УДК 347.97:351.74
DOI https://doi.org/10.32782/2307-1745.2025.76.17

Малетова О. С.,
доктор юридичних наук, доцент,
завідувач кафедри кримінально-правових
дисциплін та судочинства
Сумського державного університету

МОДЕРНІЗАЦІЯ ПРАВООХОРОННИХ СИСТЕМ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ ПЕРСПЕКТИВИ[1]

Анотація. У статті досліджено сучасні тенденції реформування організаційних структур правоохоронних органів провідних країн світу з акцентом на їхню роль у забезпеченні національної безпеки через інтеграцію передових технологій і посилення міжвідомчої координації. Актуальність дослідження обумовлена появою нових загроз національній безпеці, таких як кіберзлочинність, міжнародний тероризм і транскордонна організована злочинність, які вимагають від правоохоронних органів переходу від традиційних централізованих ієрархічних структур до більш гнучких та адаптивних моделей управління. Особливої актуальності тема набуває для України в умовах воєнного стану, де ефективність правоохоронної системи безпосередньо впливає на національну стійкість.

Автор проводить комплексний аналіз досвіду реформування правоохоронних систем у Сполучених Штатів Америки, європейських країнах (Франція, Великобританія, Німеччина, Естонія, Нідерланди) та країнах Азійсько-Тихоокеанського регіону (Японія, Сінгапур, Австралія). На прикладі США продемонстровано трансформацію правоохоронної системи після подій 11 вересня 2001 року, що включала створення нових координаційних структур, розширення повноважень ФБР у сфері національної безпеки та формування об'єднаних оперативних груп з боротьби з тероризмом. Досвід Франції ілюструє важливість чіткого організаційно-правового механізму імплементації реформ через встановлення процедурних рамок для швидкого впровадження законодавчих змін.

Особливу увагу приділено розвитку спеціалізованих підрозділів кіберполіції як відповіді на зростання кіберзагроз. Детально розглянуто досвід Естонії, яка після масштабних кібератак 2007 року створила ефективну систему кіберзахисту з міжнародною координацією через NATO; Японії, що у 2022–2025 роках провела комплексну реформу кіберполіції з прийняттям історичного Закону про активну кіберзахист; та Німеччини, де функціонує розгалужена система протидії кіберзлочинності, хоча розкриваність таких злочинів залишається низькою (32%).

Значна частина дослідження присвячена цифровій трансформації правоохоронних органів. Проаналізовано впровадження технологій штучного інтелекту, аналітики великих даних, біометричних систем та прогнозної аналітики в Сінгапурі (ініціатива Smart Nation, система PolCam 2.0), Австралії (National Criminal Intelligence System, біометрична ідентифікація в реальному часі) та Нідерландах (платформа Data-driven Policing, система Sense).

У висновках автор наголошує на комплексному характері модернізації правоохоронних систем, що охоплює структурні, функціональні, технологічні та правові аспекти. Підкреслюється необхідність збалансованого підходу, який поєднує вимоги ефективності та безпеки з дотриманням демократичних принципів і прав людини. Для України запропоновано рекомендації щодо формалізації інтегрованих команд безпеки, впровадження систем прогнозної аналітики та вдосконалення міжвідомчої координації з урахуванням викликів воєнного стану та необхідності забезпечення національної стійкості.

Ключові слова: правоохоронні органи, національна безпека, міжвідомча координація, транскордонна злочинність, національна стійкість.

Постановка проблеми. Сучасні загрози національній безпеці, такі як кіберзлочини, тероризм і транскордонна злочинність, вимагають від правоохоронних органів переходу від традиційних ієрархічних структур до гнучких, адаптивних моделей, які інтегрують передові технології та посилюють міжвідомчу координацію. Відсутність ефективних організаційно-правових механізмів для впровадження реформ і координації між різними відомствами ускладнює швидке реагування на загрози та захист критичної інфраструктури. В Україні, де воєнний стан підкреслює потребу в стійких правоохоронних системах для забезпечення національної безпеки, аналіз міжнародного досвіду реформування може сприяти вдосконаленню організаційних структур і міжвідомчої взаємодії, враховуючи виклики, пов'язані з етичним використанням технологій і захистом прав громадян.

Стан дослідження. Проблематика реформування правоохоронних органів у контексті забезпечення національної безпеки активно досліджується зарубіжними вченими. Американські дослідники Б. Фрідман, Р. Хармон та Ф. Гейдарі аналізують еволюцію ролі федерального уряду США в локальній поліцейській діяльності, а З. Лауб вивчає трансформацію ФБР у сфері національної безпеки. Європейський досвід висвітлено в офіційних документах урядів Франції та Великобританії. Питання кіберзахисту досліджують С. МакЛеллан та Н. О'Лірі на прикладі Естонії, А. Добелл і Г. О'Ніл аналізують японський досвід, а М. Шуленбург та М. Судійн вивчають використання великих даних поліцією Нідерландів. Технологічні аспекти модернізації розглянуто в роботах Б. Пірсалла про прогнозну поліцейську діяльність та звітах

[1] Робота виконана в рамках проєктів «Засади діяльності правоохоронних органів у сфері контролю за системою залучення і використання МТД: глобалізаційний вимір» (номер державної реєстрації 0124U000635) та «Інституційна консолідація через правову синергію: забезпечення національної безпеки в кризових умовах» (номер державної реєстрації 0125U001542)

Graduate Institute щодо цифровізованої міської безпеки. Водночас бракує комплексних порівняльних досліджень, які б систематизували глобальні тенденції та визначали їх застосовність для країн в умовах військового конфлікту, зокрема для України.

Мета статті є аналіз сучасних тенденцій у реформуванні організаційних структур правоохоронних органів провідних країн світу з акцентом на їхню роль у забезпеченні національної безпеки через інтеграцію передових технологій і посилення міжвідомчої координації.

Виклад основного матеріалу. Сучасні тенденції в організаційному будівництві правоохоронних органів характеризуються переходом від централізованих ієрархічних структур до більш гнучких, адаптивних моделей управління. Провідні країни світу демонструють різноманітні підходи до структурної реорганізації правоохоронних систем, що відображає специфіку їх національних особливостей та історичних традицій. Наприклад, у Сполучених Штатах Америки, як зазначають Б. Фрідман, Р. Хармон і Ф. Гейдарі, спостерігалася незначна роль федерального уряду у вдосконаленні поліцейської діяльності, що була обумовлена його фрагментарним і реактивним підходом, який здебільшого обмежується переслідуванням окремих поліцейських у випадках порушень або розслідуванням системних проблем у діяльності окремих департаментів силами Відділу з громадянських прав [1].

Натомість зараз, у Сполучених Штатах Америки спостерігається інша тенденція до посилення координаційних механізмів між федеральними, штатними та місцевими правоохоронними агенціями, особливо в контексті протидії тероризму після подій 11 вересня 2001 року. Діючи на рекомендації Комісії з питань 11 вересня, Конгрес і президент Дж. Буш-молодший помістили шістнадцять відомств розвідувального співтовариства Сполучених Штатів Америки, включаючи ФБР, ЦРУ, Агентство національної безпеки та різні військові відомства, під егідою нещодавно створеного Офісу директора національної розвідки з допоміжними органами для заохочення міжвідомчого обміну інформацією з питань боротьби з тероризмом та контррозвідки [2].

Створення Департаменту внутрішньої безпеки та розширення повноважень ФБР у сфері національної безпеки свідчать про інтеграцію традиційних правоохоронних функцій з завданнями забезпечення національної безпеки. З 2001 року штат ФБР зріс більш ніж на десять тисяч осіб, особливо серед лінгвістів та аналітиків розвідки, і розширив свою присутність за кордоном. У 2005 році було створено відділ національної безпеки для централізації роботи ФБР з питань боротьби з тероризмом, контррозвідки, зброї масового знищення та збору розвідувальних даних.

Об'єднані оперативні групи з боротьби з тероризмом (JTTF), у яких агенти ФБР працюють разом із правоохоронними органами штату та місцевого самоврядування, зросли з двадцяти п'яти у 2001 році до понад ста у 2017 році. Кожен із п'ятдесяти шести польових офісів ФБР отримав команду спецназу з бойовою зброєю та спорядженням, що демонструє мілітаризацію традиційних правоохоронних структур у відповідь на нові загрози національній безпеці [2].

Цей приклад свідчить про те, що навіть у країні з традиційно децентралізованою правоохоронною системою, як-от США, нові виклики, зокрема тероризм, спонукають до посилення міжвідомчої координації, інтеграції функцій безпеки та трансформації організаційних структур. Україна також активно застосовує подібні підходи до міжвідомчої взаємодії, зокрема через координацію між правоохоронними, розвідувальними та аналітичними структурами в умовах воєнного стану. Водночас подальше вдосконалення таких механізмів може відбуватися шляхом формалізації інтегрованих команд безпеки, які працюють у межах єдиної стратегії національної безпеки та забезпечують системний обмін інформацією і спільне реагування на загрози.

Європейські країни демонструють схожі тенденції, хоча з урахуванням специфіки континентальної правової системи та традицій державного управління. Аналіз досвіду Франції ілюструє, як організаційно-правовий механізм може забезпечувати національну стійкість через чітко структуровану імплементацію реформ. У Франції, подібно до України, сучасні виклики, такі як тероризм і кіберзлочинність, спонукали до реформування правоохоронних структур, зокрема Національної поліції та Жандармерії. Циркуляр від 27 грудня 2022 року встановлює процедурний каркас для швидкого впровадження законів, вимагаючи розробки імплементаційних постанов протягом шести місяців після їх публікації в Офіційному віснику, якщо не передбачено відстрочки. Генеральний секретаріат Уряду координує міжвідомчий моніторинг, включаючи організацію зустрічей для визначення відповідальних міністерств і підготовку звітів через три місяці після прийняття закону, з подальшими оцінками через чотири-п'ять місяців. Цей механізм забезпечує ефективну координацію, подібну до українських зусиль, таких як Указ Президента України № 479/2021 [3], спрямований на створення системи національної стійкості [4]. Реформи Є. Макрона 2021 року, які передбачають подвоєння присутності поліцейських і жандармів на вулицях, створення резервних сил і модернізацію обладнання, таких як пістолети SIG Sauer Pro SP 2022, демонструють, як Франція інтегрує організаційні та технологічні зміни для підвищення безпеки [5].

Щодо досвіду Англії та Уельсу, то реформи правоохоронних органів, запроваджені за уряду лейбористів та коаліційного уряду, спрямовувалися на підвищення ефективності поліції в умовах бюджетних обмежень та зміцнення взаємодії з громадами. За лейбористів було введено партнерство на місцевому рівні, створено цивільних помічників поліції (PCSO) та нові національні органи, такі як Агентство з покращення роботи поліції (NPIA), Агентство з боротьби з організованою злочинністю (SOCA) та Незалежна комісія зі скарг на поліцію (IPCC). Коаліційний уряд замінив поліцейські ради на обраних комісарів з питань поліції та злочинності (PCC), створив Національне агентство зі злочинності (NCA) та Коледж поліції, а також реформував оплату праці за рекомендаціями огляду Вінсора. Однак скорочення фінансування на 20% у 2010–2015 роках призвело до зменшення кількості офіцерів поліції на 11% та PCSO на 25%, що поставило під загрозу місцеве патрулювання. Незважаючи на добру адаптацію до фінансових викликів, як зазначила Інспекція Її Величності, пропозиції щодо реформування структури 43 територіальних сил та системи скарг свідчать про необхідність подальших змін для забезпечення ефективної взаємодії з громадами та боротьби з транскордонною злочинністю [6].

Розширення спектра загроз національній безпеці обумовлює необхідність диверсифікації функціональних повноважень правоохоронних органів. Традиційні завдання з підтримання громадського порядку та розслідування злочинів доповню-

ються новими функціями, пов'язаними з протидією кіберзлочинності, економічним злочинам, організованій злочинності та тероризму.

Особливої уваги заслуговує розвиток спеціалізованих підрозділів, що займаються кіберзлочинністю. Провідні країни світу створюють спеціалізовані кіберполіцейські підрозділи, які поєднують традиційні правоохоронні методи з сучасними технологічними можливостями. Ці структури не лише розслідують кіберзлочини, але й здійснюють превентивні заходи з захисту критичної інфраструктури держави. Досвід Естонії, Японії та Німеччини демонструє, як організаційно-правові та інформаційно-технологічні механізми інтегруються для протидії кіберзагрозам, що є важливим для порівняльного аналізу з українськими зусиллями в умовах воєнного стану.

Естонія, відома своєю передовою цифровою інфраструктурою, створила кіберполіцейський підрозділ у складі Центрального кримінального департаменту Поліцейсько-прикордонної служби (PBGB). Цей підрозділ, як відмічають С. Маклеллан Н. О'Ліpі, відомий як Cybercrime Unit (C3), зосереджений на зборі та аналізі інформації про кіберзагрози, розслідуванні кіберзлочинів і превентивній роботі, включаючи проєкт No More Ransom для надання інструментів дешифрування після атак ransomware [7]. Після кібератак 2007 року, які паралізували банківські та державні системи, Естонія розвинула міжвідомчу координацію, співпрацюючи з NATO Cooperative Cyber Defence Centre of Excellence у Таллінні. Цей центр проводить щорічні навчання Locked Shields, які об'єднують кіберекспертів із 25 країн для моделювання захисту критичної інфраструктури, що сприяє підвищенню національної стійкості через технологічні та організаційні інновації [8].

Японія у 2022 році реформувала свою кіберполіцію, створивши Бюро кіберсправ при Національному поліцейському агентстві (NPA), яке координує боротьбу з кіберзлочинами та кібертероризмом на національному рівні. Ця реформа об'єднала кіберпідрозділи з кількох бюро, включаючи підрозділи планування кіберполітики та розслідування кіберзлочинів, для ефективного захисту критичної інфраструктури, такої як енергетичні та транспортні системи [9].

У 2024 році NPA оголосило про створення Telecom Scam Allied Investigation Team (TAIT) для боротьби з шахрайством, що свідчить про адаптацію до нових викликів. Японія також співпрацює з США в рамках U.S.-Japan Cyber Defense Policy Working Group, що дозволяє обмінюватися розвідданими та вдосконалювати кіберзахист. Ці заходи, на думку А. Добелла та Г. О'Ніл демонструють інтеграцію організаційно-правового механізму з інформаційно-технологічним [10], подібно до українських зусиль із розбудови кіберзахисту.

Важливою подією у контексті посилення кібербезпеки у Японії стало ухвалення у травні 2025 року історичного Закону про активну кіберзахист, що ознаменував собою кардинальну зміну в стратегії кібербезпеки країни. Сфера застосування законодавства значно виходить за межі його назви, охоплюючи низку положень, спрямованих на модернізацію державних установ та вдосконалення загальної системи кібербезпеки Японії. Закон також зобов'язує операторів критичної інфраструктури, які були визначені відповідно до Закону про сприяння економічній безпеці 2022 року, повідомляти уряду про інциденти кібербезпеки, хоча те, що і коли потрібно повідомляти, залишається незрозумілим [10].

У Німеччині кіберполіцейські функції виконує Федеральне управління кримінальної поліції (BKA) через спеціалізований відділ кіберзлочинності, який співпрацює з земельними поліцейськими управліннями та Федеральним управлінням із захисту інформації (BSI). Аналіз положень німецького законодавства та звіту Федерального кримінального відомства (BKA) щодо кіберзлочинності у 2024 році демонструє стійко високу загрозу для внутрішньої безпеки, що вимагає системної реакції з боку правоохоронних органів. Дані про понад 130 тисяч кіберзлочинів на території Німеччини, а також майже 202 тисячі злочинів, скоєних з-за кордону, підтверджують транснаціональний характер кіберзлочинності, що зумовлює необхідність міжнародної співпраці та координованих операцій, як-от Operation Endgame. Особливу увагу приділено загрозі від програм-вимагачів (ransomware), які, попри часткове зменшення кількості атак унаслідок поліцейських дій, залишаються однією з головних небезпек. Проблемною залишається низька розкриваність кіберзлочинів – лише 32% у порівнянні з загальною кримінальною статистикою (58%), що свідчить про виклики, пов'язані з технічною складністю, анонімністю та розподіленістю таких злочинів. Зростання хактивізму, DDoS-атак, фішингу, особливо через SMS (smishing), та використання штучного інтелекту для скоєння злочинів вимагає від правоохоронних органів посилення експертизи, кібероперативних спроможностей і міжвідомчої взаємодії, а також впровадження превентивних технологій і відповідного правового регулювання [11]. Ця модель міжвідомчої та міжнародної взаємодії підкреслює важливість організаційно-правового механізму для національної стійкості, що може бути прикладом для України у вдосконаленні координації між Радою національної безпеки і оборони України, Службою безпеки України та іншими органами.

Цифрова революція кардинально змінює методи роботи правоохоронних органів. Впровадження штучного інтелекту, аналітики великих даних, біометричних технологій та систем автоматизованого розпізнавання створює нові можливості для превентивного виявлення загроз та оперативного реагування на них. Досвід Сінгапуру, Австралії та Нідерландів демонструє, як інтеграція цифрових технологій у правоохоронну діяльність сприяє створенню цілісних організаційно-правових та інформаційно-технологічних механізмів, що можуть бути прикладом для України в умовах воєнного стану.

У Сінгапурі цифрова трансформація поліції здійснюється через ініціативу Smart Nation, яка включає використання штучного інтелекту та аналітики великих даних для прогнозування злочинності. Поліція Сінгапуру (SPF) застосовує систему PolCam 2.0, що об'єднує камери відеоспостереження з технологіями розпізнавання облич для моніторингу громадських місць у реальному часі [12]. З 2020 року SPF співпрацює з Home Team Science and Technology Agency (HTX), яке розробило платформу для аналізу даних із соціальних мереж і сенсорів для виявлення потенційних загроз, таких як масові заворушення чи терористичні акти [13]. Ці технології дозволяють поліції оперативно реагувати на інциденти, а також координувати дії з іншими відомствами, що відображає інтеграцію інформаційно-технологічного механізму з організаційно-правовим, подібно до українських зусиль із розбудови систем раннього попередження.

В Австралії Федеральна поліція (AFP) активно використовує біометричні технології та штучний інтелект у рамках про-

грами National Criminal Intelligence System (NCIS). З 2023 року AFP впровадила біометричну ідентифікацію для боротьби з транскордонною злочинністю, зокрема торгівлею людьми та кібершахрайством, використовуючи бази даних для зіставлення відбитків пальців і ДНК у реальному часі [14]. Система Predictive Policing, яка як зауважує Б. Пірсолл застосовує аналітику великих даних, дозволяє прогнозувати злочинні «гарячі точки» на основі історичних даних і соціальних індикаторів [15]. Ця модель забезпечує міжвідомчу координацію через Australian Criminal Intelligence Commission (ACIC), що сприяє обміну інформацією між федеральними та місцевими органами, зміцнюючи національну стійкість. Досвід Австралії підкреслює важливість інтеграції технологій у правоохоронну діяльність, що може бути корисним для України у вдосконаленні кіберзахисту.

У Нідерландах Національна поліція (Politie) використовує платформу Data-driven Policing, яка базується на штучному інтелекті та аналітиці великих даних для прогнозування злочинів і управління ресурсами. З 2021 року поліція впровадила систему Sense, яка інтегрує дані з камер відеоспостереження, сенсорів і відкритих джерел для виявлення загроз у реальному часі, наприклад, підозрілих моделей поведінки в аеропортах чи вокзалах [16]. Крім того, Нідерланди активно застосовують біометричні технології, такі як розпізнавання облич, у рамках програми CATCH для ідентифікації підозрюваних у громадських місцях, що викликало дискусії щодо приватності, але підвищило ефективність превентивних заходів [17]. Співпраця з Europol через Європейський центр кіберзлочинності (EC3) забезпечує обмін розвідданими, що підкреслює значення міжвідомчої та міжнародної взаємодії для національної стійкості, подібно до українських зусиль із координації між СБУ та іншими органами.

Таким чином, системи прогнозної аналітики дозволяють правоохоронним органам ідентифікувати потенційні загрози національній безпеці на ранніх стадіях, що значно підвищує ефективність превентивних заходів. Водночас, використання цих технологій порушує важливі питання щодо захисту приватності та недопущення дискримінації.

Висновки. Модернізація систем правоохоронних органів у провідних країнах світу є комплексним процесом, що охоплює структурні, функціональні, технологічні та правові аспекти їх діяльності. Головні тенденції включають диверсифікацію функцій, технологічну трансформацію, посилення міжнародного співробітництва та розвиток механізмів демократичного контролю.

Зв'язок між модернізацією правоохоронних органів та національною безпекою є очевидним і багатоаспектним. Правоохоронні структури відіграють центральну роль у забезпеченні внутрішньої безпеки держави, протидії новим формам загроз та підтриманні стабільності демократичних інститутів. Їх ефективність безпосередньо впливає на здатність держави захищати свої національні інтереси та забезпечувати безпеку громадян.

Успішна модернізація правоохоронних систем потребує збалансованого підходу, що враховує як вимоги ефективності та безпеки, так і необхідність дотримання демократичних принципів та прав людини. Важливим є забезпечення адекватного фінансування, розвиток людських ресурсів та створення сприятливого правового середовища для впровадження інновацій.

Література:

1. Friedman B., Harmon R., Heydari F. The federal government's role in local policing. Virginia Law Review. 2023. № 109(8), 1527. URL : https://virginialawreview.org/articles/the-federal-governments-role-in-local-policing/ (date of appeal: 21.07.2025)
2. Laub Z. The FBI's Role in National Security. *Counsil on foreign relation* : *website.* URL : https://www.cfr.org/backgrounder/fbis-role-national-security. (date of appeal: 21.07.2025)
3. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» : указ Президента України №479/2021 від 27 вер. 2021 р. URL : https://www.president.gov.ua/documents/4792021-40181 (дата звернення: 21.07.2025)
4. Application des lois : ce que dit la circulaire du 27 décembre 2022. *Vîa publique : website.* URL : https://surl.li/wwihna (date of appeal: 21.07.2025)
5. Renforcer la présence des forces de l'ordre sur la voie publique : créer 200 brigades de gendarmerie en milieu rural et doubler le nombre de policiers sur le terrain d'ici 2029. *EM* : *website.* URL : https://surl.li/wwxovc (date of appeal: 21.07.2025)
6. Police reform in England and Wales. *UK Parliament* : *website.* URL : https://surl.lt/xpruqy (date of appeal: 21.07.2025)
7. MacLellan S., O'Leary N. Doing Battle in Cyberspace: How an Attack on Estonia Changed the Rules of the Game. *Centre of International Governance Innovation* : *website.* URL : https://surli.cc/pvpbyx (date of appeal: 21.07.2025)
8. NATO Cooperative Cyber Defence Centre of Excellence. *Republic of Estonia Defence Forces* : *website.* URL : https://mil.ee/en/landforces/ccdcoe/ (date of appeal: 21.07.2025)
9. National Center of Incident readiness and Strategy for Cybersecurity (NISC). Overview of Cybersecurity 2022 : June 17, 2022. National Center of Incident readiness and Strategy for Cybersecurity (NISC). Tokyo : NISC, 2022. 68 p. URL : https://www.nisc.go.jp/eng/pdf/CS2022_EN.pdf
10. Dobell A., O'Neill G. Japan's new Active Cyber Defense Law: A Strategic Evolution in National Cybersecurity. *Cybersecurity and Law* : *website.* URL : https://surl.li/tdmars (date of appeal: 21.07.2025)
11. Bundeslagebild Cybercrime 2024 : BKA setzt anhaltend hoher Cyberbedrohung zahlreiche Ermittlungserfolge entgegen. *BKA* : *website.* URL : https://www.bka.de/DE/Home/home_node.html (date of appeal: 21.07.2025)
12. Shreeyaa K. With an eye on safety and security, PolCam has played a vital policing role in our neighbourhoods. *Singapore Police Force* : *website.* URL : https://www.police.gov.sg/Media-Room/Police-Life/2024/12/Vigilant-Guardians-Safer-Streets (date of appeal: 21.07.2025)
13. Jain S., Rall J., Santarpia A., Haltmeier D. Graduate Institute of International and Development Studies. Urban Digitised Security: Final Report. URL : https://surl.li/xhzkjo (date of appeal: 21.07.2025)
14. Taylor J. Australian federal police using AI to analyse data obtained under surveillance warrants. Guardian. 2023. Sep 22. URL : https://surl.li/kgohvx (date of appeal: 21.07.2025)
15. Pearsall, B. Predictive Policing: The Future of Law Enforcement. National Institute of Justice Journal. 2010. Issue 266. P. 16. URL : https://www.ojp.gov/pdffiles1/nij/230414.pdf. (date of appeal: 21.07.2025)
16. Schuilenburg M., Soudijn M. Big data policing: The use of big data and algorithms by the Netherlands Police. *Policing: A Journal of Policy and Practice*, Volume. 2023. № 17. URL : https://doi.org/10.1093/police/paad061 (date of appeal: 21.07.2025)
17. Catch A Serial Offender (Catch) Program. SAPRO : *website.* URL : https://surl.li/gevvit (date of appeal: 21.07.2025)

Maletova O. Modernizing law enforcement systems in the context of national security: international experience and ukrainian perspectives

Summary. The article examines contemporary trends in reforming the organizational structures of law enforcement agencies in leading countries worldwide, with an emphasis on their role in ensuring national security through the integration of advanced technologies and enhancement of inter-agency coordination. The relevance of the research stems from the emergence of new threats to national security, such as cybercrime, international terrorism, and transnational organized crime, which require law enforcement agencies to transition from traditional centralized hierarchical structures to more flexible and adaptive management models. The topic holds particular significance for Ukraine under martial law conditions, where the effectiveness of the law enforcement system directly impacts national resilience.

The author conducts a comprehensive analysis of law enforcement system reform experiences in the United States, European countries (France, United Kingdom, Germany, Estonia, Netherlands), and Asia-Pacific region countries (Japan, Singapore, Australia). Using the United States as an example, the transformation of the law enforcement system following the events of September 11, 2001, is demonstrated, which included establishing new coordination structures, expanding FBI powers in national security, and forming joint terrorism task forces. France's experience illustrates the importance of a clear organizational-legal mechanism for implementing reforms through establishing procedural frameworks for rapid legislative implementation.

Particular attention is given to the development of specialized cyber police units as a response to growing cyber threats. The article provides detailed examination of Estonia's experience, which created an effective cyber defence system with international coordination through NATO following the major cyberattacks of 2007; Japan, which conducted comprehensive cyber police reform in 2022-2025 with the adoption of the historic Active Cyber Défense Law; and Germany, where an extensive cybercrime prevention system operates, although the clearance rate for such crimes remains low (32%).

A substantial portion of the research is devoted to the digital transformation of law enforcement agencies. The implementation of artificial intelligence technologies, big data analytics, biometric systems, and predictive analytics is analysed in Singapore (Smart Nation initiative, PolCam 2.0 system), Australia (National Criminal Intelligence System, real-time biometric identification), and the Netherlands (Data-driven Policing platform, Sense system).

In the conclusions, the author emphasizes the comprehensive nature of law enforcement system modernization, encompassing structural, functional, technological, and legal aspects. The necessity of a balanced approach is underscored, combining efficiency and security requirements with adherence to democratic principles and human rights. For Ukraine, recommendations are proposed regarding the formalization of integrated security teams, implementation of predictive analytics systems, and improvement of inter-agency coordination, considering the challenges of martial law and the need to ensure national resilience.

Key words: law enforcement agencies, national security, inter-agency coordination, transnational crime, national resilience.

Дата надходження статті: 21.07.2025
Дата прийняття статті: 31.07.2025
Опубліковано: 30.09.2025