., Бабкова Н.О., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

ловості, транспорту та безпеки. Децентралізований характер таких інфраструктур, використання хмарних і периферійних обчислень, мікросервісних архітектур і програмно керованих мереж істотно підвищують їхню масштабованість і гнучкість, водночас ускладнюючи забезпечення цілісності, конфіденційності та доступності даних. Традиційні підходи до кіберзахисту, засновані на статичних правилах, сигнатурному аналізі та централізованому моніторингу, дедалі частіше виявляються недостатньо ефективними в умовах високої динаміки мережевих середовищ, зростання обсягів трафіку та еволюції складних цілеспрямованих кібератак.

Особливої гостроти проблема безпеки розподілених мережевих інфраструктур набуває в умовах зростання кількості атак нульового дня, розподілених відмов в обслуговуванні, внутрішніх загроз і скоординованих багатовекторних впливів, які важко виявляти та локалізувати за допомогою класичних методів. З огляду на це, актуалізується потреба в інтелектуальних механізмах захисту, здатних адаптуватися до змін мережевого середовища, навчатися на великих масивах гетерогенних даних і забезпечувати проактивне виявлення аномалій і загроз у режимі, близькому до реального часу. Саме штучний інтелект (ШІ), зокрема методи машинного навчання, глибинних нейронних мереж та інтелектуального аналізу даних, розглядається як перспективний інструмент подолання обмежень традиційних систем кібербезпеки.

Зазначена проблематика тісно пов'язана з ключовими науковими завданнями сучасної інформатики та кібербезпеки, зокрема з розробленням адаптивних моделей аналізу мережевого трафіку, методів інтелектуального виявлення вторгнень, автоматизованого управління політиками безпеки та інтеграції механізмів захисту в розподілені обчислювальні середовища. Водночас вона безпосередньо корелює з важливими практичними завданнями забезпечення стійкості та безперервності функціонування інформаційних систем, захисту критичної інфраструктури, мінімізації економічних і репутаційних втрат від кібератак і підвищення рівня національної кіберстійкості. У цьому контексті дослідження використання ШІ для підвищення безпеки розподілених мережевих інфраструктур є науково обґрунтованим і практично значущим напрямом, що відповідає сучасним викликам цифрової трансформації та потребам інформаційної безпеки.

**Аналіз останніх досліджень і публікацій.** Огляд наукових публікацій свідчить про послідовне розширення дослідницького фокусу від архітектурних рішень до прикладних механізмів захисту, зорієнтованих на конкретні типи мереж і загроз. Першу групу досліджень становлять роботи, у яких науковці акцентують на архітектурних підходах до побудови інтелектуальних систем безпеки для розподілених середовищ. У своїй праці Ю. Бершчанський (Y. Bershchanskyi) та співавтори обґрунтовують контейнеризований дизайн ШІ-систем у хмарних і кіберфізичних середовищах, що дає змогу підвищити масштабованість, ізоляцію компонентів і стійкість до відмов у розподілених інфраструктурах [1]. Натомість Н. Мустафа (N. Moustafa) пропонує розподілену архітектуру оцінювання ШІ-орієнтованих систем безпеки на рівні периферійних обчислень із використанням спеціалізованих датасетів, що забезпечує адаптацію механізмів захисту до реальних сценаріїв атак в IoT-мережах [2]. Водночас С. С. Алі (S. S. Ali) та співавтори аналізують застосування ШІ в розподілених інтелектуальних енергетичних мережах, підкреслюючи необхідність автономних рішень безпеки в умовах децентралізованого управління та складної топології [3].

Другу групу формують дослідження, зосереджені на алгоритмічних методах виявлення загроз і аномалій у розподілених мережах. У комплексному огляді Х. Ву (H. Wu) та співавторів систематизовано підходи до застосування ШІ для забезпечення безпеки IoT, зокрема методи аналізу мережевого трафіку та поведінкові моделі атак [4]. Так, М. Вакас (M. Waqas) та співавтори досліджують роль ШІ та машинного навчання у безпеці бездротових мереж, наголошуючи на здатності інтелектуальних моделей протидіяти складним багатовекторним атакам у динамічних середовищах [5]. У своєму дослідженні М. Шмітт (M. Schmitt) аналізує застосування ШІ-орієнтованих систем виявлення шкідливого програмного забезпечення та вторгнень у цифрових індустріальних інфраструктурах, де ключовим є оброблення потокових даних у реальному часі [6]. Зокрема А. О. Акінаде (A. O. Akinade) та співавтори пропонують концептуальну модель автоматизації мережевої безпеки на основі ШІ-керованих фреймворків для багатовендорних розподілених середовищ [7].

Третю групу утворюють дослідження, у яких ШІ розглядається як інструмент гарантування безпеки критичних розподілених інфраструктур. Так, С. Ахмед (S. Ahmed) та співавтори аналізують використання ШІ і машинного навчання для

захисту інфраструктур розумних міст, підкреслюючи міждисциплінарний характер проблеми безпеки кіберфізичних систем [8]. Інтеграція аналітики великих даних та інтелектуальних методів машинного навчання дозволяє ефективно виявляти вторгнення в гетерогенних мережах Інтернету речей, як продемонстрували Н. Іслам та співавтори (N. Islam et al.) [9].

Натомість А. А. Хан (A. A. Khan) та співавтори досліджують поєднання штучного інтелекту та блокчейн-технологій для підвищення безпеки розподілених систем управління електромережами й автоматизації енергорозподілу [10]. Водночас А. Чехрі (A. Chehri) та співавтори пропонують підходи до моделювання ризиків безпеки в критичних інфраструктурах smart grid із використанням великих даних і ШІ [11].

Четверту групу становлять прикладні та інженерні дослідження, зорієнтовані на конкретні механізми підвищення безпеки розподілених мереж. У своїй праці С. Поперегняк (S. Poperehnyak) та співавтори демонструють можливість посилення криптографічної стійкості систем безпеки шляхом використання ентропії довкіллєвих сенсорів у розподілених мережах [12]. Автор І. Гунько (I. Hunko) розглядає скорочення часу тестування програмного забезпечення як важливий чинник підвищення загального рівня безпеки розподілених систем за допомогою раннього виявлення вразливостей [13]. Зокрема Н. Хайдер (N. Haider) та співавтори аналізують застосування ШІ та машинного навчання в безпеці 5G-мереж, де надвисока щільність підключень вимагає автономних і масштабованих механізмів захисту [14]. Окрім того, Ю. Ван (Y. Wang) та співавтори досліджують використання алгоритмів ШІ для підвищення безпеки хмарних мереж у розподілених обчислювальних середовищах [15].

Попри активне використання ШІ у сфері кібербезпеки, залишаються недостатньо дослідженими питання комплексного врахування архітектурної різнорідності розподілених мереж, масштабованості інтелектуальних рішень у динамічних середовищах, інтерпретованості моделей і вразливості систем безпеки до атак, що спрямовані безпосередньо на механізми ШІ. З огляду на це, обмежено вивченим залишається управлінський аспект інтеграції результатів роботи ШІ в системи виявлення вторгнень і прийняття рішень, що стримує практичне впровадження таких підходів.

Запропоноване дослідження спрямоване на узгоджений аналіз архітектурних, аналітичних і управлінських аспектів використання ШІ в безпеці розподілених мереж, виявлення ключових обмежень наявних підходів і формування практичних рекомендацій щодо їх подолання. Це дає змогу поглибити наукове розуміння проблеми та підвищити прикладну ефективність інтелектуальних систем безпеки.

**Постановка завдання.** Метою статті є обґрунтування доцільності та визначення практично орієнтованих напрямів використання ШІ для підвищення рівня безпеки розподілених мережевих інфраструктур в умовах зростання складності та інтенсивності сучасних кіберзагроз.

Для досягнення поставленої мети в статті передбачено виконання таких завдань:

1. Проаналізувати сучасні підходи до гарантування безпеки розподілених мережевих інфраструктур з урахуванням їхніх архітектурних і функціональних особливостей та узагальнити напрями використання штучного інтелекту в системах захисту.

2. Дослідити можливості застосування методів ШІ для аналізу мережевого трафіку, виявлення аномалій і ідентифікації кіберзагроз у розподілених середовищах.

3. Виявити ключові науково-практичні проблеми та обґрунтувати практичні рекомендації щодо впровадження ШІ з метою підвищення стійкості й ефективності систем безпеки розподілених мережевих інфраструктур.

**Виклад основного матеріалу.** У сучасних умовах гарантування безпеки розподілених мережевих інфраструктур формується під впливом ускладнення мережевих архітектур, зростання обсягів і швидкості обміну даними, а також переходу до децентралізованих моделей оброблення інформації. Хмарні та гібридні середовища, периферійні обчислення, програмно керовані мережі та мікросервісні архітектури змінюють логіку побудови систем захисту, зміщуючи акцент із периметрової безпеки до багаторівневих і контекстно-орієнтованих механізмів. У цьому контексті безпека розглядається не як окремий функціональний модуль, а як інтегрована властивість усієї інфраструктури, що охоплює мережевий, прикладний і управлінський рівні та передбачає безперервний моніторинг стану системи.

Сучасні підходи до захисту розподілених мережевих інфраструктур базуються на поєднанні класичних засобів контролю доступу, сегментації мережі та криптографічного захисту з адаптивними механізмами аналізу поведінки користувачів і сервісів. Окрім того, особливого значення набуває концепція динамічної довіри, за

якої кожен запит до ресурсів перевіряється з урахуванням контексту, а не лише формальних прав доступу. Це дає змогу зменшити ризики компрометації окремих вузлів і локалізувати наслідки інцидентів у межах окремих сегментів інфраструктури (табл. 1).

На практиці наведені підходи реалізуються у вигляді інтегрованих систем безпеки, які функціонують безперервно та охоплюють усі рівні розподіленої мережевої інфраструктури. Периметрові механізми захисту в сучасних умовах виконують допоміжну роль і застосовуються переважно для первинної фільтрації зовнішнього трафіку та зниження навантаження на внутрішні засоби аналізу. Головний акцент зміщується на внутрішню сегментацію мережі, що дає змогу ізолювати критично важливі сервіси, обчислювальні вузли та сховища даних, обмежуючи горизонтальне переміщення зловмисника навіть у разі компрометації окремого компонента системи. З огляду на наведене, такий підхід широко використовується в корпоративних і хмарних середовищах, де один фізичний або віртуальний кластер обслуговує різні за рівнем критичності бізнес-процеси. Концепція Zero Trust у практичному застосуванні передбачає динамічну оцінку кожної сесії доступу з урахуванням контекстних параметрів, зокрема типу пристрою, місця підключення, часу доступу та попередньої поведінки користувача або сервісу. У розподілених мережевих інфраструктурах це допомагає мінімізувати ризики внутрішніх загроз і помилок конфігурації, які є однією з головних причин порушень безпеки [1, p. 153]. Наприклад, у багатохмарних середовищах доступ до обчислювальних ресурсів, а також інтерфейс прикладного програмування (application programming interface, API) обмежується не лише обліковими даними, а й поточним станом сервісу та рівнем довіри до запиту, що знижує ймовірність несанкціонованого використання ресурсів. Поведінковий аналіз мережевих взаємодій на практиці ґрунтується на формуванні профілів нормальної активності користувачів, сервісів і вузлів інфраструктури. Відхилення від цих профілів, навіть за відсутності відомих сигнатур атак, розглядаються як потенційні загрози. Такий підхід є особливо ефективним для виявлення атак нульового дня та прихованих тривалих впливів, що характерні для складних цілеспрямованих атак. Зокрема в промислових і транспортних мережах поведінковий аналіз дає змогу фіксувати нетипові запити до керувальних систем або зміну режимів обміну даними, що може свідчити про компрометацію вузлів [3, p. 7]. Автоматизоване реагування в сучасних системах безпеки реалізується через заздалегідь визначені сценарії, які активуються відповідно до результатів аналізу ризиків. У розподілених мережевих інфраструктурах це надає можливість оперативно ізолювати скомпрометовані сегменти, обмежувати доступ до критичних сервісів або змінювати мережеві маршрути без втручання оператора. Практичний ефект такого підходу полягає в значному скороченні часу між виявленням загрози та її нейтралізацією, що є критично важливим для систем, які забезпечують безперервність бізнес-процесів або функціонування критичної інфраструктури. Отже, у сукупності зазначені підходи формують адаптивну модель безпеки, здатну ефективно функціонувати в умовах високої динаміки та складності сучасних розподілених мережевих інфраструктур. У розподілених мережевих середовищах аналіз мережевого трафіку ускладнюється гетерогенністю джерел даних, високою динамікою обміну інформацією та постійною зміною мережевих маршрутів і сервісних взаємодій. Потоки трафіку формуються одночасно на рівні хмарних платформ, периферійних вузлів, мікросервісів і API, що унеможлив-

Таблиця 1

**Сучасні підходи до гарантування безпеки розподілених мережевих інфраструктур**

| Підхід | Характеристика | Практичне призначення |
|---|---|---|
| Периметрова безпека | Захист на межі мережі з використанням міжмережевих екранів і шлюзів | Базовий контроль зовнішніх з'єднань |
| Сегментація мережі | Поділ інфраструктури на ізольовані логічні зони | Локалізація інцидентів і обмеження поширення атак |
| Zero Trust | Перевірка кожного запиту незалежно від його походження | Зменшення ризиків внутрішніх загроз |
| Поведінковий аналіз | Аналіз дій користувачів і сервісів у реальному часі | Виявлення аномалій і прихованих атак |
| Автоматизоване реагування | Використання інтелектуальних сценаріїв реагування | Скорочення часу нейтралізації інцидентів |

*Джерело: сформовано автором на основі [1, p. 153; 2; 3, p. 7; 6; 7, p. 43; 9, p. 26].*

лює їхнє ефективне оброблення лише за допомогою статичних правил і сигнатур. З огляду на це, методи ШІ забезпечують можливість виявлення прихованих закономірностей у великих масивах мережевих даних, формування адаптивних моделей нормальної поведінки та своєчасної ідентифікації відхилень, які можуть свідчити про реалізацію чи підготовку кібератак (табл. 2).

Застосування методів ШІ для аналізу мережевого трафіку ґрунтується на поєднанні локальної та глобальної обробки даних. У розподілених інфраструктурах первинний аналіз здійснюється безпосередньо на периферійних або вузлових компонентах мережі, де моделі ШІ в режимі реального часу фіксують відхилення від типової поведінки трафіку. Наприклад, у корпоративних або хмарних середовищах це забезпечує можливість оперативного виявлення нетипових звернень до сервісів або аномальних обсягів передавання даних між мікросервісами, що може свідчити про компрометацію облікових даних або несанкціонований доступ [4, p. 153833]. Централізований рівень аналізу використовується для глибокої кореляції подій, які самі по собі можуть видаватися незначними, але в сукупності формують ознаки складних цілеспрямованих атак. Так, у багатохмарних середовищах одночасна поява нехарактерних API-запитів, зміна часових профілів доступу та зростання внутрішнього трафіку між сегментами мережі може бути ідентифікована моделями ШІ як рання фаза підготовки атаки. Прогностичні можливості таких моделей дають змогу не лише фіксувати факт порушення, а й оцінювати ймовірний розвиток інциденту, що створює підґрунтя для проактивного реагування. Практичний ефект використання методів ШІ полягає в зниженні кількості хибних спрацювань, підвищенні точності виявлення нових типів загроз і скороченні часу між виникненням аномалії та прийняттям управлінського рішення [14]. Це особливо важливо для розподілених мережевих інфраструктур, у яких затримки реагування можуть призводити до масштабного поширення загрози та суттєвих порушень безперервності функціонування критичних сервісів.

У сучасних розподілених мережевих інфраструктурах використання ШІ в системах виявлення вторгнень і управління безпекою поступово зміщується від суто технічних механізмів фіксації інцидентів до інтелектуально підтримуваних управлінських процесів. За умов зростання кількості подій безпеки, територіальної та логічної розподіленості мереж, а також обмежених ресурсів служб кіберзахисту ключовим завданням стає не лише виявлення загрози, а й її коректна інтерпретація, оцінювання потенційного впливу та вибір адекватної стратегії реагування. У цьому контексті ШІ постає інструментом підтримки управління безпекою, що забезпечує інтеграцію результатів детекції в єдиний контур прийняття рішень і координації дій (табл. 3).

Зазначені напрями реалізуються в межах інтегрованих систем управління безпекою, у яких ШІ використовується для оброблення великої кількості різнорідних подій, що надходять із різних сегментів розподіленої мережі. Інтелектуальна агрегація дає змогу перетворювати масиви низькорівневих сповіщень на узагальнені інциденти, зменшуючи навантаження на фахівців з безпеки та знижуючи ризик пропуску критично важливих подій. У практичних сценаріях це особливо важливо для великих корпоративних або міжорганізаційних мереж, де кількість подій може сягати сотень тисяч на добу [15].

Контекстна кореляція інцидентів на основі ШІ забезпечує зв'язування подій, що відбуваються в різних частинах інфраструктури та в різний час, у єдині логічні ланцюги. Зокрема серія незна-

Таблиця 2

**Напрями застосування методів ШІ для аналізу мережевого трафіку та виявлення кіберзагроз**

| Напрям застосування | Характер оброблюваних даних | Практичний результат |
|---|---|---|
| Аналіз мережевого трафіку | Потоки пакетів, часові ряди, агреговані мережеві метадані | Виявлення нетипових шаблонів обміну даними |
| Виявлення аномалій | Поведінкові профілі вузлів, сервісів і користувачів | Ідентифікація прихованих і нових загроз |
| Класифікація атак | Ознаки відомих і раніше невідомих атак | Автоматичне розпізнавання типів кібератак |
| Прогнозування загроз | Історичні та поточні дані мережевої активності | Попередження інцидентів на ранніх стадіях |
| Кореляція подій | Події з різних сегментів і рівнів інфраструктури | Комплексне оцінювання стану безпеки |

*Джерело: сформовано автором на основі [2; 4, p. 153833; 5, p. 5223; 6; 7, p. 46; 14].*

Таблиця 3

**Напрями використання ШІ в системах виявлення вторгнень та управління безпекою розподілених мереж**

| Напрям використання | Сфера застосування | Практичне призначення |
|---|---|---|
| Інтелектуальна агрегація подій | Централізовані платформи управління безпекою | Зменшення інформаційного перевантаження операторів |
| Контекстна кореляція інцидентів | Розподілені сегменти мережі | Виявлення складних багатокомпонентних загроз |
| Оцінювання критичності інцидентів | Управління ризиками | Пріоритизація реагування |
| Автоматизована підтримка рішень | Реагування на інциденти | Скорочення часу прийняття управлінських рішень |
| Адаптивне управління політиками | Контури безпеки мережі | Підвищення узгодженості захисних заходів |

*Джерело: сформовано автором на основі [4, p. 153835–153837; 5, p. 5232; 6; 7, p. 48; 10; 15].*

чних порушень політик доступу, змін конфігурацій і нетипових звернень до сервісів може бути інтерпретована системою як ознака цілеспрямованого впливу, навіть якщо кожна подія окремо не характеризується високим рівнем критичності [4, p. 153835–153837]. Це дає змогу переходити від реакції на окремі інциденти до управління сценаріями загроз.

Оцінювання критичності інцидентів із використанням ШІ здійснюється з урахуванням ролі залучених ресурсів, їхньої значущості для безперервності функціонування сервісів і потенційних наслідків порушення. У практиці управління безпекою це дає змогу автоматично спрямовувати зусилля на захист найбільш критичних компонентів інфраструктури, мінімізуючи вплив інцидентів на ключові бізнес- та управлінські процеси [7, p. 48]. У цьому контексті адаптивне управління політиками безпеки надає можливість коригувати правила доступу, рівні контролю та сценарії реагування відповідно до актуального профілю ризиків без необхідності повної перебудови системи. У сукупності це формує управлінсько-орієнтовану модель використання ШІ, у якій системи виявлення вторгнень стають елементом єдиного інтелектуального контуру управління безпекою розподілених мереж.

Використання ШІ у сфері захисту розподілених мережевих інфраструктур супроводжується комплексом науково-практичних проблем, які суттєво обмежують ефективність і надійність інтелектуальних систем безпеки в реальних умовах експлуатації. Зокрема однією з базових проблем є якість і репрезентативність даних, що використовуються для навчання та функціонування моделей ШІ. У розподілених середовищах дані часто є неповними, зашумленими, асинхронними та структурно неоднорідними, що призводить до спотворення навчальних вибірок і зниження здатності моделей адекватно відображати реальні профілі мережевої поведінки [10]. Окрім того, швидка еволюція мережевих сервісів і сценаріїв використання зумовлює явище концептуального дрейфу, за якого навчена модель поступово втрачає актуальність без регулярного оновлення. Суттєвим обмеженням залишається проблема масштабованості інтелектуальних рішень, особливо в умовах високонавантажених і географічно розподілених інфраструктур. Зі зростанням кількості вузлів, сервісів і подій безпеки збільшується обчислювальна складність моделей ШІ та вимоги до ресурсів, що ускладнює їх використання в режимі реального часу. На практиці це часто призводить до компромісу між точністю аналізу та швидкістю реагування, що є критичним для захисту динамічних мережевих середовищ [15]. У цьому контексті окрему науково-практичну проблему становить інтерпретованість результатів роботи моделей ШІ, що має принципове значення для управління безпекою та прийняття відповідальних рішень. Значна частина сучасних моделей характеризується високою складністю внутрішніх представлень, що ускладнює пояснення причин спрацювання системи чи логіки класифікації інцидентів. Це знижує довіру з боку фахівців з безпеки, ускладнює аудит і верифікацію рішень, а також обмежує можливість використання таких систем у критично важливих інфраструктурах, де необхідна прозорість і відтворюваність управлінських дій. Вагомим викликом є вразливість інтелектуальних систем безпеки до нових типів атак, спрямованих безпосередньо на механізми ШІ. До таких загроз належать маніпуляції навчальними даними, навмисне формування хибних зразків, атаки на етапі експлуатації моделей і спроби обійти системи детекції шляхом поступових змін поведінки.

У розподілених мережевих інфраструктурах ці ризики посилюються через складність контролю джерел даних і взаємодію великої кількості автономних компонентів, що створює додаткові вектори впливу на інтелектуальні механізми захисту. Окрім того, до переліку проблем належать труднощі інтеграції ШІ-орієнтованих рішень у наявні системи безпеки, обмежена стандартизація підходів, залежність ефективності моделей від специфіки конкретної інфраструктури та ризик надмірної автоматизації, за якої знижується роль експертної оцінки. У сукупності зазначені проблеми свідчать про те, що застосування ШІ в захисті розподілених мережевих інфраструктур потребує не лише технологічних удосконалень, а й науково обґрунтованих підходів до управління ризиками, адаптації моделей і поєднання інтелектуальних засобів з експертним контролем.

**Висновки.** У ході дослідження встановлено, що застосування ШІ є ключовою умовою підвищення стійкості та керованості систем безпеки розподілених мережевих інфраструктур в умовах зростання їхньої архітектурної складності та динамічності кіберзагроз. Обґрунтовано, що традиційні підходи до кіберзахисту не забезпечують необхідного рівня адаптивності, тоді як ШІ дає змогу інтегрувати аналітичні, детекційні та управлінські функції в єдиний інтелектуальний контур безпеки. Встановлено, що використання ШІ забезпечує перехід від реактивного реагування на інциденти до проактивного управління кіберризиками завдяки агрегації подій, кореляції інцидентів і пріоритизації загроз з урахуванням критичності ресурсів і сервісів. Водночас виявлено ключові науково-практичні проблеми застосування ШІ, що пов'язані з якістю та нестаціонарністю даних, масштабованістю інтелектуальних рішень, обмеженою інтерпретованістю моделей і зростанням ризиків атак на самі інтелектуальні механізми безпеки.

Сформульовано рекомендації щодо впровадження ШІ на основі багаторівневих архітектур, керованого використання даних, поєднання автоматизації з експертним контролем і підвищення прозорості управлінських рішень. Перспективи подальших досліджень пов'язані з розробленням інтерпретованих і стійких до маніпуляцій моделей ШІ, розвитком адаптивних механізмів управління політиками безпеки та формуванням методик комплексного оцінювання ефективності інтелектуальних систем захисту в реальних розподілених мережевих середовищах.

**Список літератури:**

1. Bershchanskyi Y., Klym H., Shevchuk Y. Containerized Artificial Intelligent System Design in Cloud and Cyber-Physical Systems. *Advances in Cyber-Physical Systems*. 2024. Vol. 9, No. 2. P. 151–157. DOI: https://doi.org/10.23939/acps2024.02.151

2. Moustafa N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustainable Cities and Society*. 2021. Vol. 72. Article 102994. DOI: https://doi.org/10.1016/j.scs.2021.102994

3. Ali S. S., Choi B. J. State-of-the-art artificial intelligence techniques for distributed smart grids: A review. *Electronics*. 2020. Vol. 9, No. 6. Article 1030. DOI: https://doi.org/10.3390/electronics9061030

4. Wu H., Han H., Wang X., Sun S. Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. *IEEE Access*. 2020. Vol. 8. P. 153826–153848. DOI: https://doi.org/10.1109/ACCESS.2020.3018170

5. Waqas M., Tu S., Halim Z., Rehman S. U., Abbas G., Abbas Z. H. The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artificial Intelligence Review*. 2022. Vol. 55, No. 7. P. 5215–5261. DOI: https://doi.org/10.1007/s10462-022-10143-2

6. Schmitt M. Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*. 2023. Vol. 36. 100520. DOI: https://doi.org/10.1016/j.jii.2023.100520

7. Akinade A. O., Adepoju P. A., Ige A. B., Afolabi A. I., Amoo O. O. A conceptual model for network security automation: Leveraging AI-driven frameworks to enhance multi-vendor infrastructure resilience. *International Journal of Science and Technology Research Archive*. 2021. Vol. 1, No. 1. P. 39–59. DOI: https://doi.org/10.53771/ijstra.2021.1.1.0034

8. Ahmed S., Hossain M. F., Kaiser M. S., Noor M. B. T., Mahmud M., Chakraborty C. Artificial intelligence and machine learning for ensuring security in smart cities. In: *Data-driven mining, learning and analytics for secured smart cities: Trends and advances*. Cham: Springer International Publishing, 2021. P. 23–47. DOI: https://doi.org/10.1007/978-3-030-72139-8_2

9. Islam N., Farhin F., Sultana I., Kaiser M. S. (M. S. Kaiser), Rahman M. S., Mahmud M., Hosen A. S. M., Cho G. H. Towards Machine Learning Based Intrusion Detection in IoT Networks. Computers, Materials & Continua. 2021. Vol. 69, No. 2. P. 1801–1821. DOI: https://doi.org/10.32604/cmc.2021.018466

10. Khan A. A., Laghari A. A., Rashid M., Li H., Javed A. R., Gadekallu T. R. Artificial intelligence and blockchain technology for secure smart grid and power distribution automation: A state-of-the-art review. *Sustainable Energy Technologies and Assessments*. 2023. Vol. 57. Article 103282. DOI: https://doi.org/10.1016/j.seta.2023.103282

11. Chehri A., Fofana I., Yang X. Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability*. 2021. Vol. 13, No. 6. Article 3196. DOI: https://doi.org/10.3390/su13063196

12. Poperehnyak S., Syvachenko I., Shevchuk Y. Enhancing pseudorandom number generation using environmental sensor-based entropy sources. In: *Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025): Proceedings of the Workshop*. Vol. 3991. CEUR-WS.org, 2025. P. 363–380. URL: https://ceur-ws.org/Vol-3991/paper26.pdf (date of access: 30.12.2025).

13. Hunko I. How to Effectively Reduce Software Testing Time: From Requirements to Regression. Lodz: Futurity Research Publishing, 2025. 158 p. URL: https://futurity-publishing.com/wp-content/uploads/2025/04/7%D0%9F-29.03.25-3.pdf (date of access: 30.12.2025).

14. Haider N., Baig M. Z., Imran M. Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends. *arXiv preprint*. 2020. arXiv:2007.04490. DOI: https://doi.org/10.48550/arXiv.2007.04490

15. Wang Y., Yang X. Research on enhancing cloud computing network security using artificial intelligence algorithms. *arXiv preprint*. 2025. arXiv:2502.17801. DOI: https://doi.org/10.1109/SCECS65243.2025.11065638

**Suprun O.M., Kravchuk Ya.Ya., Babkova N.O. USE OF ARTIFICIAL INTELLIGENCE TO ENHANCE THE SECURITY OF DISTRIBUTED NETWORK INFRASTRUCTURES**

*The relevance of this study is driven by the rapid increase in the complexity of distributed network infrastructures, the widespread adoption of cloud and edge computing, and the escalation of contemporary cyber threats characterized by high dynamism, multi-vector attack patterns, and the ability to bypass traditional protection mechanisms. Under these conditions, classical cybersecurity approaches based on static rules and signature-based analysis prove insufficient, which substantiates the need for the intellectualization of security systems.The purpose of the article is the scientific justification of the feasibility and identification of practically oriented directions for the use of artificial intelligence to enhance the security level of distributed network infrastructures in the context of increasing complexity and intensity of modern cyber threats.The methodological framework of the study includes a system analysis of distributed network architectures, generalization of current cybersecurity assurance approaches, comparative analysis of artificial intelligence methods, and logical modeling of threat detection and security incident management processes. Methods of abstraction, generalization, and analytical synthesis are applied, enabling a comprehensive assessment of the capabilities and limitations of intelligent protection systems. The results demonstrate that the use of artificial intelligence enables the integration of analytical, detection, and management functions into a unified security framework for distributed networks. It is shown that intelligent mechanisms facilitate proactive threat detection, incident correlation, and risk prioritization while accounting for the criticality of resources and services. Key scientific and practical challenges in applying artificial intelligence are identified, including issues related to data quality and non-stationarity, solution scalability, model interpretability, and the vulnerability of intelligent systems to emerging attack types. The conclusions substantiate that effective implementation of artificial intelligence in distributed network security systems is achievable through the combination of intelligent tools with traditional protection mechanisms, ensured data governance, and the preservation of expert oversight in managerial decision-making. Future research perspectives include the development of interpretable and manipulation-resistant artificial intelligence models, the design of adaptive security policy management mechanisms, and the formation of methodologies for comprehensive evaluation of the effectiveness of intelligent protection systems in real-world distributed network environments.*

***Keywords:*** *cyber resilience, cyber risk management, intelligent security systems, intrusion detection, adaptive security mechanisms, distributed computing, incident management.*

Дата першого надходження статті до видання: 12.01.2026
Дата прийняття статті до друку після рецензування: 03.02.2026
Дата публікації (оприлюднення) статті: 08.04.2026