КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1182
УДК 004.8:004.056:351.74

Кирилюк Олександр Степанович
кандидат технічних наук, старший дослідник, старший викладач
Національна академія Служби безпеки України, Київ, Україна
ORCID: 0000-0001-9248-0758
20kiril20@gmail.com

ШТУЧИЙ ІНТЕЛЕКТ ЯК ЗАСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПРАВООХОРОННІЙ СФЕРІ

Анотація. У статті досліджено роль штучного інтелекту як сучасного інструменту підвищення ефективності забезпечення інформаційної безпеки у правоохоронній сфері. У вступі обґрунтовано актуальність теми в умовах цифровізації суспільства, зростання кіберзагроз та трансформації інформаційного простору в середовище протистояння. У межах теоретичного розділу розкрито сутність ключових понять: «штучний інтелект», «інформаційна безпека», «кібербезпека» та «правоохоронна діяльність», а також проаналізовано сучасні наукові підходи до їх трактування. Визначено, що штучний інтелект виступає інтегрованим елементом системи управління безпекою, здатним забезпечити безперервний цикл виявлення, реагування та відновлення після кіберінцидентів. У результативній частині здійснено аналіз загроз інформаційній безпеці у правоохоронній сфері, зокрема витоку даних, кібератак, фішингу та внутрішніх ризиків. Обґрунтовано можливості штучного інтелекту щодо обробки великих масивів даних, виявлення аномалій, прогнозування загроз та автоматизації процесів прийняття рішень. Розкрито основні напрями застосування штучного інтелекту у правоохоронній діяльності, включаючи розслідування кіберзлочинів, використання біометричних систем, аналіз текстової та візуальної інформації, а також предиктивну аналітику. Окрему увагу приділено проблемам і ризикам використання штучного інтелекту, серед яких визначено алгоритмічні помилки, упередженість, загрози конфіденційності та недостатність правового регулювання. У статті запропоновано шляхи підвищення ефективності використання штучного інтелекту, що передбачають комплексний підхід, який поєднує технологічні, кадрові та правові аспекти. Зроблено висновок про необхідність збереження балансу між ефективністю безпеки та дотриманням прав людини. Окреслено перспективи подальших досліджень, пов’язаних із удосконаленням механізмів інтеграції штучного інтелекту у правоохоронну діяльність та підвищенням прозорості його застосування.

Ключові слова: штучний інтелект; інформаційна безпека; кібербезпека; правоохоронна діяльність; кіберзагрози; машинне навчання; цифрова криміналістика.

ВСТУП

В сучасних умовах особливо актуальності набуває питання забезпечення інформаційної безпеки. Це пов’язано з швидкою цифровізацією суспільства та зростання ролі інформаційних технологій, а також військовими діями на території України які давно вийшли на новий рівень, а саме в інформаційний простір. В цих умовах інформаційний простір постає не лише середовищем комунікації, а й широким полем протистояння, де починають формуватися нові типи загроз – від кібератак і витоку даних до інформаційно-психологічного впливу. Саме в таких умовах традиційні підходи, які раніше забезпечували безпеку, виявляються недостатньо ефективними, що активізує необхідність впровадження інноваційних рішень, що здатні оперативно реагувати на динамічні виклики сучасності.

Найбільш яскраво ця проблема проявляється у сфері правоохоронних органів, де ефективність діяльності безпосередньо залежить від швидкості обробки інформації, її точності, аналізу та здатності прогнозувати потенційні загрози. Правоохоронні органи функціонують у середовищі постійної інформаційної невизначеності, що потребує застосування нових інструментів для виявлення, попередження та нейтралізації правопорушень. Спираючись на це, штучний інтелект, в цьому контексті, розглядається як один із важливих та ключових факторів модернізації правоохоронної діяльності будь-якої країни.

Штучний інтелект відкриває широкі можливості для ефективного забезпечення інформаційної безпеки, в тому числі і у правоохоронній сфері. Передусім, застосування алгоритмів машинного навчання, обробки великих даних та інтелектуального аналізу інформації дозволяє виявити складні закономірності, передбачити чи визначати ризики та автоматизувати процеси прийняття рішень. Це сприяє переходу від реактивної моделі діяльності до проактивної, коли загрози можуть бути ідентифіковані ще на ранніх етапах їх виникнення.

Проте впровадження штучного інтелекту у сферу правоохоронних органів та їх діяльність, може супроводжуватися низкою викликів, пов'язаних із необхідністю забезпечення прозорості алгоритмів, захисту персональних даних, державних таємниць, дотримання прав людини та визначення відповідальності за прийняті рішення. Все це активізує потребу у комплексному науковому осмисленні ролі та значення штучного інтелекту як засобу підвищення ефективності забезпечення інформаційної безпеки у правоохоронній сфері, що і визначає актуальність даного дослідження.

Постановка проблеми. Нині суспільство перебуває у стані надзвичайно стрімкого розвитку інформаційних технологій, а також підвищеного рівня кіберзагроз, що посилює проблему забезпечення інформаційної безпеки, особливо у діяльності правоохоронних органів. Правоохоронні органи щодня стикаються з обробкою великої кількості даних, що потребують не лише швидкої обробки, а й глибокого аналізу для своєчасного виявлення потенційних ризиків та загроз. Проте традиційні засоби вже не завжди дозволяють ефективно реагувати на нові виклики сучасних загроз, що зумовлює потребу у впровадженні сучасних інструментів, зокрема технологій штучного інтелекту. Але їх застосування може супроводжуватися низкою складних питань, пов'язаних із захистом персональних даних, забезпеченням прозорості рішень та дотриманням прав людини, що й актуалізує необхідність ґрунтовного наукового осмислення цієї проблематики.

Аналіз останніх досліджень і публікацій. На сьогоднішній день проблема застосування штучного інтелекту у сфері інформаційної безпеки та правоохоронної діяльності активно досліджується як зарубіжними, так і вітчизняними науковцями. Значна частина досліджень присвячена можливостям штучного інтелекту у виявленні та протидії кіберзагрозам. Зокрема, Р. Каур, Д. Габрієлчіч та Т. Клобучар доводять, що штучний інтелект забезпечує комплексний підхід до управління кібербезпекою [4], а У. Околі та співавтори підкреслюють ефективність машинного навчання у виявленні загроз [9]. Водночас А. Таніконда та інші дослідники акцентують на проактивному характері інтелектуальних систем безпеки [14]. У контексті правоохоронної діяльності П. Гейлі та Д. Баррелл обґрунтовують значення штучного інтелекту для підвищення ефективності забезпечення безпеки [2], тоді як Е. Гелфорд розглядає можливості впровадження генеративного ШІ у поліцейській діяльності [3]. В. Налуцишин та співавтори аналізують зарубіжний досвід використання таких технологій у правоохоронних органах [8]. Окрему увагу приділено ризикам застосування штучного інтелекту. А. Майо наголошує на його подвійній природі [7], Н. Кшетрі – на трансформації кіберзагроз під впливом нових технологій [5], а Г. Срівастава та співавтори – на необхідності забезпечення прозорості алгоритмів [13].

В цілому, останні дослідження підтверджують значний потенціал штучного інтелекту у сфері інформаційної безпеки та правоохоронної діяльності. Проте, попри значні наукові напрацювання, питання комплексного впровадження таких технологій із урахуванням правових, етичних та організаційних аспектів потребує подальшого дослідження.

Мета статті. Метою статті є теоретичне узагальнення штучного інтелекту як ефективного засобу забезпечення інформаційної безпеки, в тому числі і у сфері правоохоронних органів та їх діяльності. Досягнення поставленої мети передбачає: розкриття теоретичних підходів до сутності штучного інтелекту; визначення принципів застосування ШІ в інформаційній безпеці; виявлення загроз інформаційній безпеці у правоохоронній діяльності; аналіз можливостей штучного інтелекту у забезпеченні інформаційної безпеки; дослідження проблем та ризиків застосування ШІ в правоохоронній сфері; розробку шляхів підвищення ефективності штучного інтелекту у забезпечення інформаційної безпеки у правоохоронній сфері.

Методи дослідження. В процесі написання статті використано комплекс загальнонаукових методів, зокрема аналіз і синтез – для узагальнення наукових підходів до проблеми застосування штучного інтелекту у сфері інформаційної безпеки; системний метод – для розгляду інформаційної безпеки як цілісної системи; порівняльний метод – для зіставлення вітчизняного та зарубіжного досвіду; метод узагальнення – для формулювання висновків. Також у процесі підготовки тексту використовувалися інструменти штучного інтелекту (ChatGPT, Gemini AI) для лінгвістичного редагування, оптимізації структури та уточнення формулювань. Згенерований контент перевірено та відредаговано автором.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Становлення сучасних підходів щодо використання штучного інтелекту в правоохоронній діяльності варто почати з визначення ключових понять дослідження, а саме: «штучний інтелект», «інформаційна безпека», «кібербезпека» та «правоохоронна діяльність».

Для початку дамо розглянемо визначення поняття «штучний інтелект». Штучний інтелект – це галузь інформатики та сукупність технологій, що спрямовані на створення комп'ютерних систем, здатних виконувати завдання, які зазвичай потребують людського інтелекту, зокрема: навчання, аналіз інформації, розпізнавання образів і мовлення, прийняття рішень, планування та розв'язання проблем [14].

У сучасних наукових праць це поняття подається у більш узагальненому науковому розумінні, штучний інтелект – це здатність програмних або технічних систем імітувати когнітивні функції людини, адаптуватися до нових даних і самостійно вдосконалювати результати своєї діяльності на основі попереднього досвіду [21].

У науковій літературі штучний інтелект розглядається також як ключовий елемент системного підходу до забезпечення кібербезпеки, що охоплює всі етапи управління загрозами . Зокрема, відповідно до дослідження Р. Каур, Д. Габрієлчіч та Т. Клобучар, застосування штучного інтелекту може бути структуровано в межах функціональної моделі NIST, яка включає процеси ідентифікації, захисту, виявлення, реагування та відновлення після кіберінцидентів. Такий підхід дозволяє розглядати штучний інтелект не як окремий інструмент, а як інтегровану систему, що забезпечує безперервний цикл управління інформаційною безпекою. Це є особливо важливим для правоохоронної діяльності, де необхідна комплексна координація дій щодо запобігання, виявлення та нейтралізації загроз [4].

Як можемо бачити, стрімкий розвиток інформаційних технологій та впровадження штучного інтелекту у різні сфери суспільного життя не лише відкривають нові можливості для обробки та аналізу даних, але й суттєво актуалізують питання їх захисту. Зростання обсягів інформації, підвищення рівня кіберзагроз та ускладнення способів несанкціонованого втручання в інформаційні системи обумовлюють необхідність переосмислення підходів до забезпечення безпеки інформаційного простору.

У цьому контексті доцільним є звернення до визначення поняття інформаційна безпека. Інформаційна безпека – це стан захищеності інформації, інформаційних ресурсів та інформаційної інфраструктури від внутрішніх і зовнішніх загроз, що забезпечує збереження їх цілісності, конфіденційності та доступності, а також гарантує стабільне функціонування інформаційних систем і захист інтересів особи, суспільства та держави.

У дослідженні У. Околі та співавторів інформаційна безпека фактично трактується як динамічний процес захисту інформаційних систем, що передбачає використання алгоритмів машинного навчання для своєчасного виявлення, аналізу та нейтралізації кіберзагроз, забезпечуючи таким чином безперервний моніторинг і адаптивну протидію атакам [9].

Водночас, на думку А. Таніконди, Б. Пандей, С. Педдінті та С. Катрагадди, інформаційна безпека – це комплексна система проактивного захисту інформаційного середовища, яка базується на застосуванні інтелектуальних технологій для прогнозування загроз, оперативного реагування на інциденти та забезпечення стійкості цифрових екосистем до складних кіберризиків [14].

Аналіз наукової літератури показав, що у межах сучасних підходів інформаційна безпека розглядається не лише як стан захищеності, а як активний, інтелектуально керований процес, що постійно вдосконалюється відповідно до нових викликів інформаційного середовища.

Сучасне розуміння інформаційної безпеки поступово трансформується від статичного уявлення про захист до динамічної, технологічно орієнтованої системи, що передбачає активне виявлення та попередження загроз. У цьому контексті логічним є уточнення більш вузького, але водночас надзвичайно актуального поняття – кібербезпека, яке безпосередньо пов'язане із захистом цифрового середовища.

У науковій літературі кібербезпека розглядається як складова інформаційної безпеки, що охоплює процеси захисту комп'ютерних систем, мереж та даних від кіберзагроз. Так, кібербезпека визначається як стан захищеності інформаційно-комунікаційних систем, мереж і даних від несанкціонованого доступу, атак, пошкодження або знищення, що забезпечує їх надійне функціонування та збереження ключових властивостей інформації – конфіденційності, цілісності та доступності [1].

Водночас у сучасних дослідженнях акцентується на проактивному характері цього явища. Зокрема, кібербезпека трактується як комплекс організаційних, технічних і інтелектуальних заходів, спрямованих на попередження, виявлення та нейтралізацію кіберзагроз, а також на забезпечення стійкості інформаційних систем до динамічних викликів цифрового середовища. Проте, кібербезпека виступає не лише як технічна категорія, а як важливий елемент загальної системи національної безпеки,

що потребує комплексного підходу до її забезпечення. У цьому контексті особливої актуальності набуває її зв'язок із правоохоронною діяльністю, яка покликана забезпечувати дотримання законності, правопорядку та захист прав і свобод громадян у цифровому середовищі.

Правоохоронна діяльність у сучасних умовах дедалі тісніше інтегрується з процесами забезпечення кібербезпеки, оскільки значна частина правопорушень переміщується у кіберпростір. Це зумовлює необхідність використання новітніх технологій, зокрема штучного інтелекту, для виявлення, попередження та розслідування кіберзлочинів, аналізу великих обсягів даних і прогнозування потенційних загроз.

У науковому розумінні правоохоронна діяльність визначається як сукупність організаційних, правових і практичних заходів, що здійснюються уповноваженими державними органами з метою охорони прав і свобод людини, забезпечення законності та правопорядку, протидії правопорушенням і притягнення винних до відповідальності.

За визначенням, Т. Латковської та А. Маращука, правоохоронна діяльність розглядається як комплексна діяльність уповноважених державних органів, спрямована на забезпечення законності, правопорядку та безпеки, що реалізується через протидію правопорушенням, захист прав і свобод людини та реагування на сучасні загрози, зокрема у сфері кібербезпеки [18].

Водночас у контексті цифровізації суспільства правоохоронна діяльність набуває нових характеристик і може розглядатися як діяльність, спрямована на забезпечення безпеки як у фізичному, так і в інформаційному (кібернетичному) просторі, що передбачає інтеграцію традиційних правових механізмів із сучасними інформаційними технологіями.

Саме в умовах сучасних безпекових викликів, пов'язаних із гібридними загрозами та цифровізацією суспільства, особливої актуальності набуває впровадження технологій штучного інтелекту у діяльність правоохоронних органів. Як зазначає В. Шевчук, використання штучного інтелекту є важливим чинником підвищення ефективності забезпечення безпеки та обороноздатності держави, оскільки дозволяє вдосконалити процеси аналізу інформації, прогнозування загроз та прийняття управлінських рішень. У цьому контексті штучний інтелект виступає не лише інструментом оптимізації діяльності правоохоронних органів, а й стратегічним ресурсом зміцнення національної безпеки [25].

Варто відмітити, що законодавство України також не обходить стороною застосування штучного інтелекту у процесі кібезбезпеки та захисту інформаційних даних. Важливим напрямом державної політики у сфері цифрової трансформації є розвиток та впровадження технологій штучного інтелекту. Зокрема, Концепція розвитку штучного інтелекту в Україні, затверджена Кабінетом Міністрів України у 2020 році, визначає стратегічні напрями формування державної політики у цій сфері, включаючи забезпечення безпеки, дотримання прав людини та розвиток інноваційних технологій. У документі підкреслюється необхідність інтеграції штучного інтелекту у сфери кібербезпеки, оборони та правоохоронної діяльності, що зумовлює актуальність дослідження його ролі у забезпеченні інформаційної безпеки [17].

Правове регулювання забезпечення інформаційної безпеки в Україні ґрунтується на положеннях Закону України «Про основні засади забезпечення кібербезпеки України», який визначає систему суб'єктів кібербезпеки та їх функції у цифровому середовищі. Відповідно до цього Закону правоохоронні органи виконують подвійне завдання: з одного боку, вони забезпечують протидію кіберзлочинності, а з іншого – самі виступають об'єктами кіберзахисту. Такий підхід підкреслює складність функціонування правоохоронної системи в умовах цифрових загроз та необхідність використання сучасних технологій, зокрема штучного інтелекту [20].

Значну роль у формуванні сучасної політики інформаційної безпеки відіграє також Стратегія кібербезпеки України, яка визначає пріоритети держави у сфері захисту інформаційних ресурсів та протидії кіберзагрозам. У контексті цифровізації суспільства особлива увага приділяється впровадженню інноваційних технологій, включаючи штучний інтелект, що сприяє підвищенню ефективності правоохоронної діяльності та зміцненню національної безпеки [23].

Варто також коротко розглянути теоретичні підходи до дослідження застосування штучного інтелекту в інформаційній безпеці. Теоретичні підходи до дослідження проблеми ґрунтуються на сучасних наукових уявленнях про безпеку як складне, багатовимірне явище, що функціонує в умовах цифровізації суспільства. Як зазначається у праці Р. Каур, Д. Габрієлчіч та Т. Клобучара, сучасний розвиток кібербезпеки пов'язаний із переходом до інтелектуально керованих систем захисту, у яких штучний інтелект відіграє ключову роль у забезпеченні адаптивності та ефективності безпекових процесів. Автори наголошують, що застосування штучного інтелекту охоплює всі основні функції кібербезпеки, зокрема ідентифікацію, захист, виявлення, реагування та відновлення після інцидентів, що

дозволяє розглядати його як комплексний механізм підвищення ефективності безпеки, особливо у сфері правоохоронної діяльності [4].

У межах дослідження доцільно виокремити такі основні підходи:

- системний підхід – передбачає розгляд безпеки як цілісної взаємопов'язаної системи;
- діяльнісний підхід – акцентує увагу на ролі суб'єктів правоохоронної діяльності у забезпеченні безпеки;
- інформаційний підхід – розглядає дані як ключовий об'єкт захисту;
- ризик-орієнтований підхід – передбачає оцінку та прогнозування загроз;
- технологічний підхід – визначає провідну роль штучного інтелекту та цифрових інструментів у забезпеченні безпеки.

Дослідження базується на поєднанні системного, діяльнісного, інформаційного, ризик-орієнтованого та технологічного підходів, що дозволяє комплексно розкрити особливості забезпечення інформаційної та кібербезпеки в умовах сучасних викликів і підвищити ефективність правоохоронної діяльності.

Логічним продовженням окреслених теоретичних підходів є визначення базових принципів застосування штучного інтелекту у сфері безпеки, які забезпечують не лише ефективність, але й правомірність використання таких технологій у правоохоронній діяльності.

Як зазначає Е. Гелфорд, ефективне впровадження штучного інтелекту у правоохоронній діяльності потребує чіткої нормативної та організаційної основи, що гарантує законність, прозорість і контроль за використанням таких технологій. Дослідник наголошує на необхідності дотримання вимог правового регулювання, зокрема положень AI Act Європейського Союзу, а також принципів відповідальності, пояснюваності та підзвітності алгоритмічних рішень. Водночас особливого значення набуває збереження людського контролю, оскільки автоматизовані рішення без належного нагляду можуть призводити до помилок, упередженості та порушення прав людини [3].

У свою чергу, С. Веласко підкреслює важливість міжнародно-правового регулювання застосування штучного інтелекту, зокрема у контексті протидії кіберзлочинності. Будапештська конвенція про кіберзлочинність розглядається як ключовий інструмент міжнародної співпраці у сфері розслідування кіберзлочинів та обміну електронними доказами. Разом із тим розвиток технологій штучного інтелекту створює нові виклики, пов'язані з визначенням відповідальності, достовірністю цифрових доказів і координацією транскордонних розслідувань, що потребує удосконалення правових механізмів [15].

Важливу увагу проблемі прозорості та надійності функціонування систем штучного інтелекту приділяють О. Скіцька, П. Складанний, Р. Ширшов, М. Гуменюк та М. Ворохоб, які зазначають, що значна частина таких систем функціонує за принципом «чорної скриньки», що ускладнює перевірку їх рішень. Це зумовлює ризики використання недостовірної інформації, особливо у правоохоронній сфері. У зв'язку з цим ключового значення набувають принципи прозорості алгоритмів, можливості їх незалежної верифікації та встановлення відповідальності за результати функціонування [21].

Подібну позицію висловлюють і Г. Срівастава та співавтори, які наголошують на необхідності розвитку explainable artificial intelligence (XAI), що забезпечує інтерпретацію результатів роботи алгоритмів і підвищує рівень довіри до них. Це є особливо важливим у правоохоронній діяльності, де кожне рішення має бути обґрунтованим і перевірюваним [13].

Узагальнюючи зазначене, до основних принципів застосування штучного інтелекту у сфері безпеки доцільно віднести:

- законність – відповідність застосування ШІ нормам права;
- захист прав людини – недопущення дискримінації та порушення прав і свобод;
- конфіденційність даних – забезпечення захисту персональної та службової інформації;
- прозорість алгоритмів – можливість розуміння та перевірки логіки роботи систем;
- відповідальність за рішення ШІ – визначення суб'єктів, відповідальних за наслідки використання інтелектуальних систем.

Дотримання зазначених принципів є необхідною умовою ефективного, безпечного та етично обґрунтованого використання штучного інтелекту у правоохоронній діяльності.

Узагальнення теоретичних підходів та сучасних наукових позицій дає підстави стверджувати, що штучний інтелект виступає перспективним інструментом підвищення ефективності забезпечення інформаційної та кібербезпеки, зокрема у сфері правоохоронної діяльності. Водночас його застосування не може бути стихійним чи виключно технологічним, а потребує ґрунтовного наукового обґрунтування, чіткого нормативного регулювання та продуманого впровадження з урахуванням можливих ризиків і

викликів. Саме це зумовлює необхідність подальшого дослідження можливостей, обмежень і умов ефективного використання штучного інтелекту у системі забезпечення безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У цьому розділі подано результати проведеного дослідження, спрямованого на аналіз можливостей застосування штучного інтелекту у сфері інформаційної та кібербезпеки. Отримані результати дозволяють оцінити ефективність сучасних підходів і визначити ключові напрями їх використання у правоохоронній діяльності.

Аналіз загроз інформаційній безпеці у правоохоронній сфері. Сучасний етап розвитку інформаційного суспільства супроводжується суттєвим ускладненням загроз інформаційній безпеці, що особливо гостро проявляється у правоохоронній сфері. Це пов'язано як із цифровізацією діяльності правоохоронних органів, так і зі зростанням кількості кіберзлочинів, які мають високий рівень організованості та технологічної складності.

Однією з найбільш поширених загроз є витік даних, який може стосуватися як персональної інформації громадян, так і службових відомостей обмеженого доступу. Подібні інциденти не лише порушують права людини, але й підривають довіру до правоохоронних органів, створюючи ризики для національної безпеки.

Значну небезпеку становлять кібератаки на державні інформаційні системи, що можуть призводити до блокування роботи ресурсів, спотворення або знищення даних, а також до несанкціонованого доступу до критичної інформації. Особливо вразливими є системи, що забезпечують обмін даними між різними органами, оскільки їх компрометація має масштабні наслідки.

Не менш актуальними залишаються такі загрози, як фішинг та шкідливе програмне забезпечення, які активно використовуються для отримання доступу до службових акаунтів, мереж і баз даних. Вони часто базуються на маніпуляції людською довірою та недостатній обізнаності користувачів, що значно підвищує їх ефективність.

Окрему групу становлять внутрішні загрози, пов'язані з людським фактором. Це можуть бути як навмисні дії працівників (зловживання доступом, передача інформації), так і випадкові помилки, спричинені недостатнім рівнем підготовки або неуважністю. Саме такі загрози є одними з найскладніших для виявлення та контролю.

Сучасні загрози інформаційній безпеці у правоохоронній сфері мають комплексний характер і постійно еволюціонують. Традиційні методи захисту, що базуються переважно на статичних підходах і реактивному реагуванні, дедалі частіше виявляються недостатньо ефективними, що зумовлює потребу у впровадженні більш гнучких, інтелектуально орієнтованих систем безпеки.

Можливості штучного інтелекту у забезпеченні інформаційної безпеки. Сучасний розвиток інформаційних технологій зумовлює активне впровадження штучного інтелекту у сферу забезпечення інформаційної безпеки, що відкриває принципово нові можливості для протидії кіберзагрозам. Особливого значення це набуває у правоохоронній діяльності, де швидкість обробки інформації, точність аналізу та своєчасність реагування мають критичне значення.

Як зазначається у праці О. Трофименко, Н. Логінової, А. Соколова, П. Чикунова та Г. Ахмаметьєвої, застосування технологій штучного інтелекту забезпечує ефективне опрацювання великих масивів різнорідної інформації – текстової, графічної, аудіо- та відео. Це дозволяє своєчасно виявляти потенційні загрози, формувати доказову базу та підвищувати ефективність роботи правоохоронних органів. Використання машинного навчання, нейронних мереж, розпізнавання образів і обробки природної мови забезпечує аналіз великих даних, виявлення закономірностей і підтримку прийняття рішень [24].

Важливою перевагою штучного інтелекту є здатність до виявлення аномалій у роботі інформаційних систем. Як підкреслюють У. Околі та співавтори, алгоритми машинного навчання дозволяють аналізувати поведінкові характеристики мереж і систем, ідентифікуючи як відомі, так і нові типи атак. Це значно підвищує точність виявлення кіберзагроз і мінімізує ризики несанкціонованого доступу [9].

Поряд із цим, сучасні підходи орієнтовані на прогнозування атак. На думку А. Редді, штучний інтелект дозволяє аналізувати поведінку користувачів, мережеві процеси та вразливості систем, що дає змогу передбачати потенційні загрози ще до їх реалізації. Такий підхід забезпечує перехід від реактивної до проактивної моделі захисту [10].

Як зазначають А. Таніконда та співавтори, інтелектуальні системи кібербезпеки забезпечують автоматизацію реагування на кіберзагрози, адаптуючи механізми захисту відповідно до змін у поведінці

атакуючих. Це підвищує гнучкість і стійкість інформаційних систем у складних цифрових середовищах [14].

Окремо варто відзначити розвиток автономних рішень. Зокрема, Н. Кшетрі звертає увагу на впровадження agentic AI, який здатний у режимі реального часу здійснювати виявлення, аналіз і нейтралізацію кіберзагроз. Такі системи суттєво скорочують час реагування, зменшують вплив людського фактора та підвищують ефективність роботи центрів кібербезпеки [5].

Інтеграція технологій штучного інтелекту у правоохоронну діяльність сприяє суттєвому підвищенню ефективності обробки та аналізу інформації. Зокрема, використання алгоритмів машинного навчання дозволяє автоматизувати рутинні процеси, здійснювати глибокий аналіз судової практики, прогнозувати результати судових рішень та виявляти потенційні ризики. Це забезпечує більш обґрунтоване прийняття рішень, підвищує швидкість реагування правоохоронних органів та сприяє ефективнішому запобіганню правопорушенням [19].

Крім того, важливу роль відіграють біометричні системи, що базуються на технологіях розпізнавання обличчя, голосу чи поведінкових характеристик. Вони використовуються для ідентифікації осіб, контролю доступу та запобігання несанкціонованому втручанню в інформаційні системи, що є особливо актуальним у правоохоронній сфері.

Узагальнюючи, можна зазначити, що штучний інтелект суттєво розширює можливості забезпечення інформаційної безпеки, забезпечуючи перехід до більш точних, швидких і проактивних моделей захисту. Його використання дозволяє не лише ефективніше реагувати на загрози, а й передбачати їх виникнення, що робить системи безпеки більш стійкими до сучасних викликів.

Застосування штучного інтелекту у правоохоронній діяльності. Сучасна правоохоронна діяльність дедалі активніше інтегрує технології штучного інтелекту, що зумовлено необхідністю швидкого реагування на нові форми злочинності, насамперед у цифровому середовищі. При цьому, як зазначає С. Скрипник, інтеграція ШІ має і певні технічні обмеження, зокрема пов’язані з якістю та доступністю даних, складністю інтеграції, масштабованістю систем, а також потребою у постійному обслуговуванні та технічній підтримці. Це свідчить про те, що ефективність таких технологій значною мірою залежить від умов їх впровадження [22].

Одним із ключових напрямів є розслідування кіберзлочинів, де штучний інтелект використовується для аналізу цифрових слідів, мережевої активності та виявлення зв’язків між правопорушниками. Як зазначається у працях Н. Сінхи та А. Алока, алгоритми машинного навчання дозволяють обробляти великі обсяги даних, виявляти аномалії та ідентифікувати організовані злочинні групи, що суттєво підвищує ефективність розслідувань [12].

Важливе місце займають технології розпізнавання облич та комп’ютерного зору, які дозволяють аналізувати відео- та фотоматеріали, ідентифікувати осіб і фіксувати підозрілу поведінку. Як підкреслюють А. Шаббір та співавтори, застосування алгоритмів глибокого навчання у реальному часі забезпечує моніторинг публічних просторів і підтримку прийняття рішень у складних ситуаціях. Наприклад, такі системи можуть автоматично ідентифікувати розшукувану особу серед великого потоку людей або зафіксувати нетипову поведінку у місцях масового скупчення [11].

Окремим напрямом є аналіз відео та великих масивів даних, а також текстової інформації. Використання технологій обробки природної мови дозволяє аналізувати судові документи, повідомлення у соціальних мережах та електронне листування, виявляючи закономірності злочинної діяльності та встановлюючи зв’язки між суб’єктами. Це, у свою чергу, значно підсилює аналітичні можливості правоохоронних органів [8].

Перспективним напрямом є також прогнозування злочинності. Як зазначають П. Гейлі та Д. Баррелл, поєднання штучного інтелекту з геопросторовим профілюванням дозволяє визначати зони підвищеного ризику та прогнозувати ймовірність вчинення правопорушень. Наприклад, на основі аналізу попередніх інцидентів система може визначити райони з найбільшою ймовірністю повторення злочинів і спрямувати туди ресурси [2].

Не менш важливим є розвиток цифрової криміналістики, де штучний інтелект використовується для автоматизованого аналізу цифрових доказів, відновлення даних та встановлення послідовності подій. У цьому контексті дослідники звертають увагу на появу нових підходів, зокрема так званого «цифрового арешту», коли доступ до ресурсів може бути обмежений автоматично на основі виявлених порушень, що, однак, потребує особливої уваги до дотримання прав людини.

Узагальнюючи, можна сказати, що штучний інтелект суттєво змінює характер правоохоронної діяльності, переводячи її від реактивної до проактивної моделі. Він дозволяє швидше обробляти інформацію, точніше виявляти загрози та приймати більш обґрунтовані рішення. Водночас ефективність його застосування залежить не лише від технологічних можливостей, а й від якості даних, правового регулювання та здатності забезпечити баланс між безпекою і правами людини.

Проблеми та ризики використання штучного інтелекту. Активне впровадження штучного інтелекту у сферу інформаційної безпеки та правоохоронної діяльності поряд із очевидними перевагами супроводжується низкою суттєвих проблем і ризиків, які потребують глибокого наукового осмислення. Це зумовлено тим, що інтелектуальні технології змінюють не лише інструменти забезпечення безпеки, а й сам характер загроз.

Як зазначає А. Майо, штучний інтелект виступає як технологія подвійного призначення: з одного боку, він підвищує ефективність правоохоронної діяльності, а з іншого – створює нові можливості для вчинення злочинів. Його застосування охоплює широкий спектр напрямів – від предиктивної аналітики та цифрової криміналістики до використання у шахрайських схемах, створенні deepfake та автоматизованих кібератаках. Така подвійна природа вимагає комплексного підходу до забезпечення інформаційної безпеки, з урахуванням як можливостей, так і потенційних загроз [7].

Однією з ключових проблем є помилки алгоритмів, які можуть виникати внаслідок недосконалості моделей або обмеженості навчальних даних. У складних правових ситуаціях такі помилки здатні призводити до хибних рішень, що має критичні наслідки у правоохоронній діяльності. Тісно пов'язаною є проблема упередженості (bias), коли алгоритми відтворюють або навіть підсилюють існуючі соціальні чи статистичні перекоси, що може спричиняти дискримінаційні рішення.

Суттєвим ризиком є також порушення прав людини, зокрема у випадках автоматизованого прийняття рішень без належного контролю. Обмежена прозорість функціонування алгоритмів ускладнює перевірку їх обґрунтованості, що підвищує ризик неправомірних дій. Водночас актуальною залишається проблема конфіденційності даних, оскільки використання великих масивів інформації створює загрозу їх витоку або несанкціонованого доступу [19]. Як підкреслюють зарубіжні науковці, інтеграція штучного інтелекту в системи кібербезпеки має подвійний ефект: підвищуючи ефективність захисту, вона одночасно створює нові вразливості. Технології, що застосовуються для виявлення загроз, можуть використовуватися і зловмисниками для створення більш складних атак, генерації маніпулятивного контенту та обходу захисних механізмів [1, 6, 15].

У цьому контексті Г. Вайцель звертає увагу на феномен «гонки озброєнь» у кібербезпеці, де як захисники, так і атакуючі активно використовують штучний інтелект. Це призводить до постійного ускладнення кіберзагроз і потребує безперервного вдосконалення систем захисту [16].

На думку Н. Кшетрі, впровадження автономних систем штучного інтелекту розширює можливості кіберзахисту, але водночас збільшує площу потенційних атак. Такі системи взаємодіють із великою кількістю даних і середовищ, що створює нові вразливості, зокрема ризики витоку даних, несанкціонованого доступу та маніпуляції алгоритмами. Це вимагає переходу до ризик-орієнтованих моделей безпеки, які враховують взаємозв'язок між загрозами, вразливостями та наслідками [5].

Додаткові виклики пов'язані з розвитком технологій deepfake, які ускладнюють боротьбу з кіберзлочинністю та сприяють поширенню дезінформації. Водночас правоохоронні органи стикаються з організаційними труднощами: обмеженістю ресурсів, складністю виявлення нових загроз та необхідністю міжнародної координації. Особливої складності набуває транснаціональний характер кіберзлочинності, який ускладнює взаємодію між державами.

Важливим аспектом, на який звертає увагу дослідник, є необхідність переосмислення існуючих підходів до кібербезпеки, оскільки традиційні моделі захисту не враховують особливостей автономних інтелектуальних систем. У зв'язку з цим виникає потреба у впровадженні ризик-орієнтованих моделей управління безпекою, які враховують взаємозв'язок між загрозами, вразливостями та можливими наслідками [5].

Окремою проблемою є відсутність єдиного правового регулювання, зокрема щодо збору, збереження та використання цифрових доказів. Різні правові системи по-різному визначають межі відповідальності за використання штучного інтелекту, що створює труднощі у правозастосовній практиці та розслідуванні злочинів.

Узагальнюючи, можна зазначити, що використання штучного інтелекту у сфері безпеки має суперечливий характер: воно одночасно підсилює можливості захисту та генерує нові ризики. Саме тому ефективне впровадження таких технологій потребує не лише технічного розвитку, а й чіткого правового регулювання, етичного контролю та постійного вдосконалення підходів до забезпечення інформаційної безпеки.

Шляхи підвищення ефективності використання штучного інтелекту у правоохоронній діяльності. Сучасні виклики у сфері інформаційної та кібербезпеки вимагають не лише впровадження інноваційних технологій, але й формування комплексного підходу до їх ефективного використання. У цьому контексті підвищення результативності застосування штучного інтелекту у правоохоронній діяльності має ґрунтуватися на поєднанні технологічних, організаційних та правових рішень.

Передусім важливим напрямом є системне впровадження AI-технологій у діяльність правоохоронних органів. Йдеться не про фрагментарне використання окремих інструментів, а про створення цілісної цифрової інфраструктури, у межах якої штучний інтелект інтегрується у ключові процеси – від аналітики та моніторингу до розслідування та прогнозування правопорушень. Такий підхід дозволяє забезпечити узгодженість дій, підвищити швидкість обробки інформації та мінімізувати втрати даних.

Не менш значущим є питання підготовки фахівців, здатних ефективно працювати з інтелектуальними системами. Практика показує, що навіть найсучасніші технології не дають очікуваного результату без належного кадрового забезпечення. У зв'язку з цим необхідно розвивати міждисциплінарну підготовку, яка поєднує знання у сфері права, інформаційних технологій та кібербезпеки. Особливу увагу доцільно приділяти формуванню навичок критичного аналізу результатів роботи штучного інтелекту, що дозволить уникнути безумовної довіри до алгоритмічних рішень.

Важливим чинником підвищення ефективності є розробка та вдосконалення нормативно-правової бази, яка регулює використання штучного інтелекту у правоохоронній діяльності. Йдеться про визначення правового статусу таких систем, встановлення меж їх застосування, а також чітке закріплення відповідальності за прийняті рішення. Наявність прозорих і зрозумілих правил сприятиме не лише підвищенню ефективності роботи, але й зміцненню довіри суспільства до правоохоронних органів.

У сучасних умовах особливого значення набуває інтеграція національних підходів із міжнародними стандартами у сфері кібербезпеки та захисту даних. Це дозволяє забезпечити сумісність інформаційних систем, підвищити ефективність міжнародної співпраці у боротьбі з кіберзлочинністю та сприяти обміну досвідом. Орієнтація на міжнародні практики також створює передумови для гармонізації законодавства та впровадження найкращих світових рішень.

Окрему увагу доцільно приділити використанню гібридних моделей взаємодії «людина – штучний інтелект». Попри високий рівень автоматизації, саме людина повинна залишатися ключовим суб'єктом прийняття рішень, особливо у складних правових ситуаціях. Штучний інтелект у цьому випадку виступає інструментом підтримки, який забезпечує швидкий аналіз даних і формування рекомендацій, тоді як остаточне рішення приймається з урахуванням правових, етичних та соціальних аспектів. Такий підхід дозволяє поєднати точність алгоритмів із критичним мисленням людини, мінімізуючи ризики помилок.

Крім того, доцільним є впровадження механізмів контролю та аудиту роботи інтелектуальних систем, що передбачають регулярну перевірку їх ефективності, точності та відповідності встановленим стандартам. Це сприятиме своєчасному виявленню недоліків і підвищенню надійності таких систем.

Узагальнюючи, можна стверджувати, що підвищення ефективності використання штучного інтелекту у правоохоронній діяльності можливе лише за умови комплексного підходу, який поєднує технологічний розвиток, підготовку кадрів, нормативне забезпечення та дотримання міжнародних стандартів. Саме така інтеграція створює передумови для формування сучасної, гнучкої та ефективної системи забезпечення інформаційної безпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, проведене дослідження дозволяє дійти висновку, що штучний інтелект поступово перетворюється на один із ключових інструментів підвищення ефективності забезпечення інформаційної безпеки у правоохоронній сфері. Його застосування змінює саму логіку безпекової діяльності – від реагування на вже вчинені правопорушення до їх своєчасного виявлення, прогнозування та попередження. Штучний інтелект дуже добре вміє обробляти значні обсяги різнорідної інформації, виявляти приховані закономірності та оперативно реагувати на загрози, що суттєво підсилює аналітичні та управлінські можливості правоохоронних органів. Водночас результати дослідження свідчать, що ефективність використання штучного інтелекту не є автоматичною і залежить від низки умов. Йдеться насамперед про якість даних, рівень технічного забезпечення, професійну підготовку кадрів, а також наявність чітких правових і організаційних механізмів його застосування. Особливого значення набуває необхідність дотримання балансу між технологічною доцільністю та захистом прав людини, адже використання інтелектуальних систем у правоохоронній діяльності без належного контролю може створювати додаткові ризики.

Аналіз проблем і ризиків показав, що розвиток штучного інтелекту має суперечливий характер: поряд із розширенням можливостей безпеки виникають нові виклики, пов'язані з помилками алгоритмів, їх упередженістю, загрозами конфіденційності та недостатнім рівнем правового регулювання. Крім того, активне використання штучного інтелекту зловмисниками ускладнює боротьбу з кіберзлочинністю та потребує постійного вдосконалення підходів до захисту інформаційних систем. У цьому контексті

підвищення ефективності застосування штучного інтелекту у правоохоронній сфері можливе лише за умови комплексного підходу, що передбачає інтеграцію сучасних технологій у діяльність органів правопорядку, розвиток професійних компетентностей фахівців, удосконалення нормативно-правової бази та орієнтацію на міжнародні стандарти. Важливим є також впровадження гібридних моделей взаємодії, у межах яких штучний інтелект виступає інструментом підтримки прийняття рішень, а ключова роль зберігається за людиною.

Перспективи подальших досліджень пов'язані з поглибленим вивченням механізмів інтеграції штучного інтелекту у правоохоронну діяльність, розробкою ефективних моделей оцінки ризиків його застосування, а також формуванням підходів до забезпечення прозорості та підзвітності інтелектуальних систем. Окремої уваги потребують питання правового регулювання використання штучного інтелекту, стандартизації цифрових доказів і вдосконалення міжнародної співпраці у сфері протидії кіберзлочинності. Сукупність цих напрямів визначає подальший розвиток наукових досліджень і практичних рішень у сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Danish, M., & Siraj, M. M. (2025). AI and cybersecurity: Defending data and privacy in the digital age. *Journal of Engineering and Computational Intelligence Review (JECIR), 3*(1), 25-35. https://jecir.com/
2. Haley, P., & Burrell, D. N. (2025). Using artificial intelligence in law enforcement and policing to improve public health and safety. *Law, Economics and Society, 1*(1), 46. https://doi.org/10.30560/les.v1n1p46
3. Halford, E. (2025). The transformer-led policing model: A framework for applying generative artificial intelligence in policing. *Policing: A Journal of Policy and Practice, 19*. https://doi.org/10.1093/police/paaf027
4. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*. https://doi.org/10.1016/j.inffus.2023.101804
5. Kshetri, N. (2025). Transforming cybersecurity with agentic AI to combat emerging cyber threats. *Telecommunications Policy, 49*(6), 102976. https://doi.org/10.1016/j.telpol.2025.102976
6. Lin, L. S. F. (2025). Organisational challenges in U.S. law enforcement's response to AI-driven cybercrime and deepfake fraud. *Laws, 14*(4), 46. https://doi.org/10.3390/laws14040046
7. Maio, A. (2025). *Artificial intelligence and crime: The dual role of AI in criminal activity and crime prevention*. Zenodo. https://doi.org/10.5281/zenodo.16945903
8. Nalutsyshyn, V., Nalutsyshyn, V., & Golovchak, R. (2025). Foreign experience in the application of artificial intelligence in law enforcement activities. *Socio-Economic Relations in the Digital Society, 3*(57). https://doi.org/10.55643/ser.3.57.2025.617
9. Okoli, U. I., et al. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews, 21*(1), 2286-2295.
10. Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology, 19*(12), 764-773.
11. Shabbir, A., et al. (2024). Analyzing surveillance videos in real time using AI-powered deep learning techniques. *International Journal of Recent Innovative Trends in Computing and Communication, 12*(2), 950-960.
12. Sinha, N., & Alok, A. (2025). Building trust in digital governance: A cybersecurity imperative with specific reference to Jharkhand. *Economic Sciences, 21*(2), 198-207.
13. Srivastava, G., et al. (2022). *XAI for cybersecurity: State of the art, challenges, open issues and future directions*. arXiv. https://doi.org/10.48550/arXiv.2206.03585
14. Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. *Journal of Science and Technology, 3*(1), 1-15.
15. Velasco, C. (2022). Cybercrime and artificial intelligence: An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum, 23*(1), 109-126. https://doi.org/10.1007/s12027-022-00702-z
16. Waizel, G. (2024). Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses. In *Proceedings of the International Conference on Machine Intelligence, Security and Smart Cities (TRUST)* (Vol. 1, pp. 141-156).
17. Cabinet of Ministers of Ukraine. (2020). *Concept of artificial intelligence development in Ukraine*. https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80

18. Latkovska, T. A., & Marushchak, A. V. (2025). Integration of artificial intelligence into law enforcement activities: Risks in the context of cybersecurity. *Public Administration and State Building*, *1*, 355-361.
19. Muravska, Y., Metelskyi, I., & Romaniv, R. (2024). Prospects for the use of artificial intelligence technologies in jurisprudence and law enforcement activities. *Actual Problems of Jurisprudence*, *2*, 90-96. https://doi.org/10.35774/app2024.02.090
20. Verkhovna Rada of Ukraine. (2017). *On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII*. https://zakon.rada.gov.ua/laws/show/2163-19
21. Skitsko, O., Skladannyi, P., Shyrshov, R., Humeniuk, M., & Vorokhob, M. (2023). Threats and risks of artificial intelligence use. *Information Technology and Security*, *2*. https://doi.org/10.28925/2663-4023.2023.22.618
22. Skrypnyk, S. S. (2025). Technical limitations in the use of artificial intelligence in law enforcement activities. In *Artificial intelligence in legal practice: Limits and opportunities* (pp. 188–190). Lviv.
23. President of Ukraine. (2021). *Cybersecurity Strategy of Ukraine*. https://zakon.rada.gov.ua/laws/show/447/2021
24. Trofymenko, O. H., et al. (2024). Artificial intelligence in the military sphere. *Information Technology and Security*, *1*, 161-176. https://doi.org/10.28925/2663-4023.2024.25.161176
25. Shevchuk, V. M. (2024). The role of artificial intelligence technologies in law enforcement activities and ensuring the security and defense capability of Ukraine. *Legal Scientific Electronic Journal*, *6*, 356-361. https://doi.org/10.32782/2524-0374/2024-6/88

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Oleksandr Kyryliuk
PhD in Technology, Senior Researcher, Senior Lecturer
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID: 0000-0001-9248-0758
20kiril20@gmail.com

ARTIFICIAL INTELLIGENCE AS A TOOL FOR IMPROVING THE EFFICIENCY OF INFORMATION SECURITY IN THE LAW ENFORCEMENT SECTOR

Abstract. The article examines the role of artificial intelligence as a modern tool for improving the efficiency of information security in the law enforcement sector. The introduction substantiates the relevance of the topic in the context of digital transformation, the growing number of cyber threats, and the transformation of the information space into a domain of confrontation. The theoretical section defines the essence of key concepts, including «artificial intelligence», «information security», «cybersecurity», and «law enforcement activity», and analyzes contemporary scientific approaches to their interpretation. It is determined that artificial intelligence functions as an integrated component of the security management system, capable of ensuring a continuous cycle of threat detection, response, and recovery from cyber incidents. The results section provides an analysis of threats to information security in the law enforcement sector, including data breaches, cyberattacks, phishing, and insider threats. The capabilities of artificial intelligence are substantiated in terms of processing large volumes of data, detecting anomalies, predicting threats, and automating decision-making processes. The main directions of AI application in law enforcement are outlined, including cybercrime investigation, the use of biometric systems, analysis of textual and visual information, and predictive analytics. Special attention is paid to the challenges and risks associated with the use of artificial intelligence, such as algorithmic errors, bias, data privacy concerns, and insufficient legal regulation. The article proposes ways to improve the effectiveness of AI implementation through a comprehensive approach that combines technological, human resource, and legal aspects. It is concluded that maintaining a balance between security efficiency and the protection of human rights is essential. Prospects for further research are outlined, particularly in relation to improving mechanisms for integrating artificial intelligence into law enforcement activities and enhancing the transparency of its application.

Keywords: artificial intelligence; information security; cybersecurity; law enforcement; cyber threats; machine learning; digital forensics.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Danish, M., & Siraj, M. M. (2025). AI and cybersecurity: Defending data and privacy in the digital age. *Journal of Engineering and Computational Intelligence Review (JECIR), 3*(1), 25-35. https://jecir.com/
2. Haley, P., & Burrell, D. N. (2025). Using artificial intelligence in law enforcement and policing to improve public health and safety. *Law, Economics and Society, 1*(1), 46. https://doi.org/10.30560/les.v1n1p46
3. Halford, E. (2025). The transformer-led policing model: A framework for applying generative artificial intelligence in policing. *Policing: A Journal of Policy and Practice, 19*. https://doi.org/10.1093/police/paaf027
4. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*. https://doi.org/10.1016/j.inffus.2023.101804
5. Kshetri, N. (2025). Transforming cybersecurity with agentic AI to combat emerging cyber threats. *Telecommunications Policy, 49*(6), 102976. https://doi.org/10.1016/j.telpol.2025.102976
6. Lin, L. S. F. (2025). Organisational challenges in U.S. law enforcement's response to AI-driven cybercrime and deepfake fraud. *Laws, 14*(4), 46. https://doi.org/10.3390/laws14040046
7. Maio, A. (2025). *Artificial intelligence and crime: The dual role of AI in criminal activity and crime prevention*. Zenodo. https://doi.org/10.5281/zenodo.16945903
8. Nalutsyshyn, V., Nalutsyshyn, V., & Golovchak, R. (2025). Foreign experience in the application of artificial intelligence in law enforcement activities. *Socio-Economic Relations in the Digital Society, 3*(57). https://doi.org/10.55643/ser.3.57.2025.617

9. Okoli, U. I., et al. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews, 21*(1), 2286-2295.
10. Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology, 19*(12), 764-773.
11. Shabbir, A., et al. (2024). Analyzing surveillance videos in real time using AI-powered deep learning techniques. *International Journal of Recent Innovative Trends in Computing and Communication, 12*(2), 950-960.
12. Sinha, N., & Alok, A. (2025). Building trust in digital governance: A cybersecurity imperative with specific reference to Jharkhand. *Economic Sciences, 21*(2), 198-207.
13. Srivastava, G., et al. (2022). *XAI for cybersecurity: State of the art, challenges, open issues and future directions*. arXiv. https://doi.org/10.48550/arXiv.2206.03585
14. Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. *Journal of Science and Technology, 3*(1), 1-15.
15. Velasco, C. (2022). Cybercrime and artificial intelligence: An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum, 23*(1), 109-126. https://doi.org/10.1007/s12027-022-00702-z
16. Waizel, G. (2024). Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses. In *Proceedings of the International Conference on Machine Intelligence, Security and Smart Cities (TRUST)* (Vol. 1, pp. 141-156).
17. Cabinet of Ministers of Ukraine. (2020). *Concept of artificial intelligence development in Ukraine*. https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80
18. Latkovska, T. A., & Marushchak, A. V. (2025). Integration of artificial intelligence into law enforcement activities: Risks in the context of cybersecurity. *Public Administration and State Building, 1*, 355-361.
19. Muravska, Y., Metelskyi, I., & Romaniv, R. (2024). Prospects for the use of artificial intelligence technologies in jurisprudence and law enforcement activities. *Actual Problems of Jurisprudence, 2*, 90-96. https://doi.org/10.35774/app2024.02.090
20. Verkhovna Rada of Ukraine. (2017). *On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII*. https://zakon.rada.gov.ua/laws/show/2163-19
21. Skitsko, O., Skladannyi, P., Shyrshov, R., Humeniuk, M., & Vorokhob, M. (2023). Threats and risks of artificial intelligence use. *Information Technology and Security, 2*. https://doi.org/10.28925/2663-4023.2023.22.618
22. Skrypnyk, S. S. (2025). Technical limitations in the use of artificial intelligence in law enforcement activities. In *Artificial intelligence in legal practice: Limits and opportunities* (pp. 188–190). Lviv.
23. President of Ukraine. (2021). *Cybersecurity Strategy of Ukraine*. https://zakon.rada.gov.ua/laws/show/447/2021
24. Trofymenko, O. H., et al. (2024). Artificial intelligence in the military sphere. *Information Technology and Security, 1*, 161-176. https://doi.org/10.28925/2663-4023.2024.25.161176
25. Shevchuk, V. M. (2024). The role of artificial intelligence technologies in law enforcement activities and ensuring the security and defense capability of Ukraine. *Legal Scientific Electronic Journal, 6*, 356-361. https://doi.org/10.32782/2524-0374/2024-6/88

Отримано редакцією журналу / Received: 23.02.26
Прорецензовано / Revised: 02.03.26
Схвалено до друку / Accepted: 25.06.26