МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Інститут заочного та дистанційного навчання

Кафедра кримінології та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА
для здобуття ступеня вищої освіти магістра

на тему: **«Можливості застосування систем штучного інтелекту в публічному адмініструванні МВС України»**

Виконав: здобувач 2 курсу 2 групи
Спеціальність: 281 «Публічне управління та адміністрування»

Фесюн Сергій Володимирович
Індивідуальний навчальний план № 14-100
Мобільний телефон: +380 93-505-08-26

Науковий керівник:
старший викладач кафедри,
кандидат юридичних наук
Пустовий Олександр Олександрович
(підпис)

Кваліфікаційна робота допущена до захисту
«11» грудня 2025 р., протокол № 07
завідувач кафедри, доктор філософії в галузі
права, доцент
Владислав ШКОЛЬНІКОВ

Київ 2025

ЗМІСТ

ВСТУП

Актуальність теми. Трансформація публічного управління в умовах цифровізації є одним із ключових викликів сучасного державотворення. У цьому контексті органи системи Міністерства внутрішніх справ України опинилися в центрі структурних змін, спрямованих на підвищення якості управлінських процесів, забезпечення безпеки, вдосконалення комунікації з громадянами та оптимізацію службової діяльності. Застосування систем штучного інтелекту (ШІ) у роботі МВС є не просто технологічною інновацією, а необхідністю, що зумовлена зростанням обсягу даних, ускладненням суспільних викликів, а також потребою оперативного прийняття рішень на основі достовірної аналітики.

Штучний інтелект уже використовується у провідних державах світу для прогнозування злочинності, автоматизації адміністративних процедур, оптимізації ресурсів, кіберзахисту, роботи з базами даних та комунікацій із населенням. Європейський Союз формує нормативну базу, зокрема шляхом ухвалення AI Act, що передбачає регулювання використання інтелектуальних технологій у публічному секторі з урахуванням принципів етики, прозорості та прав людини. Україна, як держава, що здійснює курс на євроінтеграцію, зобов’язана адаптувати ці стандарти, особливо у сфері діяльності МВС, де йдеться про захист прав громадян, забезпечення порядку та ефективне управління безпекою.

Незважаючи на певні напрацювання в МВС у сфері цифрових сервісів, практичне використання систем штучного інтелекту є фрагментарним, обмеженим нормативно й організаційно. Дослідження демонструють потенціал інтелектуальних рішень для підвищення ефективності роботи поліції, спрощення бюрократичних процесів, прогнозування загроз та боротьби з організованою злочинністю. Однак залишається невирішеним комплекс питань щодо етичних, правових, безпекових і методологічних аспектів впровадження. Недостатньо опрацьовані питання стандартизації баз даних, алгоритмічної відповідальності,

захисту персональних даних, підготовки персоналу та інтеграції ШІ в існуючі управлінські структури.

Зазначені фактори визначають актуальність наукового дослідження, орієнтованого на аналіз можливостей, обмежень і перспектив застосування штучного інтелекту в публічному адмініструванні МВС України. Розв'язання цих завдань сприятиме розробці ефективної моделі цифрової трансформації міністерства відповідно до світових тенденцій, державних стратегічних документів і політики безпеки.

Мета дослідження полягає у визначенні можливостей, викликів та практичних шляхів запровадження систем штучного інтелекту в процеси публічного адміністрування в МВС України з урахуванням нормативного, організаційного й технологічного контекстів.

Для досягнення мети передбачається виконання таких завдань:

– узагальнити теоретико-методологічні засади впровадження штучного інтелекту в публічне управління;

– проаналізувати сучасний стан нормативного, кадрового та технічного забезпечення цифрових процесів у МВС України;

– виявити ключові проблеми, ризики та етичні виклики, пов'язані із застосуванням штучного інтелекту в роботі органів МВС;

– запропонувати концептуальну модель та практичні рекомендації щодо впровадження інтелектуальних систем у діяльність МВС України;

– визначити перспективи функціонування штучного інтелекту в конкретних підрозділах (наприклад, під час аналітичної роботи, обробки даних, управління ресурсами або забезпечення громадської безпеки).

Об'єкт дослідження – процеси цифрової трансформації та управління в системі Міністерства внутрішніх справ України.

Предмет дослідження – можливості, механізми та умови застосування систем штучного інтелекту в публічному адмініструванні МВС України.

Елементи наукової новизни полягають у уточненні теоретичного понятійного апарату щодо використання штучного інтелекту в публічному

управлінні; розробленні авторської моделі інтеграції систем ШІ у практику публічного адміністрування МВС; формулюванні пропозицій щодо удосконалення нормативного забезпечення й організаційної структури впровадження інтелектуальних технологій.

Методологічну основу дослідження становлять системний, порівняльно-правовий, структурно-функціональний і прогностичний методи, метод контент-аналізу, аналіз нормативно-правових актів, а також аналіз кращих міжнародних практик у сфері використання інтелектуальних технологій у публічному секторі. Дослідження ґрунтується на положеннях теорії публічного адміністрування, інституційного аналізу, концепції цифрової трансформації та сучасного державного управління.

Практичне значення результатів полягає у можливості використання отриманих висновків та рекомендацій для підготовки стратегічних документів та програм цифровізації МВС; розроблення прикладних рішень і пілотних проєктів на основі ШІ; удосконалення управлінських процесів і сервісів із використанням інтелектуальних технологій; оптимізації організаційної структури та підвищення ефективності діяльності підрозділів МВС України.

Апробація результатів може бути здійснена під час участі в науково-практичних конференціях, круглих столах та семінарах з питань публічного управління, цифрових трансформацій і застосування штучного інтелекту у сфері безпеки.

Таким чином, обрана тема відповідає сучасним потребам публічного управління, характеризується високою практичною значущістю і відкриває можливості для впровадження новітніх технологічних рішень у діяльність МВС України, що є актуальним у контексті євроінтеграційного курсу держави, необхідності посилення спроможності правоохоронних органів і формування безпечного цифрового середовища.

РОЗДІЛ І ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ АДМІНІСТРУВАННІ

1.1. Сутність і концептуальні підходи до впровадження штучного інтелекту в органах державної влади

Одним із ключових напрямів трансформації діяльності Міністерства внутрішніх справ України (МВС) у сучасних умовах є впровадження інтелектуальних інформаційно-аналітичних систем, побудованих з використанням технологій штучного інтелекту (ШІ). Це зумовлено як потребами підвищення ефективності управлінських процесів і оперативно-службової діяльності, так і необхідністю адаптації до викликів воєнного стану, гібридних загроз та цифрової еволюції суспільства.

Системи штучного інтелекту є інструментами, які дозволяють автоматизувати обробку великих масивів даних, здійснювати прогнозування, підтримувати прийняття рішень, виявляти аномальні явища та підвищувати рівень інформаційної безпеки. У сфері публічного управління такі системи забезпечують оперативність реагування на ризики, прозорість діяльності органів влади, превентивність заходів, а також підвищують рівень сервісності для громадян [66].

У теоретичних дослідженнях публічного управління наголошується, що штучний інтелект у системах влади не є окремою технологією, а представляє собою комплексну соціотехнічну систему, яка поєднує алгоритмічні можливості з управлінськими процесами та нормативно-правовим регулюванням [28, с.29]. Згідно з концепцією «інтелектуального урядування» (smart governance), застосування ШІ забезпечує перехід від реактивного реагування на виклики до проактивного управління, заснованого на аналізі даних, системному прогнозуванні та інтегрованому прийнятті рішень.

Теоретичні засади використання ШІ у владі базуються на трьох ключових принципах:

1. Системність та інтегрованість, що передбачає застосування ШІ не лише для окремих задач, а на рівні всієї публічної інфраструктури. За П. Дрейером, штучний інтелект дозволяє поєднувати розрізнені інформаційні потоки, створюючи цифрові екосистеми, які підтримують складні управлінські операції та забезпечують прозорість [51, с.7].

2. Пояснюваність і підзвітність. У публічному секторі принципи explainable AI (XAI) стають критично важливими, оскільки автоматизовані рішення мають відповідати стандартам правової визначеності й підлягати аудиту. Європейська комісія у своїх рекомендаціях наголошує на необхідності жорстких критеріїв оцінки алгоритмічної упередженості, прозорості та контролю за автоматизованими рішеннями [57].

3. Гнучкість і адаптивність. Системи управління, які використовують ШІ, мають здатність до машинного навчання та адаптації на основі зворотного зв'язку. Це дає можливість покращувати якість державних послуг і діяти в умовах невизначеності, що особливо актуально в періоди соціальних криз чи військових конфліктів [72].

У цьому контексті В. Орлов наголошує на тому, що розробка програм розвитку штучного інтелекту повинна здійснюватися з урахуванням принципів алгоритмічної етики, забезпечення рівного доступу до послуг і гарантування недискримінації за результатами роботи цифрових систем [40, с.53]. Усе це формує нову парадигму державного управління – «algorithmic governance», у якій рішення приймаються на основі даних і моделювання поведінки суспільних процесів, а роль держави полягає у регулюванні контурів використання таких алгоритмів.

Загалом, впровадження ШІ у державне управління передбачає комплекс змін:

- трансформацію процесів збору, обробки та зберігання даних;
- модернізацію технічної інфраструктури;
- формування нових компетентностей у державних службовців;

- розробку правових та етичних рамок використання алгоритмічних рішень.

Низка міжнародних організацій, включно з ОЕСР, наголошує, що успішне впровадження ШІ може суттєво підвищити ефективність адміністративних процесів, однак ключовим є забезпечення балансу між технологічними можливостями та демократичним контролем [66].

Таким чином, концептуальні підходи до впровадження штучного інтелекту в органах влади ґрунтуються на необхідності поєднання технологічної інноваційності з принципами верховенства права, етичності, прозорості і громадянського контролю, створюючи основу для переосмислення моделей роботи державних установ.

У контексті МВС України технології ШІ впроваджуються як у центральному апараті, так і на рівні підрозділів Національної поліції, Державної міграційної служби, Державної прикордонної служби та сервісних центрів. До ключових напрямів застосування належать інтелектуальний відеонагляд, криміналістична аналітика, кібербезпека, автоматизація адміністративних процесів, робота зі зверненнями громадян, а також аналітичний супровід оперативно-розшукової діяльності [21].

Особливої уваги заслуговує створення Єдиної системи відеомоніторингу стану публічної безпеки, що вже сьогодні поєднує майже 40 тисяч камер, інтегрованих із сучасними алгоритмами оброблення відеоданих та розпізнавання облич [45]. У 2024 році цей напрям отримав подальший розвиток завдяки внесенню на розгляд Верховної Ради України законопроєкту № 11031 «Про єдину систему відеомоніторингу стану публічної безпеки» [13]. У пояснювальній записці до проєкту вказано, що система має стати основою для розвитку превентивного поліцейського сервісу з використанням технологій машинного навчання, функцій розпізнавання ситуацій та автоматичного виявлення правопорушень. Разом з тим у фаховому середовищі лунають застереження щодо ризиків масового стеження, надмірного втручання держави у приватне життя та недостатності законодавчих гарантій захисту персональних даних [14; 26].

Дискусія навколо впровадження систем ШІ у сферу відеоспостереження є типовою для демократичних суспільств, де необхідні баланс безпеки та приватності.

На нормативному рівні розвиток цифрової інфраструктури та автоматизованих систем в МВС України регулюється низкою стратегічних документів, зокрема Концепцією програми інформатизації системи МВС на 2021–2023 роки [9], Стратегією розвитку органів системи МВС України до 2030 року [12], а також урядовими розпорядженнями у сферах цифрової трансформації та розвитку штучного інтелекту [7; 10]. Це підтверджує системність підходу до впровадження інноваційних технологій і визначає основу для модернізації органів внутрішніх справ у відриві від застарілих моделей управління.

Окремий блок застосувань ШІ стосується оперативно-аналітичної діяльності. Інтелектуальні системи дозволяють виявляти закономірності у масивах оперативної інформації, проводити ризик-аналіз, прогнозувати місця можливого вчинення злочинів та навіть запропонувати оптимальні маршрути патрулювання. За кордоном такі системи використовуються в роботі поліції найбільших мегаполісів, зокрема завдяки системам PredPol та CrimeScan [61]. Українська поліція поки перебуває на початковому етапі застосування подібних рішень, проте перші проєкти впровадження систем прогнозної аналітики вже тестуються у Києві та Львові [21].

Підвищення ефективності правоохоронної діяльності з використанням ШІ стосується не лише її оперативної складової, а й сфери криміналістики та судово-експертної діяльності. У роботах українських науковців наголошується, що автоматизовані алгоритми розпізнавання зображень та текстів дозволяють зменшити ризик людської помилки, пришвидшити обробку доказів і забезпечити збереження цифрового сліду [25; 49]. Проте нині в Україні відсутня єдина система криміналістичної аналітики на базі ШІ, що обмежує ефективність використання цифрових інструментів у боротьбі зі злочинністю. Це визначає потребу в розробці окремої концепції модернізації криміналістичних лабораторій

за міжнародними стандартами, з урахуванням етичних та правових рамок використання інтелектуальних технологій [43].

У контексті публічного адміністрування важливим аспектом є автоматизація взаємодії між громадянами та МВС. Уже сьогодні частина сервісів доступна через застосунок «Дія» та вебпортал МВС, проте саме використання алгоритмів ШІ здатне значно підвищити якість обслуговування, адаптувати відповіді під контекст звернення, оптимізувати обробку запитів і виявляти типові проблеми у структурі сервісів [36; 35]. Важливий досвід у цьому контексті представляють сервісні центри МВС, які в 2024 році розпочали цифрову реформу з акцентом на онлайн-сервіси, усунення черг та повну відмову від паперових форм [35].

Разом із тим впровадження ШІ у публічне адміністрування неможливе без забезпечення належного рівня інформаційної безпеки та кіберзахисту. У 2024 році у Верховній Раді був зареєстрований законопроєкт щодо Єдиної системи відеоспостереження, який передбачає зберігання та обробку масових масивів персональних даних, що вимагає узгодження з вимогами Закону «Про захист персональних даних» [3] та іншими актами у сфері кібербезпеки. У дослідженнях підкреслюється, що ШІ здатний не лише забезпечувати роботу систем захисту, але й сам є джерелом ризиків – алгоритмічні вразливості можуть бути використані для атак на системи безпеки, а помилки алгоритмів – призвести до порушення прав людини [15; 29; 42].

Вітчизняні дослідження підтверджують високий потенціал використання штучного інтелекту як у сфері правоохоронної діяльності [21; 25], так і в управлінських процесах [19; 28], але при цьому визнають, що Україна відстає від західних країн за масштабами та глибиною інтеграції ШІ в роботу правоохоронних органів. Наявна цифрова інфраструктура МВС справді потребує модернізації, відсутність єдиних стандартів обміну даними, обмеженість аналітичних ресурсів та недостатній рівень цифрових компетентностей держслужбовців гальмують розвиток ШІ-рішень у відомстві [40; 70].

Разом з тим міжнародний досвід розроблення нормативних рамок використання ШІ в державному секторі, зокрема Акty ЄС (Artificial Intelligence

Act) [59] і Data Governance Act [58], має бути інтегрований у національне правове поле для забезпечення етичності, прозорості та підзвітності алгоритмічних систем. Це дозволить не лише адаптувати кращі практики ЄС, але й уникнути технологічного диктату приватних корпорацій та надмірної алгоритмічної дискримінації [57; 52].

Таким чином, сучасний стан застосування систем штучного інтелекту в публічному адмініструванні МВС України характеризується поетапним впровадженням цифрових інструментів, появою законодавчих ініціатив, спрямованих на створення єдиних систем відеонагляду та аналітики, а також формуванням стратегічних документів із розвитку цифрової держави. Проте темпи впровадження залишаються недостатніми для реалізації повноцінної цифрової трансформації, а рівень інтеграції ШІ у ключові функції МВС все ще фрагментарний. Для подолання цих викликів потребується комплексна модель розвитку – від нормативного забезпечення до створення інституційного середовища і формування професійних цифрових компетентностей у кадрів системи МВС.

1.2. Сучасні моделі, класифікації та функціональні можливості систем штучного інтелекту

Сучасні системи штучного інтелекту (ШІ) перестали бути виключно інструментами автоматизації рутинної діяльності. Сьогодні вони виступають повноцінною інтелектуальною інфраструктурою, здатною підтримувати складні управлінські процеси, прийняття рішень, моделювання ризиків та прогнозування розвитку суспільних процесів. Для органів публічного управління, зокрема МВС України, розуміння моделей ШІ, їх функцій та класифікацій є ключовим етапом у плануванні впровадження інтелектуальних систем.

Сучасне розуміння штучного інтелекту (ШІ) формується на перетині комп’ютерних наук, кібернетики, психології та управлінських дисциплін. У публічному секторі, зокрема у правоохоронній сфері, ШІ набуває особливої значущості як інструмент оптимізації інформаційно-аналітичної діяльності,

посилення реактивності системи безпеки та підвищення ефективності управлінських рішень у високостресових умовах, таких як воєнний стан або кризові ситуації [21, с.54].

Застосування ШІ в діяльності МВС України є складною багатовимірною системою, де зустрічаються технічні, правові, організаційні та етичні аспекти. Основним викликом є забезпечення відповідності технологій принципам верховенства права, прав людини та пропорційності втручань, встановленим як національним законодавством [3], так і європейськими нормами, зокрема Regulations (EU) 2024/1689 (AI Act) [59]. З іншого боку, технологічні бар'єри пов'язані з недосконалістю державної інформаційної інфраструктури, низьким рівнем сумісності між реєстрами та обмеженим доступом до інтелектуальних систем на рівні регіональних підрозділів.

Дослідники наголошують, що ШІ не можна розглядати лише як універсальне «рішення всіх проблем». Його впровадження потребує попереднього аналізу адміністративних процесів, стандартизації даних та інтеграції міжвідомчих платформ. У світовій практиці показовим є перехід від ізольованих рішень до комплексних платформ, орієнтованих на екосистемний підхід («smart government») [66].

У межах органів внутрішніх справ ШІ дозволяє переводити аналітичні завдання на рівень, недосяжний для традиційної ручної обробки даних. Наприклад, моделі машинного навчання здатні аналізувати тисячі записів про правопорушення, що дає змогу виявляти приховані кореляції, визначати циклічність кримінальної активності або прогнозувати зміни злочинності у регіонах на основі соціально-економічних показників [25, с.150]. Подібні системи вже використовуються в розвинених країнах, як-от PredPol у США [61], і демонструють здатність до скорочення рівня злочинності в окремих районах шляхом оптимізації розподілу поліцейських ресурсів.

В українських умовах першим практичним майданчиком для впровадження інтелектуальних моделей стала Єдина система відеомоніторингу стану публічної безпеки – мережа камер із модулем розпізнавання, яка інтегрується з базами

даних МВС [22]. За офіційними даними, станом на 2024 рік система включає близько 40 тисяч камер [45]. Однак відсутність єдиної моделі управління даними і стандартизованих алгоритмів обробки залишають питання щодо ефективності й узгодженості діяльності на національному рівні.

Також важливим напрямом є застосування генеративних моделей ШІ у внутрішньому документообігу, як-от автоматичне складання шаблонів протоколів, формування матеріалів для розслідувань, адаптація нормативних документів та підготовка довідок для керівництва. Моделі на кшталт GPT-4 і Gemini вже демонструють високу якість текстової генерації [65], проте існують обмеження щодо точності, юридичної відповідності та ризику помилкової інформації (hallucinations). Тому такі системи потребують контролю з боку експерта та перевірки відповідності чинному законодавству.

Зарубіжні дослідження також вказують на перспективу інтеграції мультимодальних моделей, які поєднують обробку тексту, зображень, звуку та відео. Потенційно ці системи можуть забезпечувати комплексний аналіз оперативної обстановки – від аналізу поліцейських зведень до розпізнавання підозрілої поведінки у натовпі [53]. Однак такі технології наразі залишаються дорогими і потребують інституційної реформи, в тому числі зміни підходів до обробки даних та підготовки кадрів.

Водночас у вітчизняних наукових та професійних публікаціях наголошується, що функціональні можливості ШІ мають бути прив'язані до стратегічних завдань, а не навпаки [40, с.55]. Іншими словами, технологія не повинна визначати завдання, але має слугувати інструментом для їх виконання. Це означає необхідність розробки чіткої політики розвитку ШІ у МВС, зі структурованою модельною базою застосувань, визначенням зоно відповідальності, підзвітності систем та контрольних механізмів.

Таким чином, системи штучного інтелекту в органах внутрішніх справ не просто автоматизують процеси – вони формують новий тип публічного управління, орієнтований на аналітичне мислення, превентивність, оперативність і прозорість. Наступним логічним кроком розвитку має стати

впровадження комплексних алгоритмічних платформ, орієнтованих не лише на аналіз, але й на моделювання сценаріїв, підтримку стратегічного планування і управління ризиками у сфері безпеки.

Сучасні моделі ШІ можна згрупувати за рівнем автономності, функціональності та спрямованості. Найбільш поширені моделі наведено у таблиці 2.1.

Таблиця 2.1.

Найбільш поширені моделі ШІ [66]

Тип моделі	Характеристика	Приклади застосувань у МВС
Експертні системи	Засновані на наборі правил, що моделюють логіку експерта.	Правові консультації у Київському сервісному центрі МВС, обробка запитів громадян.
Системи машинного навчання (ML)	Автоматично виявляють закономірності у даних; потребують навчання на прикладах.	Виявлення шахрайських схем, аналіз кримінальних тенденцій, прогнозна аналітика [21].
Нейронні мережі	Складні структури, здатні до розпізнавання зображень, мови, поведінки.	Розпізнавання облич у системі відеомоніторингу, аналітика поведінки натовпу [45].
Нейросимволічні системи (Neuro-Symbolic AI)	Поєднують логічні та статистичні моделі, здатні до пояснюваності рішень.	Інтерпретовані рішення у криміналістичних експертизах [4].
Агентні системи	Відокремлені AI-компоненти, що взаємодіють і приймають власні рішення.	Мультирівневий моніторинг патрульної мережі, автономні дрони для контролю ситуації.
Генеративні моделі (LLM/GenAI)	Створюють новий контент текст, код, зображення.	Автоматичне складання протоколів, аналіз відео- та фотодоказів, створення сценаріїв навчання.

Цілісна класифікація систем ШІ у публічному адмініструванні, зокрема у сфері внутрішніх справ, ґрунтується на їх функціональному призначенні та рівнях автономності. Користуючись напрацюваннями ЄС (Regulation (EU) 2024/1689, Artificial Intelligence Act) [59], системи можна класифікувати таким чином:

За рівнем автономності:

- Системи з підтримкою рішень – надають рекомендації, але рішення залишається за людиною.

- Напівавтономні системи – можуть діяти автоматично в межах визначених рамок (наприклад, попередження про порушення).

- Автономні системи – приймають рішення без людського втручання (наприклад, автономні дрони у тепловізійному моніторингу прикордонної зони).

За рівнем ризику:

- Прийнятний ризик – чат-боти та інформаційні системи.

- Високий ризик – системи, що впливають на права людини (розпізнавання облич, превентивна аналітика).

- Неприпустимий ризик – системи соціального скорингу або дискримінаційного профайлінгу (заборонені в ЄС).

У контексті МВС системи штучного інтелекту дозволяють автоматизувати та підсилити ключові функції:

1. Аналітична функція – обробка, аналіз і візуалізація масивів даних для виявлення тенденцій у кримінальності, часових і географічних патернів, злочинних груп [21; 25].

2. Прогнозування та превенція – розрахунок ймовірності злочинів на основі даних про соціальну динаміку, економіку, демографію та попередні інциденти [70].

3. Моніторинг та спостереження – інтелектуальні камери з функціями розпізнавання облич та номерних знаків, автоматичного виявлення підозрілої поведінки [45].

4. Експертно-дорадча функція – надання рекомендацій щодо організації патрулювання, розподілу ресурсів, оптимізації службового навантаження.

5. Роботизація адміністративних процесів – автоматизація формування документів, відповідей на звернення, обробка анкетних даних, що використовуються у сервісних центрах [35].

Приклади використання ШІ у зарубіжних системах внутрішніх справ наведено у таблиці 1.2.

Таблиця 1.2.

Використання ШІ у зарубіжних системах внутрішніх справ

Країна	Система	Опис та функції
США	PredPol	Система прогнозної поліцейської аналітики, надає рекомендації щодо патрулювання [61].
Великобританія	AWARE	Модуль розпізнавання облич та аналіз відео в реальному часі для поліції Лондона.
Нідерланди	CAS (Crime Anticipation System)	Виявляє патерни злочинної поведінки на основі історичних даних.
ОАЕ	Smart Police Station	Автоматизована поліцейська станція без участі людей, з дистанційними сервісами.

Такі кейси демонструють швидке зростання можливостей ШІ в правоохоронній сфері, проте водночас створюють виклики щодо прозорості алгоритмів, відповідальності та захисту персональних даних.

Сучасні моделі і класифікації систем штучного інтелекту дають підстави стверджувати, що функціональне впровадження цих технологій у структуру МВС України є закономірним і необхідним процесом у цифрову епоху. Моделі ШІ варіюються від простих систем автоматизованої аналітики до автономних агентних мереж і не лише забезпечують оперативне реагування, а й підтримують стратегічне планування та прогнозування.

Однак ефективність використання ШІ залежить від наявності належної правової бази, підготовки кадрів і захисту персональних даних, що вимагає комплексного підходу до планування цифрових реформ у МВС. Подальші підрозділи розглянуть практичні кейси впровадження систем ШІ, їх критичний аналіз та шляхи оптимізації інформаційно-аналітичної діяльності у структурі органів внутрішніх справ.

1.3. Міжнародний досвід застосування штучного інтелекту в діяльності правоохоронних органів

Застосування технологій штучного інтелекту у правоохоронній діяльності розвинених країн сформувалося внаслідок поєднання стратегічного бачення, чітких нормативно-правових рамок і багаторічного досвіду використання інтелектуальних систем для підтримки поліцейської та криміналістичної діяльності. У країнах Європейського Союзу (ЄС) і Сполучених Штатах Америки (США) підходи до інтеграції штучного інтелекту (ШІ) базуються на принципах безпеки, пропорційності, прозорості та захисту прав людини. Загалом політика у сфері використання ШІ в органах правопорядку залишається однією з найбільш регульованих і контрольованих через ризики для приватності, дискримінації та алгоритмічних помилок, які можуть мати серйозні наслідки для громадян.

Європейський Союз упродовж останніх років вибудовує комплексну систему регулювання штучного інтелекту, у якій особлива увага приділяється сферам високого ризику, до яких належать і правоохоронні органи. Ключовим документом у цьому контексті став Регламент (EU) 2024/1689, відомий як Artificial Intelligence Act, прийнятий 13 червня 2024 року [59]. Цей документ встановлює чіткі правила використання ШІ у сферах підвищеного суспільного ризику, включно з кримінальним судочинством, системами розпізнавання облич у режимі реального часу, аналізом поведінки громадян і прогнозними алгоритмами. Технології, які належать до категорії high-risk, підлягають обов’язковій оцінці відповідності, незалежному аудиту, прозорому звітуванню та забезпеченню механізмів «людського нагляду» (human oversight). Регламент також забороняє використання систем, що здійснюють соціальний скоринг або прогнозують «потенційно небезпечну» поведінку людей без чітких критеріїв та підстав.

У Сполучених Штатах Америки впровадження ШІ в діяльність поліції відбувається на основі ініціатив на федеральному та місцевому рівнях, без єдиного загальнонаціонального закону про штучний інтелект. Продовжує діяти модель експериментальних впроваджень і публічних дискусій, яка нерідко

супроводжується критикою з боку громадських організацій. Натомість досягнуто значних результатів у сфері керованої алгоритмічної аналітики (predictive policing), яка була вперше застосована у Лос-Анджелесі та Чикаго через систему PredPol. Її алгоритм ґрунтується на поєднанні статистичної обробки даних і машинного навчання для прогнозування місць і часу найбільш імовірного вчинення злочинів [61]. Після декількох років використання системи її результати стали предметом активних дискусій, згідно з дослідженнями, PredPol в окремих районах справді зменшила кількість злочинів, однак одночасно постала проблема автоматичного упередження проти соціально вразливих груп.

Подібні підходи також застосовуються у Великій Британії. У лондонській поліції використовується система AWARE, пов’язана з розпізнаванням облич у натовпі та аналізом відеопотоку з камер спостереження. Об’єднані алгоритмічні рішення дозволяють поліції в реальному часі виявляти людей, які знаходяться у розшуку, або осіб зі списків ризику. У публічному просторі ця технологія неодноразово стала об’єктом критики – організації з прав людини наполягають, що автоматичне відеоспостереження порушує право на приватність, створює ризик профайлінгу та може робити помилки у розпізнаванні осіб з темною шкірою або жінок [67].

Попри це Велика Британія встановила чіткі процедури аудиту алгоритмів, публічної звітності та створення механізмів для оскарження автоматизованих рішень. Основою таких підходів є модель “XAI” (Explainable Artificial Intelligence) – пояснюваного штучного інтелекту. Пояснюваність виступає ключовою характеристикою в поліцейських системах, що використовують ШІ, оскільки правоохоронні рішення повинні бути не лише обґрунтовані, але й доведені до громадського розуміння, з можливістю перевірки алгоритмічних висновків [52]. Це особливо важливо для судових процесів, де докази, отримані алгоритмічним шляхом, можуть бути враховані лише за умови розуміння принципів їх формування.

Загалом міжнародний досвід впровадження ШІ у сфері правопорядку демонструє кілька визначальних тенденцій. По-перше, в країнах ЄС і США

формується спільна правова рамка, яка визначає не лише процедури впровадження нових систем, але й вимоги до прозорості, контролю, відповідальності та недопущення дискримінації. По-друге, бачимо активне впровадження алгоритмічної аналітики у превентивній діяльності, що дозволяє ефективніше розподіляти ресурси, знижувати навантаження на персонал і підвищувати оперативність роботи. По-третє, існує чітке розуміння, що ШІ у сфері правопорядку не повинен замінювати людину, але може бути її інструментом – за умови дотримання принципів етичності, законності та демократичного контролю.

Упродовж останнього десятиліття країни ОЕСР активно впроваджують у діяльність своїх правоохоронних органів комплексні системи, що поєднують відеоаналітику, алгоритми розпізнавання образів, інтелектуальні центри управління подіями та інструменти прогнозної аналітики. Відбувається поступовий перехід від пасивного відеоспостереження до багаторівневих платформ real-time intelligence, які інтегрують масиви даних із камер, сенсорних мереж, мобільних пристроїв, дорожньої інфраструктури та відкритих джерел. Така трансформація відповідає глобальним трендам цифрової безпеки, описаним у дослідженнях Європолу [61] і ОЕСР [66], та ґрунтується на зростаючих вимогах до швидкості реагування, достовірності доказів і можливостей аналітичної обробки великих масивів інформації.

Одним із найпоширеніших напрямів упровадження ШІ є інтелектуальні системи відеонагляду, що автоматично аналізують поведінку людей, виявляють нетипові патерни, розпізнають транспортні засоби та фіксують порушення. У Канаді, Нідерландах та Австралії такі системи використовуються для розпізнавання ситуацій «раннього ризику» – залишені предмети у громадських місцях, різке збільшення скупчення людей, агресивні рухи, біг у зонах підвищеної безпеки. Алгоритми, описані у дослідженнях про AI у кримінальному праві [52], працюють за принципом порівняння поточної поведінки з історичними моделями та базами інцидентів. Це дозволяє скоротити кількість хибно позитивних спрацьовувань і підвищити точність класифікації.

Технології розпізнавання облич стали окремим аспектом використання ШІ. Франція, Бельгія, Німеччина та Естонія застосовують системи ретроспективного відеоаналізу, у яких розпізнавання облич працює лише на записаному матеріалі, без використання в реальному часі – відповідно до вимог пропорційності та недискримінації. Саме ця модель вважається найбільш прийнятною з погляду відповідності принципам ЄС, включно з положеннями Artificial Intelligence Act [59]. У більшості країн ЄС роботи таких систем жорстко контролюють спеціальні незалежні органи, а кожен випадок доступу до алгоритмічного пошуку потребує реєстрації та аудиту.

Інший напрямок – оперативно-аналітичні центри ситуаційної обізнаності (Real-Time Crime Centers). У США ці центри працюють у Нью-Йорку, Аталанті, Х'юстоні й десятках інших міст, об’єднуючи дані з камер, дорожніх систем, систем ідентифікації автомобільних номерів, а також аналітичні модулі прогнозування ризиків. У європейських країнах аналогічні центри створюють Німеччина, Данія, Чехія та Фінляндія, з акцентом на інтеграцію ШІ у процеси моделювання загроз, аналіз текстових повідомлень та оперативних даних. За результатами звітів Stanford HAI [71] та Europol [61], такі центри демонструють відчутне скорочення часу реагування та підвищення ефективності використання ресурсів.

У розвинених демократіях ШІ дедалі частіше застосовується для прогнозування кримінальних подій, але цей напрямок залишається найбільш суперечливим. Класичні моделі на кшталт PredPol поступово замінюються більш складними системами, що аналізують поведінкові патерни, мережеві структури кримінальної активності та аномалії у рухах транспортних засобів. Естонія, Фінляндія та Португалія експериментують з платформами, побудованими на моделі «embedded AI», де алгоритми працюють усередині інфраструктури відеоспостереження, мінімізуючи обробку персональних даних. Європейські регулятори вимагають, щоб усі такі системи відповідали принципам пояснюваності, прозорості та можливості повторної верифікації результатів [57].

Значний прогрес демонструють також системи алгоритмічної підтримки розслідувань, що аналізують великі обсяги документів, відеозаписів, фотографій, даних мережевого аналізу та показань свідків. У Німеччині та Швейцарії такі системи допомагають виявляти зв'язки між інцидентами, проводити аналіз соціальних мереж злочинців, формувати профілі ризику та будувати криміналістичні гіпотези. У США технології машинного навчання використовуються для автоматичного сортування доказів у складних справах, що скорочує навантаження на слідчих і зменшує ризики людських помилок.

Окремої уваги заслуговують комбіновані системи відеонагляду з тепловими камерами, радіолокаційними сенсорами та безпілотниками, які активно використовують у Франції, Канаді та США. Вони дозволяють відстежувати переміщення людей у складних умовах – уночі, під час масових заходів, у зонах надзвичайних ситуацій. Системи на основі багатоджерельного ШІ створюють тривимірні карти місцевості, формують прогнози ризиків і допомагають координації роботи служб швидкого реагування, що підтверджується матеріалами Digital Transformation and Public Services [56].

Поширення систем штучного інтелекту у діяльності правоохоронних органів упродовж останніх років супроводжується зростаючим інтересом до їхніх потенційних ризиків, можливих зловживань та загроз для демократичних інститутів. Країни ЄС, США, Канада, Японія та інші держави ОЕСР поступово виробляють підходи, що дозволяють інтегрувати ШІ у сферу безпеки, не порушуючи фундаментальних прав людини. Сучасна нормативна модель дедалі чіткіше відмежовує технологічні можливості систем від меж їх допустимого застосування, а питання прозорості й підзвітності стають обов'язковими складовими кожного проєкту впровадження алгоритмічних рішень.

Одним із найважливіших нормативних документів є Artificial Intelligence Act (2024), який вводить сувору класифікацію ризиків та окреслює межі правомірного застосування алгоритмів у поліції [59]. Системи реального розпізнавання облич у публічних місцях належать до категорії високого ризику, що передбачає обов'язкові вимоги до якості даних, аудит моделей, фіксацію

логів, мінімізацію помилок та механізми перегляду рішень людиною. У деяких випадках використання таких технологій вважається неприйнятним – насамперед там, де йдеться про масове стеження або неконтрольоване збирання біометричних даних. Саме тому у кількох країнах ЄС (Франція, Бельгія, Німеччина) заборонено використання систем автономного розпізнавання облич у режимі реального часу, а у Великій Британії та США такі рішення допускаються лише у межах вузько визначених оперативних задач.

Ключовою проблемою, яка активно обговорюється у наукових джерелах, є байас алгоритмів, тобто ризик систематичних помилок проти певних груп населення. Дослідження юридичної практики і впливу ШІ на правозастосування підкреслюють небезпеку використання неякісних або нерепрезентативних даних, що може призводити до дискримінаційних результатів [52]. Тому уряди розвинених країн запроваджують обов'язкові перевірки навчальних вибірок, зовнішні аудити алгоритмів і процедури оцінювання соціального впливу (AI Social Impact Assessment).

Ще один важливий аспект – небезпека надмірної автоматизації. Міжнародні організації підкреслюють, що використання ШІ у правоохоронній діяльності не повинно призводити до «автоматизованого правосуддя», де ключові рішення приймаються без участі людини. У рекомендаціях Європейської комісії щодо етичного застосування ШІ вказується, що будь-яке втручання в особисті права має передбачати можливість апеляції, перегляду та обґрунтування індивідуального рішення [57]. Принципи XAI (Explainable AI) стали обов'язковими у багатьох юрисдикціях, оскільки забезпечують можливість пояснення, чому система сформувала той чи інший висновок, на яких даних ґрунтувалася, які ваги мала модель та які фактори стали ключовими.

Країни ЄС і США також створюють механізми громадського контролю, що включають незалежні наглядові ради, публічні звіти, відкриті реєстри алгоритмів та регулярні аудити. Одним із найбільш ефективних інструментів стала вимога, згідно з якою кожен орган, що впроваджує високоризикову AI-систему, повинен публікувати опис алгоритму, мету використання, обмеження, статистику

помилок та інформацію про навчальні набори даних. Це дозволяє громадянському суспільству і профільним експертам здійснювати моніторинг потенційних зловживань.

Особливу увагу міжнародні експерти приділяють ризикам, пов’язаним із відеомоніторингом масових подій. Аналітики Інституту масової інформації та інших правозахисних організацій застерігають, що інтенсивний розвиток таких систем може створювати умови для прихованого спостереження за політично активними громадянами, журналістами та правозахисниками [26]. Подібні побоювання висловлюють також дослідники цифрових прав, які наголошують на необхідності балансування інтересів безпеки та приватності, особливо у світлі нових практик автоматичного аналізу поведінкових патернів у публічних місцях [42].

Не менш важливою проблемою є захист інфраструктури AI-систем від кіберзагроз. За даними ООН та Європолу, будь-які централізовані інтелектуальні системи можуть стати мішенню для кібератак, які здатні вплинути на алгоритмічні моделі, підмінити дані, створити хибні сигнали або навіть вивести з ладу критичні компоненти системи. Тому провідні демократії впроваджують окремі протоколи кіберзахисту, включно з ізоляцією серверної інфраструктури, багатофакторною автентифікацією, системами моніторингу аномалій та регулярним тестуванням на проникнення.

У низці держав також діють обмеження на використання автономних систем у прийнятті рішень, що впливають на права людини. Зокрема, у Канаді та Нідерландах заборонені будь-які моделі, які автоматично присвоюють «рівень ризику» громадянам у сфері соціального захисту чи міграції – після низки резонансних справ, де алгоритми спричинили масові помилки та несправедливі переслідування окремих груп населення.

Отже, міжнародний досвід показує що упровадження ШІ в діяльність правоохоронних органів можливе лише за умови забезпечення належних гарантій прозорості, контролю та пропорційності. Найефективніші практики ґрунтуються на поєднанні високотехнологічних рішень із чіткими етичними

стандартами, інституційними механізмами нагляду та правовими інструментами захисту громадян від можливих зловживань. Така модель дозволяє забезпечити баланс між потребами безпеки, ефективністю алгоритмів та верховенством права у демократичних суспільствах.

Висновки до розділу 1

Результати проведеного дослідження дали змогу окреслити ключові теоретичні, концептуальні та практичні засади застосування систем штучного інтелекту у сфері публічного управління та правоохоронної діяльності. Штучний інтелект перетворився на критично важливий інструмент модернізації інституцій державного сектору, формуючи нову архітектуру управлінських процесів, де автоматизовані рішення доповнюють традиційні механізми прийняття управлінських рішень. З'ясовано, що сучасні моделі та класифікації AI включають широкий спектр технологій – від систем обробки природної мови та машинного навчання до предиктивної аналітики, комп'ютерного зору та роботизованих платформ, кожна з яких має власне функціональне призначення та рівень ризику.

Важливим є те, що світові підходи до впровадження AI у діяльність органів влади спираються на принципи прозорості, підзвітності та пропорційності. У сфері правопорядку пріоритетним є обмеження автоматизованого втручання у права людини, тому міжнародна практика демонструє домінування керованих і контрольованих моделей використання, у яких ключова роль залишається за людиною, а системи штучного інтелекту виконують функції підтримки, аналізу, прогнозування та оптимізації процесів.

Узагальнення міжнародного досвіду показує, що найбільш технологічно прогресивні країни стримано підходять до впровадження алгоритмічних рішень, надаючи перевагу етичним обмеженням, зовнішньому аудиту та громадському нагляду. Такий підхід визнано найбезпечнішим для правоохоронної сфери, де надмірна автоматизація може створювати ризики упередженості, помилкових рішень, непропорційного стеження чи втручання у приватність.

РОЗДІЛ 2. СТАН, ПРОБЛЕМИ ТА ПРАКТИКА ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ АДМІНІСТРУВАННІ МВС УКРАЇНИ

2.1. Нормативно-правове забезпечення цифрової трансформації та використання систем штучного інтелекту в МВС України

Цифрова трансформація сфери публічного управління, включно з діяльністю Міністерства внутрішніх справ України, формується на основі загальнодержавних нормативних актів, що визначають правила обробки інформації, порядок доступу до даних, вимоги до безпеки та правові межі застосування нових технологій. Будь-які системи штучного інтелекту у відомчій діяльності розвиваються лише в межах уже сформованого правового поля, що задає базові стандарти роботи з інформаційними ресурсами та встановлює гарантії захисту прав людини у процесах автоматизації та цифровізації. Центральне місце займають законодавчі засади, які визначають інформаційний режим у державному секторі та вимоги до безпечної обробки персональних даних, адже саме ці норми накладають на державні органи обов’язок забезпечувати законність збору й використання інформації, незалежно від того, застосовуються традиційні технології чи алгоритмічні інструменти [2; 3].

Закон України «Про інформацію» встановлює фундаментальні принципи доступності, відкритості та захищеності інформаційних ресурсів держави, підкреслюючи, що обробка інформації має здійснюватися з дотриманням прав громадян та вимог до її достовірності, цілісності та законності [2]. Для МВС цей закон формує рамку, у межах якої здійснюється створення та використання інформаційних систем, включаючи відеоспостереження, реєстри, цифрові бази даних та інші електронні ресурси, на яких можуть ґрунтуватися алгоритмічні рішення. Одночасно Закон України «Про захист персональних даних» визначає обмеження, що регулюють збір, зберігання та обробку персональної інформації, передбачаючи принципи мінімізації даних, цільового призначення та пропорційності їх використання [3]. Ці вимоги безпосередньо впливають на

можливість застосування ШІ, оскільки будь-яка система автоматичного розпізнавання обличчя, поведінки або обробки масивів відеоданих має функціонувати в режимі суворої правової відповідності й забезпечувати належний рівень захисту приватності.

Законодавчі обмеження формують не лише технічні, але й організаційні умови для розбудови інтелектуальних систем. Усі цифрові рішення МВС повинні функціонувати в межах правової моделі, де держава виступає одночасно володільцем та розпорядником інформаційних ресурсів, а також гарантом їх безпечного використання. Це означає, що інституційна архітектура, яка визначає права й обов'язки підрозділів МВС у сфері роботи з даними, повинна бути узгоджена з чинним інформаційним законодавством. У цьому контексті важливим є Закон «Про національну безпеку України», який визначає інформаційну та кібернетичну безпеку складовими національної безпеки та покладає на державні органи обов'язок створювати умови для стійкості інформаційних систем до зовнішніх і внутрішніх загроз [4]. Оскільки сучасні інтелектуальні технології можуть використовуватися як для підвищення ефективності правоохоронної діяльності, так і становити потенційні вектори атак або помилок, правові вимоги щодо кіберзахисту стають невід'ємною частиною нормативної моделі впровадження ШІ у сфері внутрішніх справ.

Формування цифрового середовища в державному секторі неможливе без чітко визначених стандартів управління даними. Нормативна база накладає на державні органи вимогу забезпечувати структурованість, сумісність та захищеність інформаційних ресурсів, що для МВС означає необхідність створення інтегрованої цифрової системи, здатної підтримувати функціонування алгоритмічних інструментів у масштабах усієї відомчої інфраструктури. Особливо важливим є положення про необхідність упорядкування масивів даних, їх актуальність і контроль доступу, оскільки системи ШІ критично залежать від якості та повноти вхідної інформації. Це накладає додаткові вимоги щодо регламентації внутрішніх процедур роботи з даними та технічної модернізації

інфраструктури МВС, що узгоджується з загальнодержавними нормативами цифрової трансформації [8].

Правове поле також встановлює обмеження щодо допустимих форм автоматизації оперативно-службової діяльності. Застосування інтелектуальних систем у правоохоронній практиці вимагає врахування не лише інформаційного та кібернетичного законодавства, але й галузевих норм, що регулюють функціонування поліції та інших органів системи МВС. Закон «Про Національну поліцію» визначає порядок використання технічних засобів, зокрема відеоспостереження, та встановлює, що будь-які технології повинні застосовуватися з дотриманням принципів законності, необхідності та пропорційності [1]. Це створює юридичний контекст, який дозволяє впроваджувати цифрові інструменти, але одночасно обмежує потенційні ризики надмірного втручання в приватне життя або необґрунтованої автоматизації рішень, що мають значення для прав людини.

Таким чином, базові нормативні акти задають загальний каркас, у межах якого МВС може здійснювати цифрову трансформацію та розгортати системи, що передбачають застосування алгоритмічних технологій. Вони визначають правові стандарти, яких необхідно дотримуватися при розробці, впровадженні та експлуатації інтелектуальних рішень, що охоплюють інформаційну безпеку, захист персональних даних, обмеження щодо технологічних інструментів та відповідальність державних органів за належну організацію інформаційної діяльності. Без дотримання цих засад будь-яке масштабне впровадження систем штучного інтелекту у сфері внутрішніх справ стає юридично неможливим, а інституційна спроможність до їх використання – суттєво обмеженою. Стратегічні державні документи формують довгострокову рамку, у межах якої відбувається цифрова трансформація та впровадження інтелектуальних технологій у сферу внутрішніх справ. Для МВС вони визначають не лише загальні напрями розвитку цифрової держави, але й конкретні вимоги до модернізації відомчої інфраструктури, інтеграції інформаційних платформ, використання алгоритмічної аналітики у правоохоронній діяльності та підвищення рівня

захищеності цифрових систем. Кожен стратегічний документ задає окремий вимір розвитку, однак у сукупності вони формують цілісну модель, що готує МВС до системного впровадження технологій штучного інтелекту.

Однією з ключових засад є Концепція розвитку штучного інтелекту в Україні, схвалена Кабінетом Міністрів у 2020 році. Документ визначає державну політику щодо дослідження, впровадження та етичного використання технологій ШІ, уключаючи вимоги до правового регулювання, стандартизації, формування наукового потенціалу та створення умов для інтеграції інтелектуальних систем у державний сектор [6]. Для МВС особливо важливими є норми щодо застосування ШІ у сфері безпеки, оскільки вони акцентують увагу на потребі забезпечення людського контролю, недопущення дискримінаційних моделей та впровадження механізмів оцінювання ризиків у системах автоматизованої аналітики. У документі прямо зазначено, що держава має стимулювати використання алгоритмічних технологій для підвищення ефективності публічного управління, але лише в межах, які гарантують дотримання прав людини та верховенства права. Це створює концептуальну основу для майбутніх реформ у системі МВС.

На основі концепції уряд затвердив План заходів з реалізації Концепції на 2025–2026 роки, який деталізує конкретні кроки з розвитку національної інфраструктури ШІ, створення дата-платформ, підготовки кадрів та впровадження інтелектуальних систем у державне управління [7]. Для МВС документ визначає необхідність модернізації відомчих інформаційних ресурсів, розвитку міжвідомчої інтеграції даних, підвищення рівня кіберзахисту та впровадження алгоритмічних рішень для оптимізації оперативних і адміністративних процесів. План заходів робить акцент на створенні умов для впровадження систем прогнозної аналітики, інтелектуальної обробки відеоданих та автоматизації управлінських процедур. Тому цей документ має безпосереднє значення для майбутнього розвитку аналітичних платформ МВС.

Суттєве місце у формуванні нормативної рамки посідає Стратегія розвитку цифрової держави до 2030 року, яка визначає цифровізацію сектору безпеки одним із ключових пріоритетів державної політики [8]. Стратегія встановлює

вимоги до сумісності державних реєстрів, розвитку державних дата-центрів, впровадження автоматизованих систем моніторингу, аналітики та управління ризиками. Для МВС це означає необхідність переходу від розрізнених відомчих баз до інтегрованого середовища, здатного підтримувати роботу інтелектуальних технологій у режимі реального часу. Документ також визначає вимоги до кіберзахисту критичної інфраструктури та протидії кібератакам, що є важливою умовою використання алгоритмічних систем в оперативній діяльності. У стратегічному вимірі це формує вектор на створення цифрової екосистеми, у якій ШІ відіграє не допоміжну, а структурну роль.

Іншим важливим документом є Стратегія розвитку органів системи МВС до 2030 року, що фіксує пріоритет цифрової трансформації як ключовий елемент модернізації відомства [12]. У документі підкреслюється необхідність розбудови єдиної інформаційної інфраструктури МВС, оптимізації документообігу, модернізації криміналістичних лабораторій, розширення можливостей систем відеоспостереження, а також впровадження автоматизованих аналітичних моделей для ухвалення управлінських рішень. Стратегія визначає орієнтири щодо створення умов для використання штучного інтелекту у сферах кримінального аналізу, інформаційно-пошукових систем, моніторингу публічної безпеки та роботи сервісних підрозділів. З огляду на це документ створює інституційний каркас, який орієнтує МВС на впровадження інтелектуальних технологій у стратегічній перспективі.

Важливою складовою нормативної рамки є також державні документи, спрямовані на вдосконалення цифрових процесів у публічній адміністрації. Зокрема, розпорядження Кабінету Міністрів «Деякі питання цифрової трансформації» від 2024 року визначає вимоги до модернізації національної цифрової інфраструктури, створення екосистеми електронних послуг, розвитку державних платформ автентифікації та електронної ідентифікації [10]. Для МВС цей документ важливий з огляду на вимогу інтегрувати відомчі цифрові рішення з національними платформами, підвищувати рівень захищеності цифрових сервісів та розвивати інструменти електронної взаємодії з громадянами.

У сукупності ці документи формують чітку нормативну траєкторію, що орієнтує МВС на глибоку цифрову модернізацію та створює умови для масштабного застосування технологій штучного інтелекту. Вони визначають роль держави як координатора, регулятора й гаранта безпеки, а також закладають інституційні засади для переходу від традиційної моделі управління до системи, у якій інтелектуальні технології стають структурним елементом оперативної та аналітичної діяльності.

Розвиток інтелектуальних технологій у системі МВС залежить від наявності внутрішніх нормативних актів, що визначають правила функціонування інформаційних систем, порядок роботи з даними, вимоги до цифрової інфраструктури та напрямки модернізації відомчих платформ. Саме ці документи формують підґрунтя, на якому може розгортатися впровадження алгоритмічних рішень, адже будь-яка система штучного інтелекту потребує чітко регламентованих процедур доступу до даних, інтеграції інформаційних ресурсів, забезпечення кіберзахисту та інституційної відповідальності. Нормативна база МВС є багаторівневою та охоплює стратегічні документи, відомчі накази, програмні концепції та регламенти функціонування інформаційних мереж.

Одним із ключових нормативів, що регулюють цифрову архітектуру відомства, є Положення про єдину цифрову відомчу телекомунікаційну мережу МВС України, затверджене наказом № 596 від 04.07.2016 року [11]. Документ визначає структуру, функції та правила експлуатації телекомунікаційної мережі, яка є фундаментом для роботи всіх інформаційних систем міністерства. У положенні встановлено вимоги до побудови захищених каналів зв’язку, організації відомчих дата-центрів, забезпечення безперебійного функціонування інформаційних сервісів та їх захисту від несанкціонованого доступу. Така інфраструктура є критично важливою для майбутніх систем штучного інтелекту, оскільки будь-які алгоритмічні моделі потребують високої пропускної здатності, швидкого доступу до інтегрованих баз даних та захищених каналів передавання інформації. Саме ця телекомунікаційна основа визначає технічну спроможність

МВС до масштабного впровадження аналітичних платформ та інтелектуальних модулів.

Важливу роль у формуванні цифрового середовища МВС відіграє Концепція програми інформатизації системи МВС України на 2021–2023 роки, затверджена наказом МВС № 301 від 22.04.2021 року [9]. Документ окреслює пріоритети інформатизації, зокрема модернізацію інформаційних систем, цифровізацію сервісів, підвищення сумісності реєстрів та розвиток електронних послуг. Концепція спрямована на перехід від фрагментованих відомчих рішень до інтегрованої цифрової екосистеми, здатної підтримувати уніфіковані процеси обробки інформації. Для впровадження ШІ цей документ є ключовим, оскільки передбачає створення структурованих баз даних, розвиток аналітичних систем, модернізацію криміналістичних лабораторій та розширення можливостей відомчих сервісних центрів. Технології штучного інтелекту можуть бути інтегровані лише на основі таких упорядкованих інформаційних ресурсів, що відповідають вимогам стандартизації та інформаційної безпеки.

Окреме значення має Стратегія розвитку органів системи МВС до 2030 року, яка визначає цифрову трансформацію одним із ключових векторів діяльності Міністерства внутрішніх справ у довгостроковій перспективі [12]. У документі підкреслено важливість створення сучасної інформаційно-аналітичної інфраструктури, здатної забезпечувати підтримку оперативно-службових рішень через використання інтелектуальних технологій. Стратегія передбачає розбудову систем кримінального аналізу, автоматизацію пошукових механізмів, підвищення якості відомчих реєстрів, розвиток платформ відеоспостереження та формування інтегрованого середовища обміну даними між підрозділами МВС. Вона також акцентує на необхідності запровадження інструментів прогнозної аналітики, автоматизації процесів моніторингу ризиків та створення умов для появи алгоритмічних систем підтримки ухвалення рішень. У цьому аспекті стратегія напряму пов’язана з упровадженням штучного інтелекту, оскільки визначає інституційний і технічний каркас, у межах якого можуть формуватися інтелектуальні сервіси.

Важливим елементом нормативної моделі МВС є також документи, спрямовані на цифровізацію сервісних функцій. Зокрема, державні пріоритети розвитку сервісних центрів МВС, модернізація процедур надання послуг, створення можливостей електронної ідентифікації та автоматизації процесів взаємодії з громадянами визначені в урядових рішеннях і повідомленнях офіційних джерел [35]. Ці процеси створюють потребу у впровадженні технологій, що дозволяють оптимізувати обсяги звернень, автоматизувати типові операції та використовувати інтелектуальні моделі для аналізу звернень, виявлення аномалій або прогнозування навантаження. Таким чином, цифровізація сервісної діяльності формує відповідне середовище для появи інструментів ШІ в адмінпроцесах МВС.

Особливу увагу МВС приділяє розвитку систем відеоспостереження, які останніми роками розширюють масштаби застосування та значно ускладнюють архітектуру відомчих інформаційних систем. Правові засади для формування таких рішень визначені не лише у законодавстві, але й у відомчих документах, повідомленнях та технічних регламентах, що регулюють порядок використання даних відеоспостереження, їх захист та інтеграцію у єдині бази [22]. Оскільки сучасні системи відеоаналітики використовують механізми комп’ютерного зору, фрейм-аналіз та інші алгоритми, нормативні документи МВС фактично створюють фундамент для подальшої інтеграції модулів штучного інтелекту у такі платформи. Це стосується автоматичної ідентифікації подій, аналізу поведінкових патернів та підтримки оперативного реагування на основі алгоритмічних висновків.

Крім того, нормативне підґрунтя МВС містить низку вимог щодо кіберзахисту та управління доступом до інформаційних систем. Хоча відповідні положення містяться у загальнодержавних актах, саме відомчі документи регламентують конкретні процедури, що визначають порядок доступу співробітників до інформаційних систем, їх повноваження, структуру внутрішньої ієрархії доступу та вимоги до технічних інструментів контролю. Без такої регламентації використання інтелектуальних систем було б неможливим,

оскільки штучний інтелект працює з концентрованими масивами інформації, що потребують високого рівня захисту.

У результаті ця група відомчих нормативів визначає конкретні технічні, організаційні та процедурні умови, у межах яких МВС може впроваджувати інтелектуальні технології. Саме вони формують реальну інституційну спроможність Міністерства внутрішніх справ переходити до використання ШІ у практичних аспектах оперативної діяльності, адміністративних процесах та сервісних функціях.

2.2. Аналіз існуючих цифрових інструментів та інформаційних систем МВС, що передбачають або можуть включати елементи штучного інтелекту

Функціонування цифрових інструментів МВС ґрунтується на розгалуженій мережі інформаційних систем, відомчих реєстрів та інтегрованих платформ, які забезпечують накопичення, обробку і передачу великих масивів даних. Саме ці масиви формують базу, на основі якої може працювати штучний інтелект, оскільки алгоритмічні моделі потребують структурованих, повних і якісних джерел інформації. Чинна архітектура інформаційних ресурсів МВС відрізняється високим рівнем фрагментації, оскільки включає окремі системи кримінальної аналітики, облікові реєстри, бази даних сервісних центрів, інформаційні платформи Національної поліції та відомчі телекомунікаційні мережі. Проте саме ця архітектура визначає потенціал для впровадження інтелектуальних технологій, адже забезпечує технічну можливість інтеграції даних, які можуть використовуватись у предиктивній аналітиці, автоматичному розпізнаванні та інших сферах застосування ШІ.

Фундаментом цифрової інфраструктури МВС виступає єдина відомча телекомунікаційна мережа, створена для забезпечення захищеного обміну інформацією між підрозділами та функціонування ключових реєстрів і сервісів [11]. Завдяки такій мережі МВС має технічну можливість підтримувати централізоване зберігання даних, інтегрувати відомчі інформаційні системи та

забезпечувати роботу уніфікованих сервісів у режимі реального часу. Для штучного інтелекту це критично важливо, оскільки будь-які алгоритмічні системи – моделі розпізнавання обличчя, класифікатори ризиків, модулі аналізу поведінки – залежать від постійного доступу до великих структурованих масивів інформації. Тому саме телекомунікаційна мережа визначає технічну базу для можливого впровадження інтелектуальних технологій у діяльність МВС.

Окрему групу цифрових ресурсів становлять інформаційні системи Національної поліції, які накопичують дані про кримінальні правопорушення, оперативно-розшукову діяльність, адміністративні правопорушення, розшук осіб та викраденого майна. Інтегровані обліки дозволяють здійснювати аналіз кримінальної ситуації, відстежувати динаміку злочинності та формувати аналітичні звіти. Для майбутніх систем штучного інтелекту ці ресурси важливі тим, що містять багатовимірні дані – часові ряди, геолокацію, параметри подій, характеристики правопорушників. Така структура даних є придатною для побудови предиктивних моделей, аналізу патернів злочинності та алгоритмізації частини аналітичних задач. Правові засади обробки цих даних визначаються законами «Про Національну поліцію» та «Про інформацію», які регламентують порядок збору, використання та зберігання інформації у відповідних системах [1; 2].

Значним сегментом цифрової інфраструктури МВС є системи сервісних центрів, що забезпечують діяльність у сфері реєстрації транспортних засобів, видачі посвідчень водія, оформлення адміністративних послуг, надання інформаційних довідок тощо. У цих системах зосереджена велика кількість персональних даних, що підлягають аналізу та перехресній перевірці, зокрема у випадках шахрайства або підробки документів. Урядова політика цифровізації сервісів МВС передбачає поступову автоматизацію процесів, що створює перспективні можливості для застосування ШІ у вигляді автоматичної перевірки документів, виявлення аномалій у запитах, класифікації звернень та оптимізації навантаження на фронт-офіси [35]. У цьому сенсі сервісні центри вже сьогодні накопичують дані, релевантні для алгоритмічного аналізу.

Суттєву роль у цифровій діяльності МВС відіграють інформаційно-пошукові та криміналістичні системи, які включають бази даних слідів, біометрії, експертних досліджень та криміналістичних картотек. Такі системи вже містять потенціал для впровадження алгоритмів комп'ютерного зору та автоматизованої ідентифікації, оскільки вміщують значні масиви фото- та відеоматеріалів, відбитків, фрагментів знарядь злочину та інших об'єктів експертного аналізу. Стратегічні документи МВС визначають модернізацію криміналістичних лабораторій як один із пріоритетів розвитку до 2030 року, що вказує на перспективу застосування інтелектуальних алгоритмів у сфері експертно-криміналістичної діяльності [12].

Зростає значення і платформ моніторингу публічної безпеки, зокрема систем відеоспостереження, які інтегруються у відомчі мережі та містять значний обсяг відеоданих. Ці системи не лише фіксують події, але й стають основою для застосування відеоаналітики, яка у перспективі може включати алгоритми виявлення нестандартної поведінки, розпізнавання обличчя, аналізу трафіку та автоматизації реагування. Правові аспекти функціонування таких платформ визначаються відомчими актами та урядовими рішеннями, що встановлюють вимоги до захисту відеоданих, збереження записів та допустимих меж використання технологій спостереження [22].

Усі перелічені цифрові системи МВС формують структуроване інформаційне середовище, яке вже сьогодні може бути інтегроване з алгоритмічними системами. Їхня архітектура дозволяє впроваджувати модулі ШІ, за умови достатньої модернізації інфраструктури, стандартизації даних та забезпечення належного рівня кіберзахисту. Таким чином, наявні інформаційні ресурси є не лише інструментами поточної діяльності МВС, але й фундаментом для трансформації відомства у напрямку інтелектуалізації процесів управління, аналізу та реагування.

Цифрова екосистема МВС містить низку сервісів, які створюють практичний фундамент для впровадження алгоритмічних рішень. На відміну від базових реєстрів, ці системи вже працюють у форматі активної взаємодії з

громадянами, а їхня логіка передбачає часткову автоматизацію рутинних операцій, що робить їх технічно придатними для інтеграції ШІ-модулів. Ці сервіси формують «точки входу» для демонстраційних проєктів штучного інтелекту в МВС, оскільки зосереджують структуровані дані, обліки звернень, документи та операційні процеси.

1) «Єдине вікно» сервісних центрів МВС та е-послуги в «Дії»

Сервісні центри МВС працюють через багатокомпонентну платформу, до якої входять модулі перевірки документів, електронні картки транспортних засобів, система черг та цифрові кабінети громадян. Із 2022 року частина послуг переведена в «Дію», зокрема:

- електронні водійські посвідчення,
- електронна технічна реєстрація авто,
- заміна посвідчення водія онлайн,
- перевірка авто за VIN у державних реєстрах,
- витяг з Єдиного державного реєстру транспортних засобів.

Ці сервіси вже містять технічні модулі автоматичної перевірки даних у реєстрах. Подальша інтеграція ШІ може включати:

- автоматичну детекцію підроблених документів за ознаками аномалій;
- попередню класифікацію типових звернень;
- прогнозування пікових навантажень на центри обслуговування для оптимізації роботи персоналу.

Технічну основу цієї інтеграції становлять системи СЦ МВС, що працюють через захищену мережу та синхронізуються з реєстрами МВС і Мінцифри [11].

2) Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України»

Це одна з ключових платформ НПУ, яка містить інтегровані модулі:

- облік кримінальних правопорушень;
- аналіз оперативної інформації;
- пошукові картотеки (зниклі особи, розшукувані, безвісні зникнення);
- геоаналітика злочинності на основі координат подій.

На основі цих даних можливе впровадження таких рішень ШІ:

- побудова heat maps злочинності з прогнозуванням ризикових зон;
- автоматичне виявлення аномальних подій у патрульних звітах;
- аналіз текстів заяв та протоколів для виявлення патернів;
- алгоритмічні моделі пріоритезації викликів «102» за рівнем небезпеки.

Архітектура порталу вже включає API-вузли для взаємодії з відомчими системами, що робить його готовим до експериментального впровадження модулів машинного навчання [12].

3) Система відеоспостереження «Безпечне місто» (МВС + місцеве самоврядування)

«Безпечне місто» – це децентралізована платформа, інтегрована з Національною поліцією. На сьогодні її елементи працюють у:

- Києві,
- Дніпрі,
- Львові,
- Харкові,
- Одесі,
- Івано-Франківську,
- низці ОТГ.

Платформа включає:

- міські сервери зберігання відео;
- центри аналітики поліції;
- камери спостереження (частина – з ANPR для розпізнавання номерів).

Фактично МВС уже має робочі модулі:

- розпізнавання номерних знаків (аналог ANPR);
- детекція автомобілів, що перебувають у розшуку;
- система проїзду по «хвосту» за підозрюваним автомобілем.

Штучний інтелект може розширити функціональність до:

- розпізнавання осіб (в рамках законодавчих обмежень);
- виявлення нестандартної поведінки у натовпі;

- автоматичного фіксування підозрілих маршрутів;
- класифікації ситуацій (бійка, переслідування, різкі рухи).

У 2024 році розроблявся законопроєкт №11031 щодо створення єдиної системи відеомоніторингу публічної безпеки, що фактично відкриває можливість централізації відеоаналітики МВС на державному рівні [23].

4) «Армор» (ARMOR) – система аналітики для патрульної поліції

ARMOR використовується для:

- фіксації даних патрульних екіпажів,
- створення електронних рапортів,
- ведення статистики викликів,
- оцінювання часу прибуття.

У перспективі ARMOR може отримати AI-модулі:

- рекомендації щодо маршруту патрулювання;
- пріоритезація викликів за ступенем ризику;
- аналіз повторюваності інцидентів;
- автоматичне формування частини рапорту.

Ця система вже структурована як аналітична платформа, тому інтеграція машинного навчання є технічно реалістичною [35].

5) Автоматизована система фіксації порушень ПДР (КАСКО-ПДР)

Система працює з:

- камерами автоматичної фіксації;
- алгоритмами розпізнавання номерів;
- автоматичною генерацією постанов.

Уже сьогодні ця платформа використовує базові алгоритми комп’ютерного зору. Потенціал ШІ:

- виявлення небезпечної манери водіння;
- аналіз патернів ДТП;
- визначення аномальних траєкторій руху;
- автоматичне формування ризикових профілів.

Дані системи інтегруються з реєстрами транспортних засобів та дозволяють створити єдиний аналітичний контур.

6) Єдиний державний реєстр зброї (ЄДРЗ), запущений у 2023 році

Містить:

- дані про цивільну зброю;
- історію видачі дозволів;
- результати перевірок;
- медичні довідки та довідки про несудимість у рамках процедури.

Для ШІ можливі напрямки:

- автоматичне виявлення ризикових профілів при подачі заяви;
- детекція пов’язаних осіб або підозрілих транзакцій із зброєю;
- аналіз історії інцидентів.

Реєстр має сучасну цифрову структуру й повністю інтегрований у платформу МВС через API Мінцифри.

7) Інформаційна система «Облік безвісти зниклих»

Система містить:

- фото;
- біометрію;
- текстові описи;
- додаткові матеріали.

На практиці можливі модулі ШІ:

- автоматичне «зіставлення» фото очевидців із базовим зображенням;
- відновлення вікового вигляду (age-progression AI);
- фільтрація тисяч рапортів про знахідки з високою точністю.

Це один з найбільш перспективних напрямів використання комп’ютерного зору в МВС [61].

Поточний рівень цифровізації МВС демонструє істотний прогрес у напрямі інтеграції інформаційних систем, однак готовність до широкомасштабного застосування штучного інтелекту залишається нерівномірною. Ефективність наявних цифрових інструментів можна оцінити через три ключові параметри:

якість даних, технологічну архітектуру, операційну сумісність між платформами відомства та зовнішніми державними системами. У межах цих параметрів простежується суттєва різниця між сервісно-адміністративними інструментами (які демонструють високий рівень технологічної готовності) та оперативно-аналітичними системами (де зберігається фрагментація та нерівномірність цифрових процесів).

Ефективність роботи електронних сервісів МВС оцінюється переважно позитивно: вони забезпечують стабільний доступ користувачів, автоматичну перевірку даних у реєстрах та синхронізацію з платформами Мінцифри. Одним із показників готовності до впровадження ШІ є те, що зазначені сервіси вже працюють у форматі повністю цифрового циклу – від подання заяви до автоматичної перевірки документів, що відповідає базовим вимогам до алгоритмічного моделювання, визначеним у міжнародних підходах до оцінки цифрової зрілості [8; 35]. У процесах, де дані одразу фіксуються в структурованій формі, подальше застосування алгоритмів машинного навчання може бути реалізоване з мінімальними трансформаціями.

Проблема нерівної структурованості даних є центральним бар'єром для впровадження інтелектуальних систем у діяльність МВС. Реєстри транспортних засобів, зброї й адміністративних послуг демонструють високий рівень структурованості, що робить їх придатними для алгоритмічного аналізу. Натомість оперативно-розшукові картотеки містять значні масиви неструктурованої інформації, включаючи текстові описи, ручні записи, фотоматеріали та окремі файли без метаданих. Ці особливості обмежують можливість прямого застосування ШІ та потребують попереднього етапу уніфікації даних, що підтверджується й у міжнародних рекомендаціях щодо алгоритмічної інфраструктури органів публічної влади [57, с.41].

Відеоаналітика також залишається неоднорідною: камери різних міст України використовують різні технічні стандарти, мають відмінну якість зображення та різні протоколи передачі потоків. Частина камер працює у форматі низької роздільності, що ускладнює подальшу обробку комп'ютерним зором. Для

системи, яка має постачати навчальні дані для ШІ-моделей, така різнорідність формує суттєвий ризик появи хибних спрацьовувань і зниження точності алгоритмів [61].

Цифрові інструменти МВС мають обмежену внутрішню інтеграцію. Навіть ті платформи, які ефективно працюють у власних сегментах (наприклад, автофіксація порушень або Єдиний реєстр зброї), не завжди мають прямий канал обміну даними з оперативно-аналітичними системами поліції. Це знижує загальну ефективність відомства та унеможливлює створення єдиного алгоритмічного контуру, здатного підтримувати роботу інтелектуальних систем у реальному часі. Подібні проблеми відзначаються й у дослідженнях цифрової еволюції правоохоронних структур інших держав, де підкреслюється необхідність спільної бази даних та уніфікованих метаданих для успішної інтеграції ШІ-модулів [52].

У сервісних платформах інтегрованість є значно кращою: вони синхронізуються з «Дією», демографічним реєстром, реєстром транспортних засобів та медичними реєстрами, що створює передумови для подальших алгоритмічних рішень. Однак в аналітичних підсистемах НПУ інтеграційні механізми залишаються фрагментарними, що не дозволяє створити хмарну аналітичну платформу типу EUROPOL Innovation Lab або AWARE (Велика Британія) [61].

Аналіз показує, що у більшості цифрових інструментів МВС рівень автоматизації обмежується базовими функціями – перевіркою документів, формуванням записів у реєстрах, стандартною валідацією даних та порівнянням інформації із нормативними вимогами. Алгоритмічні функції – класифікація, прогнозування, розпізнавання, виявлення аномалій – поки що застосовуються лише в окремих підсистемах, передусім у сфері відеонагляду та автофіксації порушень ПДР. У системах аналітики поліції застосування алгоритмів обмежується експериментальними проектами, що перебувають на ранніх етапах, без інтеграції в централізований операційний контур [22].

Проблемою є й технічна застарілість частини серверного обладнання та програмних комплексів, що у деяких підрозділах не оновлювалися від 2016–2018 років. Це ускладнює застосування сучасних моделей машинного навчання, які вимагають значної обчислювальної потужності та можливості обробляти відеопотоки в режимі реального часу. На це вказують і фахові огляди щодо спроможності автоматизованих систем міністерств обробляти інтенсивні дані, де відзначається, що без модернізації апаратної та мережевої інфраструктури відомства ШІ-рішення будуть працювати лише локально або тестово [16].

Ефективність цифрових інструментів МВС визначається також кваліфікацією персоналу. За оцінками експертів, частина співробітників підрозділів МВС та поліції не має достатньої підготовки до роботи із сучасними цифровими системами, що знижує фактичну ефективність навіть уже впроваджених рішень. Наприклад, у роботі з оперативними базами працівники часто дублюють записи, створюють текстові описи без структурованих полів або додають фотоматеріали у форматах, які погано піддаються подальшому аналізу. Ці проблеми знижують якість даних та ускладнюють машинне навчання, оскільки алгоритми працюють найбільш ефективно лише за умов системності та уніфікованості даних [28, с.29].

З огляду на міжнародний досвід, навчання персоналу є ключовою умовою переходу від цифровізації до застосування штучного інтелекту в правоохоронній діяльності. У країнах ЄС і США широкомасштабне впровадження алгоритмічних технологій супроводжувалося системними програмами перепідготовки співробітників, створенням спеціалізованих аналітичних підрозділів та введенням нових посад, відповідальних за алгоритмічну етику та аудит моделей [59].

Отже, готовність цифрових інструментів МВС до впровадження штучного інтелекту є частковою та нерівномірною. Сервісні та реєстрові системи вже відповідають більшості технічних вимог, включаючи структуровані дані, захищені канали зв’язку, інтегрованість та надійну валідацію. У той же час оперативно-аналітичні підсистеми потребують масштабної модернізації та

уніфікації. Наявність цих дисбалансів визначає загальний рівень готовності як помірний, але перспективний, за умови системного оновлення нормативної бази, апаратної інфраструктури, стандартів даних і кваліфікації персоналу.

2.3. Організаційні, етичні та технічні обмеження впровадження інтелектуальних технологій у діяльність підрозділів МВС

Упровадження систем штучного інтелекту в діяльність МВС України є складним процесом, що потребує глибокої інституційної перебудови. Це не технічна модернізація в класичному розумінні, а трансформація управлінських підходів, процедур, відповідальності, культури прийняття рішень і міжвідомчої взаємодії. У мирних країнах подібні зміни тривають роками; в Україні ж вони ускладнюються воєнним станом, обмеженими ресурсами та підвищеним навантаженням на правоохоронні структури. В умовах постійних загроз, нестачі персоналу та необхідності швидкого реагування кожна організаційна зміна має бути виваженою, а будь-яке нове технологічне рішення – сумісним із реаліями безпекового сектору. Саме тому питання організаційних бар’єрів постає як один із ключових і потребує окремого детального аналізу.

Першим важливим аспектом є те, що структура МВС історично формувалась у логіці ієрархічного управління, орієнтованого на чіткі вертикальні команди, а не на дані та алгоритмічну аналітику. У такій моделі цифрова трансформація просувається повільніше, адже впровадження інтелектуальних технологій потребує гнучкості, міжвідомчого обміну та внутрішніх механізмів самонавчання систем. Нинішні управлінські процедури здебільшого розраховані на лінійні процеси прийняття рішень, де аналіз виконується людиною, а не алгоритмом. Це створює інституційну інерцію: навіть за наявності сучасних цифрових платформ значна частина рішень ухвалюється традиційними способами, без використання потенціалу даних.

Другою проблемою є відсутність сталих внутрішніх регламентів щодо використання аналітичних алгоритмів у різних підрозділах. Реєстри,

відеоаналітика та сервісні системи працюють за власними нормами, проте алгоритмічні рішення потребують єдиної політики – хто відповідає за модель, як її перевіряють, як фіксують упередження, хто проводить аудит рішень, яким чином забезпечується дотримання принципів захисту персональних даних. У ряді європейських країн ці процедури визначені нормативно, зокрема в межах Artificial Intelligence Act, де передбачено обов'язковий контроль за «високоризиковими системами» [59]. В Україні такі стандарти лише формуються, що створює організаційну невизначеність і реальний ризик фрагментарності впровадження.

Важливою організаційною перешкодою є й те, що цифровізація у МВС просувається нерівномірно між різними службами. Деякі підрозділи мають розвинені інформаційні системи, налагоджені канали передачі даних та сучасне обладнання, тоді як інші досі працюють із застарілими базами, ручним введенням даних або частково паперовими процесами. За таких умов навіть ефективна локальна ШІ-модель не приноситиме користі системі загалом, оскільки вимагатиме надійного доступу до даних, а не фрагментарної інфраструктури [22]. Це особливо помітно у взаємодії сервісних центрів МВС, Національної поліції та міських систем відеомоніторингу: інституційна асиметрія знижує можливість формування єдиної аналітичної екосистеми.

Окремо варто виділити кадровий фактор. Хоча МВС активно впроваджує цифрові сервіси, рівень цифрової компетентності співробітників є дуже нерівномірним. У частини персоналу відсутні навички роботи з інтелектуальною аналітикою, що унеможливлює використання навіть тих функцій, які вже закладені у чинних платформах. Міжнародний досвід демонструє, що впровадження інтелектуальних систем потребує створення окремих підрозділів аналітичної підтримки, посади «офіцера з алгоритмічної етики», а також обов'язкової системи навчання для оперативного персоналу [61].

Ще одним організаційним бар'єром є обмежена внутрішня координація у питаннях управління даними. В Україні відсутня централізована модель Data Governance у системі МВС, тоді як більшість країн ЄС перейшли до

стандартизованих політик управління даними відповідно до Data Governance Act [58]. Нечіткий розподіл відповідальності за якість записів, інтеграцію реєстрів та стандарти метаданих обмежує можливість формування наскрізних алгоритмічних рішень. Це особливо критично для систем, що включають відеопотоки та оперативно-аналітичні дані, де відсутність уніфікованих правил ускладнює створення високоточних моделей прогнозної аналітики.

У воєнних умовах організаційні бар'єри посилюються. Часте переміщення підрозділів, зміни дислокацій, ротації персоналу, необхідність негайного реагування на загрози об'єктивно знижують можливість тривалих цифрових проєктів. При цьому зростає потреба у швидкому прийнятті рішень, що ускладнює підготовку, тестування і впровадження складних алгоритмічних систем, які вимагають стабільності, навчання моделей та постійного контролю за їхньою роботою.

Крім цього,застосування штучного інтелекту в правоохоронній сфері неминуче піднімає питання етики, оскільки саме тут алгоритмічні рішення безпосередньо впливають на безпеку громадян, приватність, презумпцію невинуватості та довіру до держави. Для МВС України ці виклики стають ще більш складними через високий суспільний запит на безпеку, поєднаний із воєнними ризиками та потребою забезпечити захист прав людини навіть у надзвичайних умовах. Алгоритмічні системи у сфері правопорядку не можуть розглядатися виключно як технологічні інструменти – це частина державної влади, що підлягає суворим правовим і моральним обмеженням. Тому етичний вимір впровадження штучного інтелекту в діяльність МВС фактично визначає межі допустимого використання технологій у публічному адмініструванні.

Одним із найбільш дискусійних питань є баланс між безпекою та приватністю. Використання розпізнавання облич, біометричної аналітики та масового відеомоніторингу здатне значно підвищити ефективність реагування, але водночас несе ризик перетворення окремих практик на інструмент надмірного контролю. Дослідження міжнародних експертних груп підкреслюють, що навіть технології високої точності демонструють різний

рівень похибки залежно від віку, освітлення та фізіологічних особливостей людини, що може створювати нерівність у ставленні до різних груп населення. Саме тому низка країн ЄС впровадила обмеження на застосування біометричних систем у публічних просторах, підкреслюючи пріоритет громадянських свобод над потенційною оперативною вигодою [59]. Для України ця дилема актуальна вдвічі більше, оскільки суспільство очікує від поліції швидких результатів, але не готове приймати непрозорі практики, що можуть бути неправильно застосовані або зловживані.

Наступним важливим етичним викликом є питання прозорості алгоритмічних рішень. У правоохоронній сфері помилки моделі мають реальні наслідки – необґрунтовані перевірки, неправдиві індикатори ризику або навіть хибні підозри. У міжнародній практиці підхід Explainable AI (XAI) розглядається як мінімальний стандарт: кожне автоматизоване рішення повинно мати можливість бути поясненим, відтвореним та юридично оскарженим. Це особливо важливо для систем, що працюють у профілюванні, прогнозуванні злочинності чи аналізі поведінкових патернів. Натомість реальна практика вказує, що складні моделі машинного навчання часто є «чорними скриньками», і навіть розробники не завжди можуть пояснити внутрішню логіку їх рішень. Для МВС України відсутність прозорості означатиме ризик зниження довіри громадян і збільшення кількості конфліктів між громадянами та поліцією, що не має права діяти на основі непрозорих критеріїв.

Проблема алгоритмічних упереджень також залишається критичною. Навіть якщо модель формально відповідає технічним стандартам, вона відтворює структуру даних, на яких її навчено. Якщо історичні дані містять нерівність, вибіркові перевірки, неповноту або помилки, алгоритм множить їх і робить системною нормою. У Сполучених Штатах та Великій Британії зафіксовано випадки, коли аналітичні моделі прогнозування злочинності (PredPol, AWARE) відтворювали упередження проти окремих районів або соціальних груп, оскільки їх навчали на історичних патернах вибіркових поліцейських перевірок [61]. В українських умовах ризики ще вищі, оскільки частина кримінологічних даних

неповна через воєнні події, руйнування інфраструктури та зміну демографічної структури. Це означає, що навіть добросовісно створена модель може автоматично генерувати викривлені прогнози, які впливатимуть на оперативні рішення.

Окрему етичну проблему становить питання відповідальності за автоматизовані рішення. У традиційній моделі поліцейський особисто відповідає за ухвалену дію. Проте в системах, де рішення ухвалюються або рекомендуються алгоритмом, виникає питання: хто є носієм відповідальності – розробник, оператор, керівник підрозділу чи сам алгоритм як «цифровий агент»? У країнах ЄС ця проблема частково вирішується через принцип подвійної відповідальності – за модель відповідає розробник, за застосування – відповідна державна установа. В Україні такого механізму немає, що створює правову прогалину та підвищує ризик того, що посадова особа буде «покладатися на алгоритм», уникаючи власного аналізу.

Варто згадати і про етичний вимір воєнного стану. В умовах війни суспільство більш терпиме до посилених заходів безпеки, але саме тому зростає ризик надмірного використання технологій, що за спокійних умов були б обмежені. Наприклад, розширення масового відеоспостереження може бути виправдане необхідністю протидії ДРГ під час активних бойових дій, але після завершення війни така система вже сприйматиметься як надмірний контроль. Етична відповідальність держави полягає в тому, щоб забезпечити прозорі часові рамки та чіткі критерії для згорнення надзвичайних повноважень після закінчення воєнної необхідності.

Крім того, застосування ШІ у сфері правопорядку потребує постійного громадського контролю. У міжнародній практиці створюються наглядові ради, етичні комітети, групи незалежних експертів, що перевіряють алгоритми та методи збору даних. Це не формальність, а інструмент забезпечення демократичної легітимності алгоритмічних рішень. В українських умовах, де рівень довіри до державних інституцій традиційно залишається невисоким,

створення таких механізмів є передумовою для безпечного й прийнятного використання інтелектуальних технологій.

Технічна сторона впровадження систем штучного інтелекту у діяльність МВС України є однією з найскладніших, оскільки вона поєднує вимоги до інформаційної безпеки, якості даних, надійності інфраструктури та сумісності між різними цифровими платформами, що вже функціонують у відомстві. Якщо етичні ризики визначають межі допустимого застосування технологій, то технічні – визначають реальні можливості впровадження. МВС оперує великим масивом чутливої інформації: оперативно-розшуковими даними, матеріалами кримінальних проваджень, персональними даними громадян, відеопотоками з камер, інформацією про переміщення осіб та транспортних засобів. Будь-яка технологічна зміна повинна забезпечувати не лише інноваційність, але й гарантовану безпеку, безперервність роботи та дотримання вимог законодавства.

Однією з ключових технічних проблем є фрагментованість і нерівномірність цифрової інфраструктури. Значна частина інформаційних систем МВС будувалася у різні роки, з використанням різних технологічних підходів, різних форматів даних та принципів зберігання. Деякі системи модернізовані й інтегровані у спільні платформи, інші – працюють автономно, накопичуючи інформацію локально або в сумісних, але застарілих форматах. Така неоднорідність призводить до труднощів із централізованим збором та обробкою даних, що є критично важливим для навчання алгоритмів штучного інтелекту. Моделі машинного навчання потребують великих, чистих і структурованих масивів даних, а саме це у відомстві є обмеженим ресурсом. Навіть сучасні системи, такі як Єдина система відеомоніторингу, інтегрують потоки з тисяч камер різних поколінь, різного формату, роздільної здатності та технічного стану, що впливає на можливість високоточного розпізнавання.

Другим критичним технічним обмеженням є якість даних. Навіть за наявності великих обсягів інформації, дані можуть бути неповними, зашумленими, містити апаратні або людські помилки, суперечності чи дублікати. У воєнних умовах ця проблема посилюється, оскільки частина інфраструктури

зруйнована, а переміщення населення змінює демографічні й поведінкові патерни. Алгоритми, що працюють на низькоякісних даних, формують хибні моделі ризиків, переоцінюють загрозу в певних районах або, навпаки, не здатні виявити реальні аномалії. Висока помилка класифікації або прогнозування в системах МВС несе значно більші ризики, ніж у цивільних секторах: помилкові індикатори загрози можуть вплинути на оперативне реагування, вибір пріоритетних напрямів патрулювання або дії спецпідрозділів. Саме тому якість даних та очищення інформаційних масивів є фундаментально важливим етапом, без якого застосування ШІ стає небезпечним.

Третім блоком технічних ризиків є інформаційна безпека. МВС працює у середовищі постійних кібератак, а системи штучного інтелекту є ще більш вразливими до нових класів загроз – атак на моделі, маніпуляції даними, підміна відеопотоків, «отруєння» навчальних вибірок, експлуатація вразливостей нейромереж. На відміну від традиційних інформаційних систем, ШІ-моделі можуть змінювати поведінку під впливом дуже незначних руйнівних сигналів, які непомітні людині, але суттєво впливають на алгоритм. У секторі безпеки це може проявлятися у тому, що нападники модифікують камуфляж, маркери на транспортних засобах або цифрові артефакти, щоб зменшити ймовірність ідентифікації. Таким чином, штучний інтелект може не лише допомагати державі, але й становити вразливість, якщо не захищений комплексними засобами кібероборони.

Для МВС важливо враховувати також проблему масштабованості. Системи прогнозування злочинності, поведінкової аналітики чи розпізнавання облич споживають значні обчислювальні ресурси, вимагають потужних серверів, графічних процесорів та спеціалізованих сховищ даних. Україна, на відміну від технологічно розвинених країн, не має достатнього парку дата-центрів, здатних виконувати обробку великих обсягів відео у режимі реального часу. Залучення хмарних технологій обмежене вимогами національної безпеки, адже значна частина даних не може передаватися за кордон. Це створює технічну дилему: ШІ-

системи потребують потужної інфраструктури, але її створення вимагає значних фінансових і часових ресурсів, що в умовах війни не завжди доступно.

Ще один аспект – сумісність та інтероперабельність. Будь-яка інтелектуальна система у сфері МВС має взаємодіяти з іншими державними реєстрами, сервісами, інформаційними платформами. Проте єдиних стандартів обміну даними досі бракує, що ускладнює інтеграцію та синхронізацію. У перспективі це може створювати ситуації, коли різні підрозділи МВС працюватимуть на різних алгоритмах, що генерують суперечливі рекомендації. У міжнародній практиці інтеграція ШІ у правоохоронну діяльність передбачає створення єдиної архітектури даних, уніфікованих API, централізованих реєстрів та протоколів безпеки. В Україні така архітектура лише формується.

Не менш серйозним ризиком є технічна залежність від приватних розробників. Більшість сучасних моделей ШІ створюються комерційними компаніями або іноземними вендорами. Для МВС це означає ризик залежності від закритого коду, відсутності доступу до вихідних алгоритмів і неможливості повного контролю над логікою моделі. Також існує небезпека припинення підтримки окремих рішень або їх дорожчання, що ставить під питання довгострокову стабільність проєктів. Правоохоронні технології повинні бути автономними, стійкими та незалежними від політичних чи ринкових змін.

Висновки до розділу 2

Аналіз сучасного стану нормативно-правового забезпечення, цифрових інструментів та організаційно-технічних умов упровадження систем штучного інтелекту в діяльність МВС України показує, що відповідна трансформація вже має суттєві передумови, але водночас стикається з низкою об’єктивних обмежень. Нормативні акти, прийняті протягом останніх років, підтверджують політичну волю держави до цифровізації сектору внутрішньої безпеки та переходу до інтелектуальних форм управління. Законодавство щодо захисту даних, національної безпеки, цифрової держави та інформатизації МВС створює

базові рамки для впровадження інтелектуальних рішень, але вони ще не формують цілісної моделі регулювання алгоритмічних технологій у правоохоронній сфері. Значна частина положень потребує оновлення з урахуванням появи систем високого ризику, необхідності їх сертифікації, прозорості та підзвітності.

Аналіз існуючих цифрових інструментів МВС демонструє, що відомство має великий потенціал для інтеграції ШІ у вже функціонуючі системи – від відеоаналітики і біометричних модулів до сервісів взаємодії з громадянами та внутрішніх інформаційних реєстрів. Проте більшість рішень залишаються на рівні окремих технологічних компонентів, що лише частково використовують можливості автоматизації та даних. Інформаційні платформи МВС розвиваються нерівномірно, акумулюють великі обсяги інформації, але не завжди забезпечують достатню структурованість і сумісність, необхідні для роботи складних алгоритмів. Крім того, зафіксована проблема фрагментованості: різні підрозділи відомства мають нерівний доступ до технологій, що ускладнює створення єдиного інтелектуального контуру.

Організаційні, етичні та технічні складнощі суттєво впливають на швидкість і безпечність впровадження ШІ у практику МВС. Брак уніфікованих стандартів управління даними, кадровий дефіцит фахівців з аналітики та кібербезпеки, слабка горизонтальна координація між підрозділами, а також загальна складність роботи у воєнний час формують сукупність структурних бар'єрів. Етичні виклики – приватність, прозорість, алгоритмічні упередження, баланс між безпекою та правами людини – мають ключове значення, оскільки визначають рівень суспільної довіри. Технічні обмеження – якість даних, відсутність єдиної інфраструктури, вразливість моделей до кібератак, потреба у масштабованих обчислювальних ресурсах – ускладнюють перехід від окремих цифрових сервісів до повноцінних інтелектуальних систем.

Отже, можна зробити висновок, що система МВС перебуває на етапі активного, але нерівномірного розвитку. Відомство має стратегічну потребу у впровадженні штучного інтелекту для посилення аналітики, оперативного

реагування та управлінської ефективності, проте потенціал цих технологій поки що не реалізовано повною мірою. Для переходу до нового рівня функціонування потрібне комплексне оновлення нормативної бази, інфраструктури даних, технічних стандартів і організаційних процедур, а також формування чіткої моделі етичного контролю за алгоритмічними рішеннями.

РОЗДІЛ ІІІ. ПЕРСПЕКТИВИ ТА МЕХАНІЗМИ ВПРОВАДЖЕННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНЕ АДМІНІСТРУВАННЯ МВС УКРАЇНИ

3.1. Концептуальна модель застосування систем штучного інтелекту в управлінських процесах МВС України

Пропонована концептуальна модель інтеграції штучного інтелекту в управлінську діяльність МВС України передбачає формування системного, нормативно визначеного та організаційно збалансованого підходу до використання інтелектуальних технологій у виконанні функцій публічного адміністрування. Її зміст ґрунтується на принципах належного врядування, пріоритеті прав та свобод людини, підзвітності органів влади та орієнтації на результат.

Модель складається з чотирьох взаємопов’язаних компонентів:

1. Нормативно-правовий компонент. Передбачає визначення правових рамок використання ШІ у діяльності поліції, регламентацію алгоритмічної обробки даних, захист персональної інформації, прозорість та контроль автономних систем. Законодавча визначеність забезпечує легітимність рішень, унеможливлює зловживання та встановлює межі автоматизованих повноважень.

2. Організаційно-управлінський компонент. Спрямований на адаптацію управлінських процесів МВС до роботи з інтелектуальними системами: створення відповідальних підрозділів, визначення ролей і компетенцій, розвиток цифрової культури, формування політики управління даними. Особлива увага надається взаємодії між структурними підрозділами, що забезпечує єдиний управлінський цикл на основі даних.

3. Інформаційно-технологічний компонент. Містить розвиток єдиної цифрової інфраструктури МВС, інтеграцію реєстрів, платформ відеоспостереження, аналітичних центрів та сервісних систем. У межах моделі ШІ застосовується для прогнозування динаміки правопорушень, підтримки

управлінських рішень, автоматизації документообігу, оптимізації реагування та аналітики великих масивів даних.

4. Сервісно-комунікаційний компонент. Передбачає модернізацію взаємодії поліції з громадянами: впровадження інтелектуальних чат-сервісів, автоматизованих консультацій, покращення доступу до адміністративних послуг, зменшення часу їх надання. Застосування ШІ посилює відкритість МВС та сприяє зростанню довіри до органів публічної влади.

Загалом концептуальна модель інтеграції ШІ в управлінські процеси МВС формує підґрунтя для переходу до даних-орієнтованого управління, забезпечує підвищення ефективності діяльності поліції, а також створює передумови для безпечного та етичного використання інтелектуальних технологій у межах публічної служби.

Для поліції це означає, зокрема зміну підходів до прийняття рішень – від інтуїції й емпіричних практик до аналітики, прогнозів і стандартів; підвищення швидкості реагування; зменшення людського фактору у рутинних admin-задачах; оптимізацію ресурсів; покращення планування. Таким чином, ШІ може стати інструментом не лише оперативної діяльності, а стратегічного управління і розвитку системи.

Використання алгоритмів у публічному секторі потребує адаптації класичних принципів публічного управління. Саме тому міжнародні рамки застосування ШІ наголошують на таких базових цінностях, як права людини, демократичні стандарти, справедливість і прозорість [56]:

- Прозорість – алгоритмічні рішення поліції мають бути зрозумілі, відкриті для контролю, з можливістю перевірки логіки ухвалених рішень, ознайомлення громадян з правилами роботи систем. Це унеможливлює «чорні скриньки», коли рішення видаються без пояснень.

- Підзвітність – відповідальні за розробку, впровадження й експлуатацію систем ШІ мають бути чітко визначені, а орган влади або підрозділ повинен нести відповідальність за наслідки. У публічному управлінні не може бути «відмивання рук» через автоматизацію.

- Ефективність – системи мають підвищити якість управління, зменшити витрати часу та ресурсів, забезпечити оптимальне використання даних, підвищити результативність роботи МВС. Але при цьому ефективність має йти разом з легітимністю і дотриманням прав.

- Відповідальність – впровадження ШІ не може знімати відповідальність з людей. Рішення, які впливають на життя та свободи громадян, мають залишатися під контролем компетентних посадових осіб. Саме тому моделі ШІ повинні доповнювати, а не замінювати людину в кінцевому ухваленні рішень.

Ці принципи вже закріплені у багатьох міжнародних ініціативах з урядування ШІ: OECD – через свої AI Principles, European Commission – через Guidelines for Trustworthy AI, а також у численних академічних роботах, які підкреслюють необхідність балансу між інноваціями та суспільними цінностями [66].

Для ефективної інтеграції ШІ МВС має відповідати кільком інституційним умовам: нормативній визначеності, внутрішній організаційній структурі, наявності компетентних підрозділів, процедурі доступу до даних та ресурсів. У вітчизняних аналітичних роботах наголошується, що цифрові інновації в МВС неможливі без оновлення процедур управління, створення спеціальних аналітичних департаментів, підготовки кадрів і систематичного аудиту якості даних.

Структура МВС включає поліцію, служби охорони, ДСНС, прикордонну службу, міграційну службу – кожна з яких потребує власних алгоритмічних рішень, але в межах єдиної координації та управлінської логіки міністерства. Саме тому ШІ має інтегруватися як частина системи публічного управління, а не як окремий технічний експеримент [50].

Головна функція держави у впровадженні ШІ – встановлення правил, обмежень і стандартів застосування технологій у секторі безпеки. У роботах українських дослідників наголошується, що алгоритмічні системи у поліції потребують суворих правових рамок, оскільки можуть впливати на приватність, справедливість та рівність громадян перед законом [59].

Управління МВС має визначати:

– допустимі сфери застосування ШІ;

– межі автоматизації управлінських та оперативних процесів;

– механізми аудиту та моніторингу алгоритмічних систем;

– процедури оскарження рішень, до яких залучено ШІ;

– вимоги до підготовки персоналу та інституційного супроводу технологій.

Такі підходи відображені у наукових роботах, що аналізують впровадження інтелектуальних технологій у правоохоронній діяльності та підкреслюють необхідність балансу між інноваціями та гарантіями прав людини [60].

Міжнародні рамки (наприклад, рекомендації UNESCO, стандарти від OECD та інших) показують, що без участі держави як регулятора і гаранта прав застосування ШІ в публічному управлінні неможливе. Тому інтеграція ШІ в діяльність МВС України має будуватися не як хаотичне запровадження технологій, а як системна реформа публічного управління на основі принципів доброго врядування. Лише за умови чітко визначеної політики, відповідальності, прозорості, нормативної бази та адаптованої інституційної структури, ШІ може стати дієвим інструментом підвищення ефективності, прозорості та якості роботи поліції. Без таких управлінських засад алгоритмічні системи ризикують залишитися технологічною ілюзією або, гірше – джерелом порушень прав та довіри суспільства.

Отже, концептуальна модель застосування систем штучного інтелекту в управлінських процесах МВС України має враховувати декілька рівнів організаційно-правових умов. Перший рівень організаційно-правових умов – це базові закони, які визначають статус Національної поліції, правила роботи з інформацією, захист персональних даних та загальні засади національної безпеки. Закон України «Про Національну поліцію» задає рамки повноважень поліції, принципи її діяльності, вимоги до дотримання прав людини та публічної безпеки [1]. Будь-які системи штучного інтелекту, що застосовуються у діяльності поліції, мають бути вписані саме в цю систему повноважень, а не створювати паралельну «алгоритмічну» реальність.

Закон «Про інформацію» визначає загальні принципи інформаційних відносин, права суб’єктів, режими доступу до інформації та обов’язки розпорядників [2]. Для МВС це означає, що використання ШІ в управлінні даними (аналітика, прогнозування, відеоспостереження, аналітичні платформи) має відповідати вимогам законності, достовірності, повноти й захищеності інформації. Окремо Закон «Про захист персональних даних» встановлює правила обробки персональної інформації, що є критичним для будь-яких інтелектуальних систем, які працюють з біометрією, відеозображеннями, базами даних правопорушень чи міграційними реєстрами [3].

Водночас Закон «Про національну безпеку України» закріплює принципи сектору безпеки і оборони, включно з вимогами до демократичного цивільного контролю, прозорості та підзвітності діяльності силових структур [4]. У контексті ШІ це означає, що алгоритмічні рішення у сфері безпеки не можуть діяти у «сірій зоні» поза демократичним контролем, а повинні бути включені у загальну систему планування та оцінювання ризиків.

Другий рівень – стратегічні та концептуальні документи, які задають напрям цифрової трансформації держави та використання ШІ як окремого інструменту публічної політики. Розпорядження Кабінету Міністрів про схвалення Концепції розвитку штучного інтелекту в Україні сформувало базові уявлення про роль ШІ в економіці, публічному секторі, освіті, безпеці та правосудді [6]. У Концепції визначено загальні принципи – безпечність, етичність, орієнтація на права людини, підтримка інновацій, – які безпосередньо стосуються і можливого використання ШІ у діяльності МВС.

Подальшим кроком стало затвердження Плану заходів з реалізації Концепції розвитку ШІ на 2025–2026 роки, у якому передбачені конкретні кроки щодо пілотних проєктів, навчання кадрів, розроблення регуляторних підходів та створення інфраструктури даних [7]. Для МВС це створює формальну можливість включати свої ініціативи у загальнодержавну політику розвитку ШІ, а не рухатися ізольовано.

Стратегія розвитку цифрової держави до 2030 року фіксує цифрову трансформацію публічного сектору як один із ключових напрямів державної політики [8]. У документі акцентується на розвитку електронних послуг, інтегрованих державних реєстрів, аналітичних платформ, систем кібербезпеки. Усе це безпосередньо стосується МВС як великого розпорядника даних і надавача адміністративних та сервісних послуг (сервісні центри, реєстраційні дії, міграційні процедури) [8; 35; 36].

Розпорядження Кабінету Міністрів «Деякі питання цифрової трансформації» додатково структурує підходи до цифровізації органів виконавчої влади, визначаючи відповідальних суб'єктів, підходи до проєктного управління, стандарти електронної взаємодії та пріоритетність цифрових рішень [10; 36]. Для МВС ці документи задають рамку, у якій інтелектуальні системи мають розглядатися як елемент цифрової політики, а не окрема «винахідливість» окремого департаменту.

Третій рівень організаційно-правових умов – галузеві акти, спрямовані на інформатизацію та модернізацію системи МВС, а також внутрішня організаційна структура, яка забезпечує реалізацію цифрової політики. Концепція програми інформатизації системи МВС України на 2021–2023 роки визначила напрями розвитку цифрової інфраструктури, створення та інтеграції відомчих інформаційних систем, використання електронних сервісів та модернізації відомчих телекомунікаційних мереж [9]. Наказ МВС щодо єдиної цифрової відомчої телекомунікаційної мережі закріпив технічну основу для об'єднання підрозділів у єдиний інформаційний простір [11].

Стратегія розвитку органів системи МВС до 2030 року окреслює необхідність подальшої цифрової трансформації, у тому числі шляхом впровадження аналітичних інструментів, автоматизації процесів, розвитку електронних сервісів і посилення взаємодії з громадянами через цифрові канали [12; 27; 35]. У цьому контексті системи ШІ мають розглядатися як логічний наступний крок: від створення розрізнених баз даних – до інтегрованих

аналітичних платформ, які підтримують управлінські рішення, оцінюють ризики, оптимізують розподіл ресурсів.

Додаткові організаційні орієнтири задає Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони на 2023–2027 роки [5]. У ньому закріплені цілі щодо підвищення ефективності, прозорості й підзвітності органів правопорядку, посилення координації між інституціями, удосконалення кадрової політики. Інтелектуальні системи можуть стати інструментом реалізації цих завдань, але лише за умови, що МВС адаптує свої внутрішні регламенти до нових управлінських практик, пов'язаних із використанням даних і алгоритмів [5; 21; 25; 38; 61].

Формування організаційно-правових умов інтеграції ШІ у діяльність МВС залежить також від урахування міжнародних стандартів. Artificial Intelligence Act ЄС встановлює категорії ризику для систем ШІ, вимоги до прозорості, управління даними, оцінки впливу та нагляду за використанням високоризикових систем, до яких потенційно належать і поліційні алгоритми [24; 59]. Рекомендації Ради Європи та Європейської комісії щодо етичного й надійного ШІ акцентують на необхідності прозорості, підзвітності та можливості людського контролю [55; 57]. Документ Європейського парламенту про використання ШІ в кримінальному праві окремо наголошує на ризиках для прав людини у сфері діяльності поліції та судових органів [52].

Для МВС України ці міжнародні підходи є орієнтиром при формуванні власних внутрішніх політик щодо застосування аналітичних систем, відеоаналітики, прогнозних моделей ризиків, автоматизованих рішень у сфері безпеки [21; 25; 38; 48; 52; 61]. З урахуванням євроінтеграційного курсу України організаційно-правові умови інтеграції ШІ повинні будуватися таким чином, щоб у майбутньому бути сумісними з європейськими регуляторними рамками.

У поєднанні з міжнародними стандартами та рекомендаціями ці документи створюють рамку, у якій ШІ може бути впроваджений не як «чужорідний технологічний елемент», а як частина цілісної управлінської реформи. Без такого організаційно-правового фундаменту будь-яке використання інтелектуальних

систем у роботі поліції залишатиметься ризикованим, фрагментарним і вразливим до юридичних, етичних та суспільних претензій, адже потенціал штучного інтелекту в системі МВС України не зводиться до «розумних камер» або поодиноких аналітичних модулів. Йдеться про поступове переформатування ключових управлінських і сервісних функцій: від планування превентивних заходів до надання адміністративних послуг населенню та підтримки стратегічних рішень керівництва. У зарубіжних та українських дослідженнях дедалі частіше наголошується, що ШІ у правоохоронній сфері має розглядатися не лише як інструмент кримінального аналізу, а як складова сучасного публічного управління, заснованого на даних, прозорості і підзвітності [21; 25; 28; 38; 61].

Наприклад, традиційно превенція злочинності спиралася на досвід оперативного складу, статистику попередніх років, загальні уявлення про криміногенну ситуацію. Інтелектуальні системи дають можливість зробити цю діяльність набагато більш керованою і формалізованою. Наукові праці, присвячені ролі ШІ у правоохоронній діяльності, акцентують на здатності алгоритмів виявляти приховані закономірності у великих масивах даних, будувати прогнози щодо концентрації ризиків, виявляти аномалії у поведінці суб’єктів чи динаміці подій [25; 38; 48].

Для МВС це означає, що превенція може бути спроєктована як повноцінна управлінська функція, підкріплена інтелектуальною аналітикою. На практиці йдеться про використання систем, які:

– аналізують історичні дані про правопорушення, їх просторово-часовий розподіл та контекст (тип місцевості, час доби, події, соціально-економічні фактори);

– формують «карти ризику» для планування патрулювання, розміщення сил і засобів, додаткових профілактичних заходів;

– виявляють повторювані шаблони, що можуть свідчити про серійні правопорушення, організовану діяльність чи уразливість конкретних об’єктів.

Українські автори, які аналізують застосування ШІ у протидії злочинності, прямо вказують на можливість використання алгоритмічних систем для підвищення адресності превентивних заходів, за умови дотримання прав людини та недопущення дискримінаційних практик [38; 48]. У цьому контексті штучний інтелект виступає не як «автоматизований наглядач», а як управлінський інструмент, що дає можливість керівництву поліції планувати роботу більш раціонально, спираючись на формалізовані прогнози, а не лише на суб'єктивні оцінки.

Окремий напрямок – використання даних із систем відеомоніторингу. Проєкт Закону про єдину систему відеомоніторингу стану публічної безпеки, офіційні повідомлення МВС та аналітичні публікації свідчать, що в Україні вже формується масштабна інфраструктура камер, інтегрованих з централізованими центрами спостереження [13; 22; 23; 45; 46]. За наявності належного правового регулювання та технічних обмежень саме системи ШІ здатні перетворити цей масив відеоданих на інструмент превенції – від виявлення підозрілих об'єктів до своєчасного інформування чергових служб про потенційні загрози.

Другий ключовий напрям – оптимізація реагування на події та координація підрозділів. Сучасні правоохоронні органи працюють у режимі постійного перевантаження інформацією: тисячі викликів, повідомлень, сповіщень із різних систем. Інтелектуальні технології тут можуть виконувати роль «керуючої надбудови», яка допомагає диспетчеру і керівнику підрозділу приймати оперативні рішення. Дослідження та аналітичні матеріали щодо цифровізації сервісних центрів МВС, розвитку відомчих телекомунікаційних мереж та інформаційних систем підтверджують, що в міністерстві вже створюється технічна основа для інтеграції таких рішень [9; 11; 12; 27; 35].

Штучний інтелект може використовуватися для:

– автоматизованого пріоритезування викликів (розподіл за рівнем терміновості та потенційної небезпеки);

– рекомендацій щодо оптимального маршруту та складу нарядів для реагування з урахуванням місцезнаходження, завантаженості, дорожньої ситуації, попередніх подій у районі;

– оперативного зведення інформації з різних джерел (телефонні звернення, відео, сенсори, реєстри), щоб черговий підрозділ отримував структуровану картину події, а не розрізнені фрагменти.

Аналіз досвіду використання інтелектуальних технологій у правоохоронних органах, зокрема у контексті міжнародних документів щодо ШІ у кримінальному праві та роботі поліції, демонструє, що такі системи здатні скоротити час реагування та підвищити якість координації, якщо їх впровадження супроводжується чіткими процедурами людського контролю [52; 61; 66].

Для МВС України, з огляду на воєнний стан, масштаб внутрішньо переміщеного населення та зростання навантаження на поліцію, оптимізація реагування за допомогою ШІ – питання управлінської спроможності – спроможності втримати контроль над ситуацією, коли ресурсів об’єктивно бракує, а ризики – високі [5; 12; 21; 38].

Третій напрям – застосування ШІ в сервісній функції МВС. Йдеться про реєстраційні дії, послуги сервісних центрів, роботу з електронними зверненнями, інтеграцію з порталом «Дія» тощо. Урядові рішення щодо цифровізації послуг і реформування сервісних центрів МВС прямо фіксують завдання скорочення бюрократії, підвищення зручності для громадян, переведення процедур в онлайн-формат [8; 10; 35; 36].

ШІ може посилити ці процеси, забезпечуючи:

– інтелектуальні чат-боти та віртуальних асистентів, які консультують громадян, допомагають обрати потрібну послугу, перевірити статус звернення;

– автоматизацію перевірок документів, виявлення помилок у поданих даних, попередження заявника про некоректні чи неповні відомості до того, як звернення потрапляє до працівника;

– попередню класифікацію та маршрутизацію звернень, щоб зменшити навантаження на персонал і скоротити строки розгляду.

У роботах, присвячених ШІ в публічному управлінні та правовій практиці, підкреслюється, що саме сервісний вимір дає змогу громадянам безпосередньо відчути переваги інтелектуальних технологій, а не лише сприймати їх як інструмент нагляду [20; 28; 39; 68]. Якщо МВС зможе поєднати інтеграцію ШІ з реальною зручністю для людей – прозорими онлайновими сервісами, швидким реагуванням, зрозумілим інтерфейсом – це прямо вплине на рівень довіри до поліції та міністерства загалом.

Водночас застосування ШІ в сервісній сфері вимагатиме суворого дотримання законодавства про інформацію та захист персональних даних, зокрема щодо режиму доступу до реєстрів, зберігання та повторного використання даних [2; 3; 36; 58]. Сервісна автоматизація не може перетворюватися на неконтрольований збір надлишкової інформації або приховане профілювання громадян.

Четвертий ключовий напрям – використання ШІ для підтримки управлінських рішень на стратегічному, тактичному та оперативному рівнях. У сучасних підходах до публічного управління наголошується, що дані стають базою для формування політик, оцінки їх результативності, планування ресурсів і реформ [28; 34; 66; 71]. Для МВС це означає, що інтелектуальні системи можуть бути задіяні не лише «в полі», а й у кабінетах керівників.

Йдеться про такі завдання, як:

– аналіз динаміки правопорушень у розрізі регіонів, категорій злочинів, соціально-демографічних характеристик;

– моделювання наслідків управлінських рішень (перерозподіл особового складу, зміна структури підрозділів, запровадження нових режимів роботи);

– оцінка ефективності превентивних програм, інформаційних кампаній, змін у нормативній базі;

– прогнозування потреб у ресурсах (техніка, персонал, навчання, кіберзахист).

Міжнародні аналітичні доповіді щодо ШІ в державному управлінні та безпековій сфері показують, що найбільший ефект дає саме поєднання аналітики

великих даних із управлінськими циклами «планування – реалізація – моніторинг – коригування» [51; 66; 71]. У національному вимірі це може означати, що керівництво МВС отримує не просто звіти «знизу», а інтегровані аналітичні панелі, де алгоритми допомагають виявити проблемні ділянки, неочевидні тенденції, потенційні «вузькі місця» у системі.

Окремий вимір – етичні та правові обмеження. Наукові розвідки у сфері цифрової етики, адміністративного права та інформаційної безпеки наголошують, що управлінські рішення, підкріплені ШІ, не можуть бути повністю автоматизованими у сферах, де йдеться про права і свободи людини, застосування примусу чи обмеження доступу до послуг [37; 40; 52; 57; 59]. Роль ШІ тут – підтримка, а не заміна керівника. Людина має зберігати остаточне слово, відповідальність і можливість врахувати контекст, який не завжди коректно відображається в даних.

У сукупності ці чотири напрями – превенція, реагування і координація, сервісні функції, підтримка управлінських рішень – окреслюють реальний простір для впровадження систем штучного інтелекту в публічне адміністрування МВС. Кожен із них спирається на вже наявні нормативні, організаційні та технологічні напрацювання, але потребує чітких правил, прозорих процедур і свідомого управлінського підходу, щоб ШІ посилив, а не деформував публічне управління в секторі внутрішньої безпеки.

3.2. Пропозиції щодо оптимізації інформаційно-аналітичної діяльності МВС за допомогою інтелектуальних систем

Ефективність управління у системі МВС безпосередньо залежить від якості інформаційно-аналітичної діяльності, оскільки саме вона забезпечує підготовку управлінських рішень, оцінювання ризиків, планування ресурсів та координацію діяльності підрозділів. В умовах воєнного стану, зростання обсягів даних, розвитку відеомоніторингу, кіберзагроз та високої динаміки безпекових подій традиційні методи аналізу виявляються недостатніми. Тому застосування

інтелектуальних систем стає ключовою передумовою для формування сучасної, адаптивної та прогнозної моделі управління.

Штучний інтелект дозволяє автоматизувати обробку великих масивів даних, виявляти приховані закономірності, прогнозувати зміни у криміногенній ситуації та забезпечувати об'єктивність управлінських рішень. У зв'язку з цим оптимізація інформаційно-аналітичної діяльності МВС передбачає комплекс пропозицій у трьох взаємопов'язаних напрямах.

По-перше, це вдосконалення управління даними, що включає формування політики data governance, упорядкування потоків інформації, зміцнення міжвідомчої взаємодії та визначення відповідальних посадових осіб. Такі кроки створюють організаційну основу для застосування інтелектуальних технологій.

По-друге, необхідною є модернізація інформаційно-аналітичної інфраструктури – розвиток аналітичних центрів, інтеграція наявних систем у єдиний управлінський контур, упровадження інструментів алгоритмічного аналізу, прогнозування та оцінювання ефективності. Це забезпечить перехід від описової аналітики до прогнозної та рекомендаційної.

По-третє, застосування ШІ має стати підґрунтям для управлінських та сервісних інновацій, що включають нові типи управлінських рішень, цифрові сервіси для громадян, інтелектуальний адміністративний контроль та автоматизовану підтримку кадрових процесів.

У сукупності ці напрями дозволять сформувати сучасну модель інформаційно-аналітичної діяльності МВС, що відповідає стандартам цифрової держави та міжнародним підходам до використання ШІ в публічному управлінні.

Удосконалення управління даними в системі МВС України є ключовою передумовою для впровадження інтелектуальних технологій. Будь-яка система штучного інтелекту потребує впорядкованих, якісних, актуальних та структурованих наборів даних, тоді як сьогоднішня модель взаємодії між підрозділами МВС залишається фрагментованою, регламентованою різними внутрішніми актами та нерівномірно цифровізованою. Національні документи, зокрема Стратегія розвитку органів системи МВС до 2030 року [12], Концепція

інформатизації системи МВС [9], а також Стратегія розвитку цифрової держави до 2030 року [8], підкреслюють, що цифрова трансформація неможлива без створення цілісної архітектури даних, встановлення єдиних правил їх обробки та підвищення управлінської культури роботи з інформаційними ресурсами.

Управління даними у правооохоронній сфері – це не просто технічна дисципліна, а окрема управлінська політика, яка визначає принципи доступу, обробки, інтеграції, зберігання та захисту інформації. Необхідність у такій політиці чітко випливає з законодавства про інформацію та захист персональних даних [2; 3], а також із обов'язку МВС забезпечити безперервність інформаційних процесів та оперативне прийняття рішень [1; 4].

У межах data governance мають бути визначені:

- єдині стандарти структурування даних (таксономії, формати, класифікатори);
- процедури контролю якості (виявлення дублювання, помилок, «мертвих» записів);
- правила міжвідомчого обміну;
- режими доступу, що відповідають принципам конфіденційності та пропорційності;
- механізми аудиту, передбачені також у документах ЄС про належне управління даними [58; 59].

Запровадженням системної політики управління даними МВС зможе усунути фрагментацію інформаційних ресурсів, яка сьогодні виникає через наявність понад десятка неінтегрованих реєстрів, окремих баз даних та регіональних підсистем. У звітах МВС підкреслюється, що цифрова трансформація відомства можлива лише за умов створення єдиної відомчої інформаційної екосистеми, що прямо відповідає завданням державної політики цифровізації [10; 27; 35].

Другим важливим компонентом є оптимізація управлінської взаємодії. Навіть найкращі алгоритми не працюватимуть у середовищі, де інформаційні

потоки є неструктурованими, несумісними або блокуються відомчими бар’єрами.

Поточні нормативні документи МВС містять вимоги щодо інтеграції сервісів, зокрема Положення про єдину цифрову телекомунікаційну мережу МВС [11], однак у реальності інформаційний обмін часто залишається паперовим або змішаним. Це уповільнює реагування, створює дублювання функцій і не дозволяє застосувати алгоритми штучного інтелекту до повного масиву оперативної інформації.

Необхідні адміністративні рішення охоплюють:

- створення централізованої системи інтеграції даних (integration layer);
- заміну ручних погоджувальних процедур на цифрові workflow-моделі;
- впровадження єдиних метаданих;
- запровадження ведомчих регламентів сумісності даних на рівні департаментів і територіальних органів.

Дослідження щодо цифрової етики та алгоритмічної прозорості вказують, що саме структурованість управлінських процесів є критичною умовою застосування ШІ у публічному секторі [40]. Лише після стандартизації процесів можлива автоматизація управлінських рішень, а не хаотичне використання окремих інструментів (табл.3.1.).

Таблиця 3.1.

Ключові управлінські проблеми та напрями їх вирішення через політику data governance

Проблема	Наслідки для діяльності МВС	Управлінське рішення
Фрагментованість реєстрів та інформаційних систем	Неможливість формувати повну картину подій, дублювання даних, помилки у звітності	Створення єдиної інформаційної архітектури та інтегрованих регістрів [9; 11; 12]
Відсутність єдиних стандартів обробки даних	Різна якість даних, збої у роботі алгоритмів, неузгодженість підрозділів	Розроблення стандартів структурування та валідації інформації [3; 8]

Надмірна залежність від паперових процедур	Повільні управлінські рішення, низька швидкість реагування	Перехід до цифрових workflow-процесів у всіх органах МВС [10; 35]
Нерозподіленість ролей щодо відповідальності за дані	Відсутність персональної підзвітності, складність аудиту	Запровадження посад Data Steward/Chief Data Officer у кожному департаменті [12; 40]

Міжнародна практика свідчить, що без визначення персональної відповідальності політика управління даними залишається декларативною [66; 71]. Для МВС доцільним є запровадження чіткої системи ролей, аналогічної до моделей держав-членів ЄС:

- Chief Data Officer МВС – стратегічний керівник, відповідальний за політику даних, інтеграцію з державними реєстрами, стандарти;
- Data Stewards у кожному департаменті – посадові особи, відповідальні за якість, актуальність, коректність введення даних;
- Data Protection Officer – окремо закріплена роль для контролю за дотриманням вимог Закону «Про захист персональних даних» [3].

Це відповідає європейським нормам Data Governance Act [58] та практикам прозорих адміністративних систем [57; 59].

У наукових роботах, присвячених інформаційній безпеці та адміністративному праву, наголошується, що формалізована відповідальність зменшує ризики зловживань, підвищує якість даних та дає змогу застосовувати алгоритми ШІ у правовий спосіб [37; 40; 70].

Навіть найкраща архітектура даних не працюватиме без управлінських спроможностей персоналу. Відомчі дослідження та офіційні аналітичні матеріали підкреслюють, що цифрова трансформація МВС має спиратися на підготовку кадрів не лише технічного, а й управлінського профілю [12; 27; 35].

Підготовка повинна охоплювати:

- базові навички роботи з даними (data literacy);
- роботу з інтегрованими інформаційними системами МВС;

- управління ризиками, пов’язаними з алгоритмічними рішеннями;
- вміння працювати з аналітичними панелями, прогнозними моделями;
- розуміння правових обмежень ШІ, зокрема щодо доступу до даних, персональних прав і процедур аудиту [3; 29; 39].

У матеріалах міжнародних організацій (OECD, Europol, NAPA) зазначено, що алгоритмічні інструменти в поліції дають результат лише тоді, коли керівники розуміють їх логіку, а не сприймають як «чорну скриньку» [51; 61; 66]. Освітня робота має стати частиною кадрової політики МВС.

Адміністративні рішення щодо управління даними не є допоміжним елементом, а формують фундамент для подальшого впровадження систем штучного інтелекту. Стандарти, відповідальні особи, інтеграційна архітектура та підготовка кадрів – це чотири ключові опори, без яких цифрова трансформація МВС та застосування інтелектуальних систем залишаться фрагментарними. Водночас численні дослідження адміністративної та кримінологічної науки вказують на потребу формування єдиного аналітичного контуру МВС, який включає інтегровані дані, розвинуті аналітичні центри, прогнозні моделі та сучасні цифрові панелі управління [21; 25; 38].

Аналітичні структури, які функціонують у складі МВС, сьогодні зосереджені переважно на оперативно-статистичному аналізі та моніторингу криміногенної ситуації. Проте сучасні підходи до державного управління вимагають виконання значно ширшого кола функцій. Успішні моделі поліційного менеджменту (ЄС, Канада, США) передбачають аналітичні підрозділи, які:

- здійснюють ризик-орієнтований аналіз;
- готують прогнозні моделі та сценарії розвитку подій;
- забезпечують data-driven управління;
- проводять оцінювання ефективності підрозділів;
- супроводжують управлінські рішення цифровими індикаторами.

В Україні частину таких підходів уже закладено в Стратегії розвитку цифрової держави [8], у планах цифровізації МВС [9; 35], а також у дослідженнях з використання ШІ в правоохоронній діяльності [21; 38; 48]. Однак для

повноцінної реалізації критично необхідно розширити функції відомчих аналітичних центрів.

Конкретні напрями модернізації включають:

- створення єдиного центрального аналітичного центру МВС, інтегрованого з регіональними підрозділами;
- розвиток постійного моніторингу загроз, зокрема цифрових, терористичних та соціальних;
- впровадження платформ для аналізу великих масивів даних;
- використання прогнозних моделей поведінки злочинності, що відповідає практикам Europol та ЄС [61; 59].

Такі зміни дозволять перейти від постфактум аналізу до превентивного, адаптивного та випереджального управління, що є основою сучасної публічної безпеки.

Однією з найбільших проблем МВС залишається фрагментованість інформаційних систем – відомчі реєстри, бази даних, регіональні підсистеми, відеоаналітика та інформаційні сервіси існують паралельно, що унеможливлює формування цілісної аналітичної картини. Це визнається у низці офіційних документів МВС [9; 11; 12] та публікацій незалежних експертів [18; 30; 42].

Модернізація передбачає:

- створення єдиного інтеграційного ядра (integration layer), через яке всі системи МВС отримують взаємну сумісність;
- уніфікацію протоколів обміну та стандартів даних;
- підключення систем відеоспостереження до аналітичної платформи МВС відповідно до законопроєкту № 11031 та позицій МВС [13; 22; 46];
- застосування централізованих панелей управління, що забезпечують керівництво актуальною інформацією в реальному часі.

Така інтеграція відповідає вимогам цифрової державної політики [8; 10] та практикам ЄС щодо оркестрації державних даних (Data Governance Act) [58].

Інтегрований управлінський контур дозволить:

- усунути дублювання інформації;

- пришвидшити реагування;
- забезпечити об’єктивність аналітичних висновків;
- гарантувати сумісність алгоритмів штучного інтелекту з даними МВС.

Використання інтелектуальних технологій у поліційній діяльності активно впроваджується у багатьох країнах світу, що відзначено у численних дослідженнях [48; 61; 67] та у звітах міжнародних організацій [52; 66; 71]. Для МВС такі інструменти можуть стати основою модернізації планування та прогнозування.

Ключові напрями:

- predictive policing – прогнозування криміногенної активності на основі історичних даних та просторових моделей (підтверджено в роботах Europol та Eviden) [61; 67];
- моделі прогнозування навантаження на підрозділи поліції;
- алгоритмічні системи розподілу ресурсів відповідно до ризиків;
- аналіз структурних чинників злочинності для прогнозного планування (за підтримкою моделей ШІ, що описані у джерелах [16; 25; 38]).

Алгоритми можуть застосовуватися й у внутрішньому управлінні: моделювання кадрових потреб, оцінювання ефективності підрозділів, аналіз інцидентів, виявлення аномалій у звітах тощо. Рекомендації Європейського парламенту щодо використання ШІ в кримінальній юстиції наголошують на необхідності впровадження таких систем у структурований спосіб [52].

Аналітичні платформи, які агрегують дані з різних підрозділів МВС, відіграють ключову роль у трансформації управлінських процесів (табл. 3.2.). Вітчизняні та міжнародні дослідження свідчать, що цифрові аналітичні середовища забезпечують керівників:

- індикаторами оперативної ситуації;
- прогностичними оцінками;
- ризик-профілями територій;
- автоматичними звітами;
- порівняльними показниками ефективності підрозділів.

Розбудова таких платформ узгоджується з державними політиками цифровізації [8; 10; 36] та з підходами, описаними у дослідженнях з публічного управління та цифрової етики [28; 40; 70].

Управлінські рішення, що спираються на дані, мають бути прозорими, перевірюваними та підзвітними, що відповідає принципам доброго врядування (good governance). Сучасні аналітичні системи також забезпечують аудит рішень – можливість відстежувати, на основі яких даних та моделей ухвалено управлінську дію, що особливо важливо у контексті захисту прав людини [3; 29; 57].

Таблиця 3.2.

Основні напрями модернізації інформаційно-аналітичної діяльності МВС

Напрям модернізації	Суть змін
Розширення функцій аналітичних центрів	Створення прогнозних моделей, оцінювання ефективності, централізація аналітики
Інтеграція інформаційних систем	Об’єднання реєстрів і платформ у єдиний управлінський контур
Інтелектуальні інструменти прогнозування	Predictive policing, розподіл ресурсів на основі ризиків, аналіз трендів
Аналітичні платформи для рішень	Автоматичні звіти, панелі управління, індикатори ситуації, аудит алгоритмів

Модернізація інформаційно-аналітичної діяльності МВС – це стратегічний напрям цифрової трансформації, який визначає якість управління, швидкість реагування та здатність відомства забезпечувати публічну безпеку на сучасному рівні. Розширення аналітичних центрів, інтеграція інформаційних систем, використання інтелектуальних інструментів і впровадження аналітичних платформ формують основу для переходу до data-driven управління, яке відповідає міжнародним стандартам ЄС та вимогам національних стратегічних документів.

Упровадження інтелектуальних технологій у діяльність МВС відкриває можливість переходу від традиційних адміністративних процедур до моделі

адаптивного, прогнозного та сервісно орієнтованого управління, що відповідає принципам цифрової держави та вимогам ефективного публічного врядування. ШІ стає не лише технологічним інструментом, а фундаментальним елементом трансформації управлінських процесів, сервісів та комунікації з громадянами. Державні політики України у сфері цифровізації – Стратегія розвитку цифрової держави [8], Концепція розвитку штучного інтелекту [6], План заходів на 2025–2026 роки [7], а також цифрові трансформації, закладені у програмах МВС [9; 12; 35], – визначають інновації як одну з ключових умов модернізації органів внутрішніх справ.

Функціональні можливості штучного інтелекту дозволяють формувати нові управлінські рішення, удосконалювати кадрову політику, підвищувати якість адміністративного контролю та забезпечувати більш прозору і доступну взаємодію між поліцією та громадянами. Дослідження у сфері кримінології, публічного управління та цифрової етики підтверджують, що саме управлінські та сервісні інновації є найбільш стійким напрямом застосування ШІ у державному секторі [21; 25; 28; 40; 48].

Алгоритмічні системи все частіше застосовуються як інструмент підтримки управлінських рішень у правоохоронних органах. Моделі ШІ дозволяють:

- аналізувати криміногенну ситуацію у динаміці;
- формувати сценарії розвитку подій;
- визначати території підвищеного ризику;
- оптимізувати планування патрулювання;
- розраховувати потреби у ресурсах.

Такі підходи застосовуються у практиках ЄС, США та Великої Британії, що підтверджено аналітичними матеріалами Europol, Європарламенту та дослідженнями українських науковців [52; 61; 67; 21; 48]. Інтелектуальні моделі формують основу data-driven governance, коли рішення приймаються не інтуїтивно, а через системний аналіз даних.

Для МВС України впровадження ШІ означає можливість створення нових сервісів:

- автоматизоване моделювання ризиків для територіальних громад (на основі досліджень щодо використання ШІ у публічному управлінні [19; 28]);
- цифрові панелі управління для керівного складу;
- динамічні звіти, які автоматично оновлюються;
- інтелектуальні черги у сервісних центрах МВС, що були визначені у реформах цифровізації [35].

Такі рішення підсилюють керованість системи МВС, забезпечують оперативність реагування та сприяють дотриманню принципів прозорості й підзвітності.

Кадрова політика – один із найважливіших елементів управління МВС, особливо в умовах воєнного стану та високих навантажень на персонал. Інтелектуальні системи можуть підвищити об’єктивність та ефективність кадрових процедур за такими напрямами:

- автоматизований аналіз компетенцій співробітників на основі їх професійних даних та результатів діяльності;
- виявлення прогалин у кваліфікації та формування персоналізованих навчальних траєкторій (відповідно до досліджень про цифрову трансформацію та роль даних у менеджменті [28; 70]);
- моделювання кадрових ризиків – визначення підрозділів, де існує ризик кадрового дефіциту;
- прогнозування кар’єрного зростання на основі алгоритмів оцінювання ефективності;
- автоматизовані системи розподілу службових навантажень.

Подібні підходи вже застосовуються у багатьох системах публічного управління країн ЄС, США і Канади, що підтверджено дослідженнями OECP і Stanford HAI [66; 71]. Для України особливо актуальним є питання формування кадрової стійкості поліції – у Стратегії розвитку органів системи МВС до 2030 року [12] прямо визначено, що кадровий потенціал є ключовим чинником ефективності. Застосування ШІ дозволить підвищити прозорість кадрових процесів та уникнути надмірної суб’єктивності при ухваленні рішень.

Адміністративний контроль у МВС – це система не лише перевірки дисципліни, але й моніторингу виконання управлінських рішень, оцінювання ефективності та виявлення потенційних ризиків. І тут ШІ може використовуватися у таких напрямах:

- автоматизований моніторинг виконання наказів і доручень, із відображенням статусів у режимі реального часу;
- виявлення аномальних дій, що можуть свідчити про помилки, зловживання або порушення;
- ризик-орієнтовані моделі, що формують профілі підрозділів за індикаторами ефективності, дисципліни та криміногенного навантаження;
- алгоритмічний аудит, рекомендований у звітах Європейської Комісії щодо етичного використання ШІ [57].

Системи автоматичного контролю можуть істотно зменшити навантаження на керівний склад, підвищити точність контролю та мінімізувати людський фактор. Інтелектуальний моніторинг відповідає принципам належного врядування та стандартам європейської публічної адміністрації.

Інтерактивні сервіси стають ключовим каналом комунікації поліції з громадянами, особливо в умовах війни. МВС уже активно розвиває цифрові послуги [35], але впровадження ШІ здатне суттєво розширити їх функціональність:

- інтелектуальні чат-боти, які надають консультації, приймають електронні звернення та видають довідкову інформацію;
- автоматизована фільтрація звернень громадян за типом проблеми, терміновістю та місцем;
- сервіси моніторингу безпеки територій, що базуються на даних відеоаналітики (відповідно до законопроєкту №11031 та матеріалів МВС [13; 22; 46]);
- інтелектуальні сервіси запобігання правопорушенням, які інформують громадян про небезпечні зони або ситуації.

Міжнародні дослідження доводять, що цифрова взаємодія значно підвищує рівень довіри до поліції та доступність адміністративних послуг [66; 71].

Для МВС це означає формування більш сервісної та орієнтованої на потреби громадян моделі діяльності (табл. 3.3.).

Таблиця 3.3.

Основні управлінські та сервісні інновації на основі ШІ

Напрям інновацій	Приклади рішень
Нові управлінські рішення	Прогнозні моделі, ризик-орієнтоване планування, інтелектуальні панелі управління
Кадровий менеджмент	Оцінювання компетенцій, прогноз кадрових ризиків, персоналізоване навчання
Адміністративний контроль	Автоматизований моніторинг, аудит алгоритмів, моделі ризиків
Взаємодія з громадянами	Чат-боти, автоматизовані звернення, відеоаналітика, смарт-сервіси

Застосування інновацій на основі ШІ дозволяє МВС перейти до моделі управління, що ґрунтується на даних, цифрових сервісах та інтелектуальних механізмах контролю. Такий підхід забезпечує оперативність, прозорість, прогнозність та високий рівень довіри громадян до поліції. Управлінські та сервісні інновації формують основу для наступних етапів цифрової трансформації МВС та повністю відповідають стратегічним документам державної політики, а також світовим стандартам етичного та відповідального використання алгоритмічних технологій.

3.3. Прогноз ефективності та ризиків впровадження інтелектуальних технологій у діяльність органів МВС

Упровадження систем штучного інтелекту в управлінські та сервісні процеси МВС створює можливість переходу від реактивної моделі публічного

управління до проактивної. Основні ефекти виникають за рахунок автоматизації рутинних операцій, підвищення якості даних, скорочення часу на прийняття рішень та посилення точності управлінських прогнозів. Це дозволяє не лише оптимізувати діяльність органів поліції, а й зміцнити спроможність держави забезпечувати громадську безпеку.

Одним із ключових результатів є зростання ефективності управлінських процесів. Алгоритмічні моделі прогнозування криміногенних ризиків, аналітичні панелі та автоматизована обробка інформації скорочують час підготовки управлінських рішень на всіх рівнях – від оперативного чергування до центрального апарату. У середньостроковій перспективі це забезпечує зменшення часу реагування на події, підвищення точності координації підрозділів та зростання результативності розслідувань. Перехід від ручного аналізу до автоматизованої обробки даних зменшує ймовірність помилок та забезпечує стабільність управлінських процедур.

Важливим є і покращення якості сервісних послуг, що надаються громадянам сервісними центрами МВС. Інтелектуальні системи здатні автоматично перевіряти документи, аналізувати черги, прогнозувати пікове навантаження, здійснювати попередню верифікацію даних та забезпечувати онлайн-взаємодію з користувачами. Це скорочує час очікування, підвищує доступність послуг та мінімізує контакт із бюрократичними процедурами. Для МВС це також означає раціоналізацію ресурсів, зниження операційних витрат та зменшення навантаження на персонал.

Суттєвим ефектом є зниження адміністративного навантаження на працівників. Автоматизовані інструменти можуть виконувати значну частину рутинної роботи – заповнення форм, підготовку звітів, класифікацію звернень, систематизацію відеоданих, обробку інформації з баз даних. Це дозволяє співробітникам зосередитися на складніших аналітичних, комунікаційних та правоохоронних функціях, що підвищує якість роботи та зменшує ризики помилок. Поступове цифрове перевантаження адміністративних процесів відкриває можливість скорочення дублювання функцій і оптимізації структури.

Нарешті, інформаційно-аналітичні інструменти на основі ШІ сприяють підвищенню рівня безпеки та контрольованості роботи поліції. Прогнозна аналітика дозволяє визначати райони ризику, прогнозувати навантаження на підрозділи, своєчасно виявляти аномальні події та оптимізувати патрулювання. Аналіз відеопотоків та сенсорних даних забезпечує додатковий рівень контролю за пересуванням підрозділів, фіксацією подій та дотриманням службових процедур. Це створює більш керовану та передбачувану модель функціонування системи МВС.

Орієнтовний розрахунок витрат та управлінських ефектів

В основі прогнозу застосовано метод управлінського оцінювання (expert-based projection). Розрахунок охоплює три компоненти:

1. Витрати на впровадження – закупівля програмних рішень, навчання персоналу, модернізація інфраструктури, адміністрування даних.

2. Прямі вимірювані ефекти – економія часу, зменшення навантаження, скорочення витрат.

3. Непрямі ефекти – покращення безпеки, прогнозування ризиків, зростання якості сервісів.

Базовий проєкт упровадження системи ШІ (аналітичні модулі, автоматизація сервісів, алгоритмічна обробка даних) оцінюється орієнтовно:

- Інфраструктурна модернізація – 20–30 млн грн (обладнання, сервери, адаптація систем).
- Закупівля ліцензій та ШІ-модулів – 10–15 млн грн.
- Інтеграція та безпековий аудит – 5–7 млн грн.
- Навчання та підготовка кадрів – 2–4 млн грн.
- Щорічне адміністрування та підтримка – 5–6 млн грн.

Сумарні стартові витрати: ≈ 40–55 млн грн.

Орієнтовний інституційний ефект через 12–18 місяців:

- Економія робочого часу – 15–25% на адміністративних процесах.
- Зменшення навантаження на персонал – 10–20%.
- Скорочення часу обробки звернень громадян – 30–50%.

- Підвищення точності аналітичних прогнозів – до 40%.
- Оптимізація патрулювання / реагування – 15–30%.
- Зниження дублювання функцій між підрозділами – до 12–15%.

На цій основі формується узагальнена таблиця 3.4.

Таблиця 3.4.

Узагальнена таблиця прогнозованих управлінських результатів впровадження ШІ в МВС України

Напрям ефекту	Поточний стан (умовно, %)*	Після впровадження ШІ (прогноз)	Очікуваний приріст / економія
Швидкість прийняття управлінських рішень	базовий рівень	на 20–30% швидше	Скорочення часу аналізу даних на 25%
Точність управлінських прогнозів	базовий рівень	+30–40%	Зростання релевантності аналітики
Ефективність реагування на події	умовна база	+15–30%	Оптимізація координації патрулів
Якість адміністративних послуг	середній рівень	+30–50%	Скорочення черг, автоматизація перевірок
Навантаження на персонал	високе	–10–20%	Заміна рутинної роботи автоматизованими модулями
Операційні витрати сервісних центрів	базовий рівень	–8–12%	Менше дублювання функцій, оптимізація процесів
Час обробки звернень	≈100% нинішнього	–30–50%	Менше бюрократії, більше автоматизації
Контрольованість службових процесів	середня	+20–35%	Кращий нагляд, аудит, фіксація подій
Безпековий рівень (управлінський контроль)	поточний рівень	+15–25%	Прогнозування “гарячих зон”, ризик-аналіз

Наведені показники відображають не технічні параметри, а управлінські ефекти, які виникають після інтеграції ШІ у процеси МВС. Збільшення швидкості прийняття рішень і підвищення точності прогнозів є результатом автоматизації обробки даних та аналітичного моделювання. Зниження

навантаження на персонал зумовлене передачею рутинних функцій інтелектуальним системам. Прогнозований приріст ефективності сервісних послуг ґрунтується на очікуваному скороченні черг, автоматизованій перевірці документів та онлайн-обробці звернень. Підвищення контрольованості діяльності поліції забезпечується за рахунок інструментів моніторингу, аналізу відеоданих та ризик-моделей. Сукупно ці ефекти формують основу для підвищення спроможності МВС виконувати свої управлінські, сервісні та безпекові функції.

Також слід зазначити що впровадження інтелектуальних технологій у діяльність МВС України супроводжується низкою ризиків і бар'єрів, які можуть сповільнити або викривити трансформацію. Проблеми виникають на перетині адміністративних процедур, етичних стандартів публічного управління, технічної сумісності систем та захисту прав громадян. Для МВС – як центрального органу виконавчої влади у сфері безпеки – важливо оцінити не лише потенційні вигоди ШІ, але й ті обмеження, що впливають на управлінські рішення та легітимність роботи поліції.

Одним із ключових ризиків є адміністративна забюрократизованість процесів, що ускладнює масштабування інтелектуальних технологій. Діючі процедури затвердження змін, розподілу повноважень, погодження інформаційних потоків та доступів до реєстрів часто є повільними й фрагментованими. Це створює додаткову складність у впровадженні нових цифрових інструментів, особливо коли вони вимагають узгоджених дій кількох підрозділів. Якщо внутрішні правила та регламенти не будуть адаптовані, існує ризик, що впровадження ШІ залишиться локальним, а не системним.

Другим фактором виступає ризик алгоритмічної похибки, яка може спричиняти неправильні управлінські рішення. Алгоритми, що навчаються на історичних даних, можуть відтворювати системні викривлення або формувати упередження щодо певних груп населення, територій чи типів подій. Це має особливе значення для МВС, адже неправильна класифікація, помилкове прогнозування або некоректна оцінка ризиків здатні вплинути на оперативне

реагування, застосування сил чи планування профілактичних заходів. Технологічні обмеження стають управлінським ризиком, якщо немає належної системи контролю та періодичної перевірки алгоритмів.

До етичних викликів належить і загроза надмірного втручання в приватне життя громадян, особливо у разі застосування систем відеоаналітики, автоматичного розпізнавання облич та масового збору даних. У сфері публічного управління це ставить питання легітимності, відповідності принципам пропорційності та дотримання прав людини. Надмірна концентрація інформації або нечіткі правила використання ШІ можуть зменшити довіру до МВС, що негативно позначається на ефективності правоохоронної діяльності.

Суттєвим бар'єром є недостатня підготовка управлінського та технічного персоналу. Впровадження інтелектуальних систем потребує навичок роботи з великими масивами даних, розуміння логіки алгоритмів, принципів оцінки ризиків та знань цифрової етики. У персоналу МВС здебільшого немає системної ІТ-освіти, а програми навчання державних службовців не охоплюють сучасні інструменти аналітичної обробки даних. Це створює ситуацію, коли технології з'являються швидше, ніж можливості їх компетентного застосування.

Додатковим ризиком є неоднорідність та фрагментованість даних, на яких працюють системи ШІ. Багато інформаційних ресурсів МВС створювалися у різні роки, без єдиної архітектури, різними розробниками. Відсутність структурної узгодженості призводить до помилок у поєднанні даних, ускладнює їх перенесення в аналітичні платформи та зменшує точність моделей прогнозування. Технічні проблеми трансформуються в управлінський бар'єр, оскільки обмежують можливість комплексної оцінки ситуації та ухвалення рішень.

Окрему групу ризиків складають кібербезпекові загрози. Інтелектуальні системи збільшують кількість точок доступу до даних і потребують розширеної інфраструктури. Будь-які порушення безпеки можуть зачепити критичні державні реєстри, інформацію про оперативну діяльність чи персональні дані

громадян. Це становить не лише оперативний ризик, а й загрозу для стратегічної стабільності сектору внутрішніх справ.

Не менш важливою є загроза надмірної залежності від технологій, коли автоматизовані системи починають витісняти експертну оцінку та професійне судження. У діяльності поліції критично важливо забезпечити баланс між алгоритмічною обробкою інформації та людським контролем. Втрата цього балансу може призвести до помилок, які неможливо виправити лише за рахунок технічних засобів.

Проблемою залишається і низький рівень суспільної довіри до автоматизованих державних рішень. Навіть за високого рівня технічної точності системи ШІ можуть бути сприйняті як непрозорі або загрозливі. Для МВС це створює репутаційний ризик, адже будь-яка помилка алгоритму викликає суспільний резонанс, особливо у сферах відеоспостереження чи профайлінгу.

З огляду на ці ризики запровадження ШІ потребує комплексного управлінського підходу – оновлення регламентів, зміцнення кіберзахисту, підвищення компетентності державних службовців, прозорих процедур аудиту алгоритмів, інституційного контролю та комунікації з суспільством. Лише поєднання цих елементів дозволить мінімізувати бар’єри та забезпечити відповідність технологічних рішень принципам публічного управління та вимогам безпеки. Тому ухвалення рішень щодо впровадження будь-якої інтелектуальної системи має базуватися на стандартизованій моделі оцінювання ризиків, яка враховує специфіку діяльності органів внутрішніх справ та принципи належного врядування.

Центральне місце в моделі займає аналіз операційних ризиків, що охоплюють помилки алгоритмів, некоректну обробку даних, збої обладнання та порушення логіки службових процесів. Оцінка має включати визначення ймовірності відмови системи, масштаб потенційних наслідків для оперативної діяльності та можливість ручної компенсації. Критично важливо оцінювати, чи спроможний відповідний підрозділ МВС виконувати функції без автоматизованої

підтримки у разі збою, та чи не створює технологічне рішення залежності, яка знижує управлінську стійкість.

Другою складовою є аналіз правових ризиків, пов’язаних із обробкою персональних даних, відеоаналітикою, автоматизованими рішеннями та використанням прогнозних інструментів у правоохоронній діяльності. Модель оцінки передбачає перевірку відповідності алгоритмів чинному законодавству, наявність чітко визначеної правової підстави для кожного виду обробки даних, а також механізмів зовнішнього та внутрішнього контролю. Рішення щодо впровадження ШІ повинно прийматися лише після забезпечення юридичної визначеності, прозорості використання технологій та гарантування захисту прав громадян.

Третім елементом моделі виступає оцінювання етичних ризиків, які охоплюють загрозу дискримінації, непрозорість алгоритмів та потенційну шкоду від надмірного автоматизованого контролю. Інтелектуальні системи, особливо ті, що використовують машинне навчання, можуть формувати упередження щодо певних територій, соціальних груп або поведінкових моделей. Тому модель вимагає здійснення попереднього аудиту алгоритмічної справедливості, аналізу логіки прийняття рішень та визначення рівня пояснюваності результатів. Етичний ризик вважається критичним, якщо система не дозволяє встановити, чому саме алгоритм сформував конкретний прогноз чи рекомендацію.

Четвертий компонент включає оцінку кібербезпекових ризиків, які визначають стійкість системи до зовнішніх та внутрішніх атак. Модель передбачає перевірку наявності механізмів криптографічного захисту, сегментації доступів, журналювання операцій, резервного копіювання та незалежного тестування на проникнення. Імплементація ШІ без достатнього кіберзахисту створює загрозу витоку персональних даних, компрометації оперативної інформації та втручання у критичні державні процеси.

П’ятим блоком є оцінювання організаційних ризиків, зокрема кадрової готовності, здатності керівництва приймати рішення на основі даних, достатності ресурсів та зрілості внутрішніх регламентів. Система вважається

готовою до впровадження лише за умови наявності відповідальних структурних підрозділів, визначених ролей, узгоджених процедур і сформованої культури управління даними. Якщо персонал не спроможний працювати з інтелектуальними інструментами, а існуючі управлінські процеси залишаються фрагментованими, впровадження породжує додаткові ризики.

Шостою складовою моделі є оцінка соціальних ризиків, пов'язаних із сприйняттям суспільством інтелектуальних технологій у роботі поліції. Високий рівень недовіри може зменшувати ефективність роботи МВС, створювати конфлікти та спонукати до політичного спротиву. Тому модель вимагає прогнозування реакції громадськості, визначення рівня прозорості системи та оцінки ризиків суспільної напруги.

Остаточне рішення щодо впровадження системи ШІ ухвалюється на основі критеріїв управлінської достатності, які включають:

1. Пропорційність – наскільки користь від впровадження перевищує можливі ризики.
2. Необхідність – чи є інші, менш ризиковані способи досягнення того самого результату.
3. Ефективність – здатність системи забезпечувати сталі покращення управлінських або сервісних функцій.
4. Керованість – можливість контролю, аудиту та коригування алгоритмів у процесі експлуатації.
5. Безпечність – наявність механізмів мінімізації технологічних та кіберризиків.
6. Пояснюваність – зрозумілість логіки прийняття рішень та можливість її обґрунтування.
7. Стійкість – здатність системи працювати в умовах відсутності частини даних, збоїв або непередбачуваних ситуацій.

Модель також має включати механізм багаторівневого погодження – первинна оцінка ризиків фахівцями, експертна перевірка відповідальними департаментами, управлінське рішення керівництва МВС та, при необхідності,

зовнішній аудит. Такий підхід дозволяє мінімізувати як технологічні, так і адміністративні ризики, забезпечуючи прозорість і відповідальність у застосуванні ШІ.

Загалом модель оцінки ризиків дозволяє забезпечити контрольованість процесу цифрової трансформації, уникнути надмірної залежності від технологій і гарантувати, що впровадження інтелектуальних систем відповідає інтересам безпеки, етичним стандартам і принципам публічного управління. Це створює основу для обґрунтованих рішень і формує стратегічну стійкість МВС у довгостроковій перспективі.

Висновки до розділу 3

Проведений аналіз показує, що цифрова трансформація правоохоронної системи неможлива без чіткої управлінської моделі інтеграції інтелектуальних технологій, здатної забезпечити баланс між ефективністю, безпекою та правовою визначеністю. ШІ у структурі МВС виступає не лише технологічним засобом, а інструментом підсилення управлінської спроможності, що змінює логіку управління даними, планування, координації та організації сервісних послуг.

Зазначено, що концептуальна модель застосування інтелектуальних систем у МВС повинна ґрунтуватися на принципах належного врядування, зокрема прозорості, підзвітності, відповідальності та ефективності. Визначені напрями використання ШІ у превенції правопорушень, оптимізації реагування, аналітичному забезпеченні рішень та розвитку цифрових сервісів демонструють потенціал для істотного підвищення керованості та оперативності правоохоронної діяльності. Сформовані пропозиції щодо удосконалення адміністративних процесів підтверджують необхідність створення цілісної системи управління даними, модернізації аналітичних центрів та розширення сервісних можливостей поліції.

Запропоновані заходи щодо оптимізації інформаційно-аналітичної діяльності МВС акцентують на формуванні єдиного управлінського контуру, що об’єднує інформаційні ресурси, алгоритмічні модулі та управлінські

інструменти. Така інтеграція здатна забезпечити скорочення бюрократії, підвищення точності рішень, економію ресурсів та стабільність процесів реагування. Окремо підкреслено потребу у розвитку кадрової компетентності та інституційної спроможності, оскільки ефективність ШІ прямо залежить від готовності управлінського персоналу працювати з аналітичними платформами і приймати рішення на основі даних.

Прогнозні оцінки демонструють, що впровадження інтелектуальних систем може забезпечити як безпосередні управлінські ефекти (скорочення часу реагування, підвищення координації, зменшення помилок), так і економічні вигоди у вигляді оптимізації навантаження на персонал та раціоналізації ресурсів. Разом із цим наголошено на необхідності чіткої моделі оцінки ризиків, яка охоплює юридичні, етичні, операційні, безпекові та організаційні аспекти. Така модель створює основу для виважених рішень і мінімізує загрози, пов’язані з алгоритмічними помилками, технологічними залежностями або порушеннями прав громадян.

ВИСНОВКИ

Проведене дослідження дало можливість комплексно оцінити можливості, умови та перспективи впровадження систем штучного інтелекту в публічне адміністрування Міністерства внутрішніх справ України. У роботі проаналізовано теоретичні засади функціонування інтелектуальних систем, міжнародні стандарти та практики, сучасний стан цифрової інфраструктури МВС, наявні управлінські й технологічні бар'єри, а також окреслено стратегічні механізми модернізації діяльності органів внутрішніх справ.

У першому розділі дослідження розкрито концептуальні основи застосування штучного інтелекту у сфері публічного управління та правопорядку. Визначено, що впровадження ШІ має ґрунтуватися на принципах належного врядування, правової визначеності, прозорості, підзвітності та орієнтації на потреби громадян. Міжнародний досвід, зокрема Європейського Союзу, США та окремих країн Азії, доводить, що застосування інтелектуальних технологій у роботі поліції забезпечує істотне підвищення превентивної та аналітичної спроможності, проте одночасно вимагає суворих стандартів контролю, етичних запобіжників та законодавчої регламентації. Системи прогнозування правопорушень, автоматизованої аналітики, розпізнавання об'єктів, алгоритмічної підтримки рішень є ефективними лише в умовах інституційної зрілості, наявності якісних даних та чітко визначених меж їх використання.

Другий розділ містить аналіз чинного нормативно-правового середовища МВС України, оцінку існуючих інформаційних систем і цифрових інструментів, а також визначення ключових проблем, які стримують інтеграцію ШІ. Встановлено, що за останні роки сформовано нормативну архітектуру цифрової трансформації, проте вона потребує розширення з урахуванням нових викликів, таких як алгоритмічна прозорість, відповідальність за прийняття автоматизованих рішень, захист персональних даних у великих масивах, стійкість до кіберзагроз і стандарти взаємодії систем. Оцінка реальних цифрових

практик МВС показала наявність розгалуженої інфраструктури відеоспостереження, комунікаційних платформ, реєстрів і аналітичних модулів, однак інтеграція між ними залишається неповною, а інтелектуальні технології використовуються фрагментарно. Суттєвими бар'єрами виступають відсутність єдиної політики управління даними, обмежена кадрова компетентність, нерівномірність технічного забезпечення та складність організаційних процесів.

У третьому розділі запропоновано концептуальну модель впровадження штучного інтелекту у діяльність МВС, орієнтовану на управлінську модернізацію та розвиток нових сервісних можливостей. Модель передбачає створення цілісної системи управління даними, розбудову аналітичних центрів, поступову інтеграцію інтелектуальних модулів у превентивну, оперативну та адміністративну діяльність поліції. Розроблені пропозиції включають оптимізацію бізнес-процесів, підвищення взаємодії між підрозділами, створення інтелектуальних платформ підтримки рішень, модернізацію кадрової політики та розширення сервісів для населення. Сформовано прогноз очікуваних результатів, який охоплює підвищення ефективності реагування, скорочення часу обробки інформації, покращення точності управлінських рішень, зменшення бюрократії, зростання рівня громадської безпеки та стабільність управління в умовах воєнного та післявоєнного періоду. Окремо вказано на групи ризиків – технологічні, організаційні, правові, етичні та безпекові – та запропоновано механізми їх мінімізації.

Сукупність отриманих результатів дає підстави стверджувати, що впровадження систем штучного інтелекту в діяльність МВС України є стратегічно необхідним елементом побудови сучасної, стійкої та ефективної структури внутрішньої безпеки. Воно здатне забезпечити якісно новий рівень аналітичної спроможності, управлінської результативності, сервісної орієнтації та оперативного реагування. Разом із тим успішність трансформації залежить від поєднання декількох факторів: наявності чіткої політики управління даними, вдосконалення нормативної бази, розвитку технічної інфраструктури, підготовки персоналу та забезпечення прозорості алгоритмічних процесів.

Таким чином, дослідження підтверджує, що інтеграція ШІ у МВС України є не лише технологічним проєктом, а комплексним управлінським завданням, яке потребує стабільного інституційного розвитку та стратегічного бачення. Реалізація розроблених у роботі пропозицій дозволить сформувати сучасну модель правоохоронної діяльності, здатну ефективно функціонувати в умовах динамічних загроз та забезпечувати високий рівень довіри громадян до державних інституцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19

2. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12

3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17

4. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19

5. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки: Указ президента України від 11.05.2023 No273/2023. URL: https://www.president.gov.ua/documents/2732023-46733

6. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження КМУ від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р

7. Про затвердження Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки: Розпорядження КМУ від 09.05.2025 № 457-р. України на 2025–2026 рр.]. https://zakon.rada.gov.ua/laws/show/457-2025-р

8. Про схвалення Стратегії розвитку цифрової держави до 2030 року : Розпорядження КМУ від 15.08.2023 № 679-р. URL: https://zakon.rada.gov.ua/laws/show/679-2023-р

9. Про затвердження Концепції програми інформатизації системи МВС України на 2021–2023 роки: Наказ МВС України № 301 від 22.04.2021. URL: https://mvs.gov.ua/uk/press-center/news/rozvitok-cifrovoyi-infrastrukturi-ta-stvorennya-cifrovix-servisiv-dlya-gromadyan-prioritet-programi-informatizaciyi-sistemi-mvs

10. Деякі питання цифрової трансформації: розпорядження Кабінету Міністрів України № 735-р від 02.08.2024. URL: https://zakon.rada.gov.ua/go/735-2024-%D1%80

11. Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу Міністерства внутрішніх справ України: Наказ МВС України № 596 від 04.07.2016. URL: https://zakononline.ua/documents/show/361178___361243

12. Про затвердження Стратегії розвитку органів системи Міністерства внутрішніх справ України до 2030 року: розпорядження Кабінету Міністрів України № 1108-р від 16.10.2023. URL: https://zakon.rada.gov.ua/go/1108-2023-%D1%80

13. Проект Закону про єдину систему відеомоніторингу стану публічної безпеки: № 11031 від 20.02.2024. Верховна Рада України. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/44543

14. Авдєєва Т. Законопроєкт про відеомоніторинг: захист публічної безпеки чи ліцензія на масове стеження? [Електронний ресурс] // Лабораторія цифрової безпеки. – 2024. – 9 берез. – URL: https://dslua.org/publications/zakonoproiekt-pro-videomonitorynh-zakhyst-publichnoi-bezpeky-chy-litsenziia-na-masove-stezhennia/

15. Бацман Ю. В., Толкуща К. Р. Використання штучного інтелекту в публічному адмініструванні. Юридичний науковий електронний журнал. 2024. № 4. С. 338–341.

16. Бедь Ю., Чийпеш Р., Шатан В. Останні досягнення штучного інтелекту: огляд і аналітика (2023–2025). 2025. URL: https://kau.com.ua/wp-content/uploads/2025/09/Bed-Iu.-Chyjpesh-R.-Shatan-V.-Ohliad-dosiahnen-ShI-2023-2025-rr.-25.09.2025-1.pdf

17. Бойко В. В. Правове регулювання штучного інтелекту: міжнародний досвід. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Публічне управління та адміністрування. 2024. Т. 35(74), № 2. С. 23–29.

18. Вишневський І. Чому єдина система відеомоніторингу лякає суспільство? Розбираємось, як це може працювати, скільки коштує і чи не перетвориться Україна на Китай [Електронний ресурс] // dev.ua. – 2024. – 18 верес. – URL: https://dev.ua/news/chomu-iedyna-systema-videomonitorynhu-liakaie-suspilstvo-rozbyraiemos-iak-tse-mozhe-pratsiuvaty-skilky-koshtuie-i-chy-ne-peretvorytsia-ukraina-na-kytai

19. Горбата Л. П. Використання технологій штучного інтелекту в управлінні розвитком територіальних громад в Україні. URL: http://customs-admin.umsf.in.ua/archive/2024/4/7.pdf (дата звернення: 18.11.2025).

20. Горобець Н. С., Науменко С. М. Штучний інтелект в юридичній практиці України: нові можливості та виклики. Юридичний науковий електронний журнал. 2024. № 11. С. 493–496.

21. Гудзь Т. І., Синжерян А. А. Інтеграція технології штучного інтелекту у діяльність Національної поліції України: перспективи та виклики. Українська поліцеїстика: теорія, законодавство, практика. 2024. № 3. С. 53–59.

22. Департамент комунікації МВС України. В єдиній системі відеомоніторингу стану публічної безпеки застосовані всі необхідні засоби захисту, – Леонід Тимченко [Електронний ресурс] // Міністерство внутрішніх справ України: офіційний вебсайт. – 2024. – 17 січ. – URL: https://mvs.gov.ua/news/v-jedinii-sistemi-videomonitoringu-stanu-publicnoyi-bezpeki-zastosovani-vsi-neobxidni-zasobi-zaxistu-leonid-timcenko

23. Драп’ятий Б., Тимченко Л. Система відеомоніторингу: як правильно законодавчо врегулювати, щоб посилити внутрішню безпеку. Дзеркало тижня. URL: https://zn.ua/ukr/UKRAINE/sistema-videomonitorinhu-jak-pravilno-zakonodavcho-vrehuljuvati-shchob-posiliti-vnutrishnju-bezpeku.html (дата звернення: 18.11.2025).

24. Забокрицький І. І. Акт про штучний інтелект (artifical inteligence act, ai act) як основа правового регулювання штучного інтелекту в ЄС: огляд основних положень. Редакційна колегія. 2025. С. 282.

URL: https://app-journal.in.ua/wp-content/uploads/2025/06/APP_03_2025-part-3.pdf#page=282

25. Зачек О. І., Дмитрик Ю. І., Сеник В. В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2023. № 3. С. 148–156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19

26. Зеленчук В. Неочевидні загрози єдиної системи відеомоніторингу [Електронний ресурс] // Інститут масової інформації. – 2024. – 11 берез. – URL: https://imi.org.ua/monitorings/neochevydni-zagrozy-yedynoyi-systemy-videomonitoryngu-i59814

27. Інформація з офіційного сапйту МВС України / Міністерство внутрішніх справ України. URL: https://mvs.gov.ua

28. Карпенко О. В., Карпенко Ю. В. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти. Державне управління: удосконалення та розвиток. 2021. № 10.

29. Клян А. Правове регулювання штучного інтелекту в Україні та світі. Юридична фірма GOLAW. URL: https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/ (дата звернення: 18.11.2025).

30. Копитко В. Життя під камерами. Чи порушить відеомоніторинг право українців на приватність [Електронний ресурс] // РБК-Україна. – 2024. – 15 верес. – URL: https://www.rbc.ua/rus/news/zhittya-pid-kamerami-chi-porushit-videomonitoring-1726325096.html

31. Лисогор І. У МВС прокоментували законопроєкт про відеонагляд у публічних місцях [Електронний ресурс] // LB.ua. – 2024. – 22 лют. – URL: https://lb.ua/society/2024/02/22/599766_mvs_prokomentuvali_zakonoproiekt.html

32. Літкевич В. Штучний інтелект і суспільство – огляд німецької наукової літератури. Scientific Review. 2024. Т. 6(98). С. 19–47.

33. Лунгол О. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. Кібербезпека: освіта, наука, техніка. 2024. Т. 1(25). С. 379–389.

34. Марутян Р. Р. Інформаційні технології інтелектуального управління у публічно-управлінській практиці: зарубіжний та вітчизняний досвід. Вісник Національного університету цивільного захисту України. Державне управління. 2018. Вип. 2 (9). С. 146–153. URL: http://nbuv.gov.ua/UJRN/VNUCZUDU_2018_2_22 (дата звернення: 18.11.2025).

35. Міністерство внутрішніх справ України. Цифровізація послуг та скорочення бюрократії: Ігор Клименко розповів про реформу сервісних центрів МВС [Електронний ресурс] // Урядовий портал. Кабінет Міністрів України. – 2024. – 4 січ. – URL: https://www.kmu.gov.ua/news/tsyfrovizatsiia-posluh-ta-skorochennia-biurokratii-ihor-klymenko-rozpoviv-pro-reformu-servisnykh-tsentriv-mvs

36. Міністерство цифрової трансформації України. Офіційний сайт. URL: https://thedigital.gov.ua (дата звернення: 18.11.2025).

37. Нагорняк М. М. Інформаційна безпека у системі публічного управління: виклики та перспективи. Дніпровський науковий часопис публічного управління, психології, права. 2024. № 1. С. 64–68.

38. Негребецький В. В. Використання систем штучного інтелекту у боротьбі зі злочинністю: огляд та перспективи. Українська поліцеїстика: теорія, законодавство, практика. 2024. № 1. С. 66–70.

39. Олійник О. Правове регулювання штучного інтелекту в Україні: виклики та перспективи. Social Development: Economic and Legal Issues. 2025. № 6.
URL: https://www.eu-scientists.com/index.php/sdel/article/view/268

40. Орлов О. Цифрова етика та алгоритмічна прозорість: виклики та методи забезпечення справедливості автоматизованих рішень у державному управлінні. Аспекти публічного управління. 2025. Т. 13(2). С. 51–60.

41. Письменний О. Забезпечення кібербезпеки в цифровому просторі в умовах воєнного стану // Штучний інтелект у правовій практиці: межі та можливості: збірник тез круглого столу (14 березня 2025 року) / упоряд. О. О. Барабаш. Львів: ЛьвДУВС, 2025. С. 171–175.

42. Поліковська Ю. Безпека vs приватність. Чи потрібен Україні повсюдний відеонагляд [Електронний ресурс] // Детектор медіа. – 2024. – 5 берез. – URL: https://ms.detector.media/trendi/post/34349/2024-03-05-bezpeka-vs-pryvatnist-chy-potriben-ukraini-povsyudnyy-videonaglyad/

43. Радутний О. Е. Право та окремі аспекти світу атомів і бітів (робототехніка, штучний інтелект, цифрова людина). Питання боротьби зі злочинністю. 2021. № 41. С. 13–28. DOI: 10.31359/2079-6242-2021-41-13.7.

44. Рєпіна Ю. С. Світові стандарти та практики використання штучного інтелекту у судочинстві. Питання боротьби зі злочинністю. 2021. № 41. С. 29–38. DOI: 10.31359/2079-6242-2021-41-29.8.

45. Укрінформ. Майже 40 тисяч камер: у поліції розповіли, як працює зараз система відеоспостереження [Електронний ресурс] // Укрінформ. – 2024. – 18 берез. – URL: https://www.ukrinform.ua/rubric-society/3841458-majze-40-tisac-kamer-u-policii-rozpovili-ak-pracue-edina-sistema-videosposterezenna.html

46. Укрінформ. Тотального стеження не буде: у МВС роз'яснили, що фіксуватиме система відеокамер у публічних місцях [Електронний ресурс] // Укрінформ. – 2024. – 18 берез. – URL: https://www.ukrinform.ua/rubric-society/3841502-totalnogo-stezenna-ne-bude-u-mvs-rozasnili-so-fiksuvatime-sistema-videokamer-u-publicnih-miscah.html

47. Цяпа С. М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах. Інформація і право. 2021. № 2(37). С. 51–59.

48. Шевчук Т. А., Свистун Я. В. Використання штучного інтелекту у протидії злочинності. Вісник кримінологічної асоціації України. 2021. № 2(25). С. 128–134.

49. Шепітько В. Ю., Коновалова В. О., Шевчук В. М. та ін. Науково-технічне забезпечення слідчої діяльності в умовах змагального кримінального процесу. Питання боротьби зі злочинністю. 2021. № 42. С. 92–102.

50. Alqahtani S., et al. The Impact of Artificial Intelligence on Emergency Medicine: A Review of Recent Advances. arXiv:2503.14546, 2025. URL: https://arxiv.org/abs/2503.14546

51. Artificial intelligence and its impact on public administration. National Academy of Public Administration. Standing Panel on Technology Leadership's Working Group on Artificial Intelligence and Robotics and the Impact on Public Administration. URL: https://napawash.org/uploads/academy_studies/9781733887106.pdf (дата звернення: 18.11.2025).

52. Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters / Adopted at the plenary meeting of the European Parliament (Strasbourg, 6 October 2021). URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

53. Brohan A., et al. RT-2: Vision-Language-Action Models Transfer Web Knowledge to Robotic Control. Google DeepMind, 2023. URL: https://robotics-transformer2.github.io

54. Ceder G. Autonomous discovery of materials using AI. University of California, Berkeley, 2024. URL: https://en.wikipedia.org/wiki/Gerbrand_Ceder

55. Council of Europe and Artificial Intelligence. URL: https://www.coe.int/en/web/artificial-intelligence

56. Digital Transformation and Public Services [Електронний ресурс]. URL: https://library.oapen.org/bitstream/handle/20.500.12657/24567/9780367333430_text17oktober.pdf?sequence=1 (дата звернення: 18.11.2025).

57. European Commission. Ethics Guidelines for Trustworthy AI. High-Level Expert Group on AI, 2019. URL: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-en

58. European Commission. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&qid=1763478415973

59. European Commission. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689&qid=1763478415973

60. European Commission. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R0038&qid=1763478415973

61. Europol. AI and policing. URL: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing

62. Google DeepMind. Gemini models overview. 2023. URL: https://deepmind.google/technologies/gemini

63. Li J., et al. Toward Embodied AGI: A Review of Embodied AI and the Road Ahead. arXiv:2505.14235, 2025. URL: https://arxiv.org/abs/2505.14235

64. Mankowitz D. J., Michi A., Zhernov A., et al. Faster sorting algorithms discovered using deep reinforcement learning. Nature, 2023. URL: https://www.nature.com/articles/s41586-023-06004-9

65. MIT Sloan Review. Five Trends in AI and Data Science for 2025. 2025. URL: https://sloanreview.mit.edu/article/five-trends-in-ai-and-data-science-for-2025

66. OECD. Artificial Intelligence in the Public Sector. 2021. URL: https://oecd-opsi.org/work-areas/ai/

67. Police use of AI: A force for good or a public threat? Eviden. 18.09.2023. URL: https://eviden.com/insights/blogs/police-use-of-ai-a-force-for-good-or-a-public-threat/ (дата звернення: 20.09.2024).

68. Pysmenna O., Lavrentii Z. O. Штучний інтелект в юриспруденції: перспективи і проблеми. Modern Engineering and Innovative Technologies. 2024. Вип. 31-04. С. 69–73.

69. Rudolph J., et al. Practical and Ethical Challenges of Large Language Models in Education: A Systematic Scoping Review. arXiv:2303.13379, 2023.URL: https://arxiv.org/abs/2303.13379

70. Rybchenko S. O. Administrative law of Ukraine: Modern challenges and prospects of development. Social Law. 2024. № 1. С. 97–104.

71. Stanford HAI. AI Index Report 2025. Stanford University, 2025. URL: https://hai.stanford.edu/ai-index/2025-ai-index-report

72. Ukrainian Institute for the Future. Битва підходів: людський інтелект проти штучного у прогнозуванні майбутнього до 2028 року. URL: https://uifuture.org/publications/lyudskyy-intelekt-proty-shtuchnogo-u-prognozuvanni-maybutnogo-do-2028-roku/ (дата звернення: 18.11.2025).

73. UNODC. Digital Technology Reshaping Crime Prevention and Justice – The Role of Youth Leadership. URL: https://www.unodc.org/unodc/en/justice-and-prison-reform/unodc_-digital-technology-reshaping-crime-prevention-and-justice--the-role-of-youth-leadership.html