УДК 351.74:331.108:004.056(477)
DOI https://doi.org/10.32850/LB2414-4207.2025.37.13

# ТРУДОВІ ФУНКЦІЇ ОПЕРУПОВНОВАЖЕНОГО В ПАРАДИГМІ ILP: НОРМАТИВНО-ПРАКТИЧНІ ОРИСИ ТА КІБЕРКОМПОНЕНТ

**Шаронов Андрій Павлович,**
orcid.org/0009-0002-1761-9646
аспірант
(Одеський державний університет внутрішніх справ, м. Одеса, Україна)

У статті здійснено науково-практичний аналіз трудових функцій оперуповноваженого поліції крізь призму переходу до поліцейської діяльності, керованою розвідувальною аналітикою (Intelligence-Led Policing, ILP) з акцентом на кіберкомпонент. На основі чинного законодавства України, міжнародних актів та переліку трудових функцій і дій з проєкту професійного стандарту «Оперуповноважений (поліція)» запропоновано систематизацію функцій, оновлені компетентності та організаційні механізми їх реалізації. Обґрунтовано необхідність інтеграції ризик-аналізу, OSINT, протидії кіберзлочинності та управління електронними доказами в повсякденну роботу оперуповноважених, із дотриманням прав людини та вимог процесуального закону. Приділено увагу компетентностям оперуповноваженого від нормативного знання до кіберкомпонента (OSINT, моніторинг віртуальних активів, негласні розшукові заходи у сфері комп'ютерних систем, AI). Визначено нормативні орієнтири трудових функцій сучасного оперуповноваженого. Зроблено висновок, що актуалізація трудових функцій кіберполіцейського вимагає цілісної моделі діяльності, у якій аналітика, реагування на інциденти, процесуальне забезпечення, цифрова криміналістика, захист критичної інфраструктури та робота з криптоактивами утворюють єдиний, взаємопов'язаний цикл. Крім того, кіберкомпоненти трудових функцій кіберполіцейського формують взаємодоповнювану систему: аналітика дає змогу приймати обґрунтовані рішення; реагування – трансформувати події у процесуально значущі кейси; процесуальне забезпечення та цифрова криміналістика – перетворювати технічні знахідки на допустимі докази; робота з критичною інфраструктурою – зберігати стійкість життєво важливих послуг; компетентність у криптоактивах – протидіяти фінансовим і технологічним зловживанням у цифровій економіці.

**Ключові слова:** оперуповноважений, розвідувальна аналітика, оперативно-розшукова діяльність, компетентність, трудова функція, кібербезпека, НСРД, OSINT, AI, електронні докази.

# LABOR FUNCTIONS OF THE OPERATIONAL AUTHORITY IN THE ILP PARADIGM: REGULATORY AND PRACTICAL ASPECTS AND CYBERCOMPONENTS

**Sharonov Andrii Pavlovych,**
orcid.org/0009-0002-1761-9646
Postgraduate Student
(Odessa State University of Internal Affairs, Odessa, Ukraine)

The article provides a scientific and practical analysis of the work functions of a police officer through the prism of the transition to intelligence-led policing (Intelligence-Led Policing, ILP) with an emphasis on the cyber component. It is based on the current legislation of Ukraine, international acts and the list of work functions and actions from the draft professional standard "Officer (Police)", a systematization of functions, updated competencies and organizational mechanisms for their implementation are proposed. The need to integrate risk analysis, OSINT, countering cybercrime and managing electronic evidence into the daily work of officers is substantiated, while respecting human rights and the requirements of procedural law. Attention is paid to the competencies of the officer from normative knowledge to the cyber component (OSINT, monitoring of virtual assets, covert investigative measures in the field of computer systems, AI). The normative guidelines for the work functions of a modern officer are determined. It is concluded that the actualization of the work functions of a cyber police officer requires a holistic model of activity in which analytics, incident response, procedural support, digital forensics, critical infrastructure protection, and work with crypto assets form a single, interconnected cycle. In addition, the cyber components of the work functions of a cyber police officer form a mutually complementary system: analytics allows for informed decisions; response – to transform events into procedurally significant cases; procedural support and digital forensics – to transform technical findings into admissible evidence; work with critical infrastructure – to maintain the stability of vital services; competence in crypto assets – to counteract financial and technological abuse in the digital economy.

**Key words:** operational officer, intelligence analytics, operational and investigative activities, competence, work function, cybersecurity, NSRD, OSINT, AI, electronic evidence.

**Актуальність.** Трансформація криміногенного середовища у цифрову площину, поява транснаціональних злочинних екосистем «crime-as-a-service» та інтенсивна міграція доказової інформації в електронні середовища, а також розвиток аналітично-розвідувальних (intelligence-led) та алгоритмічно підсилених (AI-enabled) підходів вимагають переосмислення трудових функцій та трудових дій оперативних працівників підрозділів Національної поліції України, насамперед співробітників Департаменту кіберполіції та Департаменту кримінального аналізу.

Міжнародні стандарти та національне законодавство України створюють рамкові умови для переходу від реактивної моделі до проактивної поліцейської діяльності (Intelligence-Led Policing, ILP), де рішення ухвалюються на підставі розвідданих, ризик-аналізу та прогнозної аналітики [1]. Таке переорієнтування відповідає стратегічним документам України у сфері кібербезпеки й забезпечує збалансованість між правами людини та ефективністю правоохоронної функції та з урахуванням релевантних європейських актів (Директива Мережева та інформаційна безпека 2 (NIS2) [2], Закон ЄС про штучний інтелект (AI Act) [3].

Саме тому необхідно систематизувати компетентності оперуповноваженого поліції від нормативного знання до кіберкомпонента у професійний стандарт «Оперуповноважений (поліція)».

**Мета і завдання дослідження.** Мета статті – на основі національної нормативної бази та сучасних підходів поліцейської діяльності, керованою розвідувальною аналітикою розробити цілісну модель трудових функцій сучасного оперуповноваженого з акцентом на: по-перше, правові засади дій і гарантії прав людини; по-друге, ризик-орієнтований підхід сучасної поліцейської діяльності, по-третє, кіберкомпонент (OSINT, криптоактиви, електронні докази, негласні слідчі (розшукові) заходи у сфері комп'ютерних систем).

Під час дослідження ми ставимо перед собою такі **завдання:** конкретизувати зміст трудових функцій; інтегрувати ILP у трудові функції оперуповноваженого; сформулювати пропозиції до проєкту професійного стандарту «Оперуповноважений (поліція)».

**Методологія.** Дослідження проведено на прикладі організації професійної діяльності поліцейських Департаменту кіберполіції Національної поліції України. Застосовані інструменти включали аналіз відповідних теоретичних і методологічних джерел, а також узагальнення досвіду управління зазначеним міжрегіональним підрозділом на посаді першого заступника начальника департаменту. Для досягнення поставленої мети дослідження використано низько методів, а саме: теоретичний – для вивчення й аналізу службової документації, науково-методичної та навчальної літератури, узагальнення інформації для визначення теоретико-методологічних основ дослідження; логічного аналізу – для формулювання основних понять та проведення класифікації; конкретно-історичний – для демонстрації динаміки розвитку функцій у різних моделях поліцейської діяльності; діалектики – для встановлення змісту й особливостей складових елементів в поліцейській діяльності; емпіричні методи – для узагальнення практичного досвіду, спостереження та обговорення.

**Виклад основного матеріалу.** На початку нашої роботи розглянемо нормативні орієнтири трудових функцій оперуповноваженого. Так, правовий статус, обсяг повноважень і засади діяльності Національної поліції України визначаються Конституцією України [4], законом України «Про Національну поліцію» (ст. ст. 2, 5, 17, 18, 23, 25, 30, 31) [5], а також спеціальним законодавством – насамперед законом України «Про оперативно-розшукову діяльність» [6], Кримінальним процесуальним кодексом України (ст. ст. 36, 40, 41, 104, 107, 208 глава 21) [7] та законом України «Про основні засади забезпечення кібербезпеки України» (ст. ст. 8-10) [8] та іншими актами. У сукупності ці документи формують цілісну нормативну рамку, в межах якої оперуповноважений поліції як посадова особа оперативного підрозділу реалізує свої функції, взаємодіючи зі слідчими підрозділами, іншими органами публічної влади та інститутами громадянського суспільства. Вказана рамка органічно спирається на принципи верховенства права, законності, недискримінації, прозорості, поваги до гідності та прав людини, а також пропорційності втручання у приватність, підзвітності й належного врядування; саме ці принципи задають межі будь-яких оперативно-розшукових і слідчих дій та повинні бути інтегровані у планування, проведення й документування відповідних заходів. З огляду на цифровий вимір злочинності, діяльність у сфері комп'ютерних систем координується також Стратегією кібербезпеки України [9], а у міжнародному вимірі ключовим є Будапештська конвенція про кіберзлочинність [10] і Другий додатковий протокол до Європейської конвенції про взаємну допомогу у кримінальних справах (2022) [11], які створюють інструменти для прискореного доступу до електронних доказів і розширюють канали прямої взаємодії

з провайдерами послуг. Це прямо впливає на трудові дії з отримання та фіксації електронних доказів, запитів і міждержавного обміну, підкреслює необхідність обміну доказами, розбудови спроможностей кіберпідрозділів та партнерства з приватним сектором.

Оперативно-розшукова ж діяльність детермінується законом як система правових і організаційних засобів здобуття інформації про злочини та осіб, причетних до їх учинення, що для оперуповноваженого означає ініціювання й проведення оперативно-розшукових заходів, застосування оперативно-технічних засобів, роботу з конфіденційними джерелами, забезпечення належного режиму секретності та доказової верифікації зібраних доказів. Організація взаємодії органів досудового розслідування з іншими підрозділами поліції для запобігання кримінальним правопорушенням, їх виявлення та розслідування, притягнення до встановленої законодавством відповідальності осіб, які їх учинили, відшкодування завданої кримінальними правопорушеннями шкоди, відновлення порушених прав та інтересів фізичних і юридичних осіб здійснюється відповідно до наказу МВС України «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні» [12] та Інструкції щодо реагування на заяви і повідомлення [13].

Своєю чергою кіберкомпонент і міжвідомча координація вибудовуються відповідно до Стратегії кібербезпеки України: Департамент кіберполіції НПУ забезпечує протидію кіберзлочинності, превенцію та взаємодію з приватним сектором і населенням, а CERT-UA, як урядова команда реагування на комп'ютерні інциденти, виступає ключовим партнером поліції у повідомленні, обміні технічною інформацією (показники компрометації, типології атак), первинному реагуванні та ескалації інцидентів [9].

Кіберкомпонент трудових функцій кіберполіцейського – це інтегрований контур від аналітичної розвідки та реагування з CSIRT до процесуального збору електронних доказів і міжнародної координації. В нього входять:

- Моніторинг кіберпростору та аналітична розвідка;
- Реагування на кіберінциденти та міжвідомча взаємодія (CERT/CSIRT, НКЦК);
- Оперативно-розшукове забезпечення кіберпроваджень (НСРД);
- Електронні докази та цифрова криміналістика;
- Протидія кіберзлочинам у сегментах критичної інфраструктури;
- Криптоактиви та фінансово-технічні.

Актуалізація трудових функцій кіберполіцейського вимагає цілісної моделі діяльності, у якій аналітика, реагування на інциденти, процесуальне забезпечення, цифрова криміналістика, захист критичної інфраструктури та робота з криптоактивами утворюють єдиний, взаємопов'язаний цикл. Така модель спирається на національне законодавство у сфері кібербезпеки, кримінального процесу та оперативно-розшукової діяльності, узгоджується з міжнародними зобов'язаннями України й орієнтується на стандарти доказовості, пропорційності та прав людини. У філософії ILP кіберполіцейський виступає не лише виконавцем процесуальних дій, а інтегратором розвідданих, координатором міжвідомчих взаємодій і гарантом процесуальної стійкості електронних доказів.

Вихідною ланкою є постійний моніторинг кіберпростору та аналітична розвідка. Вона охоплює формулювання вимог до розвідданих, систематичне збирання відкритих і технічних даних, їх валідацію, перетворення на аналітичні продукти та контрольоване поширення користувачам у межах кримінального процесу чи превентивної

діяльності. OSINT-джерела доповнюються телеметрією мережевих подій, реєстрами доменних ідентифікаторів, профілями у соціальних мережах, даними про взаємозв'язки суб'єктів у блокчейнах. На цій підставі здійснюється картографічний і часовий аналіз інцидентів, мережевий аналіз зв'язків, атрибуція облікових записів та індикаторів компрометації. Ключовою вимогою є трасованість: кожен крок збирання та обробки матеріалів документується, а для цифрових артефактів забезпечується безперервний ланцюжок володіння. Результатом є аналітичні довідки, профілі загроз і прогнозні моделі, які безпосередньо впливають на пріоритизацію слідчих версій, визначення цілей оперативної роботи та планування профілактичних заходів [20].

Моніторингово-аналітичний цикл безпосередньо підживлює реагування на кіберінциденти та міжвідомчу взаємодію. Реагування розгортається як керований процес із чіткими фазами підготовки, виявлення та реєстрації, первинної оцінки, стримування, викорінення, відновлення та аналізу уроків. У цьому процесі кіберполіція координує кваліфікацію події як кримінального правопорушення, ініціює збереження доказових даних, організовує їх процесуальне вилучення та взаємодіє з державними й галузевими командами реагування (CERT/CSIRT) та Національним координаційним центром кібербезпеки на рівні стратегічного узгодження дій. Технічні індикатори та звіти CSIRT трансформуються в процесуально значущі матеріали, а результати поліцейського реагування повертаються у спільний інформаційний простір у вигляді артефактів, що збагачують виявлення наступних інцидентів. Дієвість цього контуру вимірюється скороченням середнього часу до виявлення та реагування (MTTD/MTTR), часткою інцидентів із повною технічною атрибуцією та відсотком випадків, які успішно інкорпоруються у кримінальні провадження.

Перехід від інцидент-менеджменту до кримінального переслідування забезпечується комплексом гласних слідчих (розшукових) дій та негласних слідчих (розшукових) дій. У кіберсередовищі це вимагає особливої уваги до необхідності та пропорційності втручання, мінімізації обсягу даних, що не стосуються провадження, і захисту приватності. Технічна безпечність НСРД означає використання методів, які не змінюють первинний стан систем і даних, забезпечують достеменність журналів подій та контроль цілісності зібраної інформації. Важливо забезпечити безшовний перехід між фазами: результати НСРД логічно підкріплюють клопотання про гласні дії (тимчасовий доступ, обшуки, експертизи) й у подальшому витримують судову експертизу на допустимість, належність і достовірність.

Центральним критерієм успіху кіберполіцейської діяльності є якість роботи з електронними доказами та рівень цифрової криміналістики. Ідентифікація, належне збирання, збереження, аналіз і представлення цифрових артефактів відбуваються за методиками, що гарантують відтворюваність і прозорість. Бездеструктивне копіювання з фіксацією контрольних хеш-сум, чітке розмежування даних, що охоплюються правовими таємницями, протоколювання інструментів і параметрів аналізу, peer-review експертних висновків – необхідні елементи процесуальної стійкості. Практика вимагає не лише технічної компетентності, а й уміння перекладати технічні знахідки на процесуально зрозумілу мову, пояснюючи межі інтерпретації та похибки, що супроводжують цифрову реконструкцію подій.

Особливий вимір становить протидія кіберзлочинності у сегментах критичної інфраструктури, де пріоритет безпеки технологічних процесів і безперервності послуг превалює над іншими міркуваннями. Тут робота кіберполіції інтегрується з вимогами безпеки промислових систем керування (OT/ICS) і враховує особливості архітектур зон і каналів, режимів промислових протоколів та обмежень на втручання в реальному часі. Операційні підходи передбачають спільне проведення форензик на працюючих

системах із мінімізацією впливу, диференціацію між подією інформаційної безпеки та технологічною аварією, контроль змін конфігурації та ланцюгів постачання. Ефективність взаємодії з операторами критичної інфраструктури посилюється за рахунок попередньо узгоджених сценаріїв реагування, спільних тренувань і двостороннього обміну індикаторами компрометації у стандартизованому форматі.

Нарешті, стрімкий розвиток криптоекосистеми та фінансово-технічних сервісів вимагає від кіберполіцейського спеціалізованої компетентності в домені віртуальних активів. Типові задачі охоплюють виявлення шахрайських схем і відмивання доходів, аналіз транзакційних ланцюгів у блокчейнах із використанням евристик спільного контролю, відстеження маршрутизації через міксери й кросчейн-мости, санкційний скринінг адрес і нод. Критичною є взаємодія з біржами та кастодіальними сервісами для збереження журналів доступів, ідентифікаційних даних і реактивного замороження активів відповідно до процесуальних механізмів і міжнародних запитів. Процесуальне доведення контролю над приватними ключами та походження активів базується на поєднанні on-chain і off-chain доказів, включно з логами автентифікації, мережевими артефактами та фінансовими документами суб'єктів первинного обміну.

Ці домени об'єднують загальносистемні вимоги, що визначають якість і довіру до результатів. По-перше, вбудована доказовість означає, що кожна дія проєктується з урахуванням майбутньої судової перевірки: від формалізації гіпотез до вибору інструментів та способів фіксації. По-друге, координація в межах національної системи кібербезпеки забезпечує узгодженість ролей поліції, CSIRT-спільноти, регуляторів і операторів критичної інфраструктури; вона уможливлює швидке сповіщення, спільні реагування й обмін розвідданими. По-третє, пропорційність і дотримання прав людини є не декларацією, а технічно реалізованою властивістю процесів: мінімізація даних, використання селективних методів доступу, захист персональних даних і контроль повноважень інструментів. По-четверте, у середовищах OT/ICS поліцейські дії підпорядковуються принципу «без переривання технології», що вимагає погоджених із операторами методик аудитів і форензик. По-п'яте, міжнародний вимір – прискорене збереження електронних доказів, взаємна правова допомога та транскордонна атрибуція – є необхідною умовою дієвості в справах із глобальними ланцюгами інфраструктури й фінансових посередників.

Усе це зумовлює потребу системної інтеграції трудових функцій у діяльність оперуповноваженого, уніфікації процедур доступу до електронних інформаційних систем та хмарних сервісів, а також закріплення у внутрішніх регламентах вимог до пропорційності втручання, захисту персональних даних, прозорого аудиту НСРД і регулярного підвищення кваліфікації персоналу на стику оперативної, процесуальної та кібербезпекової компетентностей.

Отже, сьогодні ми вже спостерігаємо створення нових аналітичних підрозділів у державі, так і в структурі Національної поліції України, а також поступовий перехід інших підрозділів поліції на використання інноваційного інформаційно-аналітичного програмного забезпечення та сучасних методик (SOCTA, IOCTA), що, безумовно, підвищує ефективність діяльності органів та підрозділів поліції. Впроваджується модель проактивної діяльності, яка замінює домінуючу парадигму реактивної поліцейської діяльності, створюючи нову сферу [21].

Також Україна поступово стає на колії стандартизованого підходу до різних державних процесів. Підготовка та підвищення кваліфікації співробітників поліції не є винятком. Так, у 2020 році впроваджено Державний освітній стандарт зі спеціальності 262 «Правоохоронна діяльність» другого (магістерський) рівня [14], а в 2024 році

ввели Державний освітній стандарт зі спеціальності 262 «Правоохоронна діяльність», першого (бакалаврський) рівня [15] та Державний освітній стандарт професії 5162 «Поліцейський (за спеціалізаціями)» для системи професійної (професійно-технічної) освіти [16]. Поряд із державними стандартами розвиваються і професійні стандарти. Зокрема, Професійний стандарт «Слідчий (поліція)» – використовується для проектування програм перепідготовки/підвищення кваліфікації та оцінювання результатів навчання поліцейських [17].

Щодо інших стандартів, то тут треба зазначити професійні стандарти «Суддя» та «Прокурор», які внесено до Реєстру 26.12.2024 та 14.01.2025 [18].

Нині триває активна фаза розробки проєкту професійного стандарту «Оперуповноважений (поліція)» [19], у межах наукового дослідження узагальнено та систематизовано перелік трудових дій у складі відповідних трудових функцій, що відображають як нормативно-правові вимоги до посади, сучасні організаційно-професійні підходи до її реалізації, так і потреби ILP.

У контексті ескалації гібридних загроз і поглиблення цифровізації публічних сервісів професійний профіль кіберполіцейського потребує чіткої систематизації кіберкомпонентів трудових функцій. Нижче узагальнено ключові функції, структуровані за принципами ILP і узгоджені з національним законодавством та міжнародними стандартами, що забезпечує доказовість і пропорційність.

Трудова функція 1. Виконання завдань та повноважень поліції відповідно до правових засад та принципів діяльності поліції:

- знати та вміти застосовувати Конституцію України, закон України «Про Національну поліцію», Кримінальний кодекс України, Кримінальний процесуальний кодекс України, закон «Про запобігання корупції» та інші нормативно-правові акти;
- дотримуватись і втілювати основоположні принципи: верховенства права, пропорційності, законності, недискримінації, публічності, прозорості, поваги до людської гідності;
- дотримуватись антикорупційного законодавства, уникати в своїх діях відносно громадян погроз, принижень, сленгу, ненормативної лексики.

Трудова функція 2. Виконання письмових доручень слідчого, вказівки прокурора та ухвали слідчого судді суду і запитів повноважних державних органів, установ та організацій про проведення оперативно-розшукових заходів:

- планувати заходи та здійснювати підготовку до реалізації доручення слідчого, дізнавача, прокурора в порядку, передбаченому Кримінальним процесуальним кодексом України, вживає ряд заходів щодо підвищення ефективності зазначеного напрямку діяльності;
- безпосереднє проводити слідчі (розшукові) дії та негласні (розшукові) дії;

Трудова функція 3. Здійснення комплексу оперативно-розшукових заходів щодо попередження, своєчасного виявлення і припинення кримінальних правопорушень та викриття причин і умов, які сприяють вчиненню кримінальних правопорушень, здійснювати профілактику правопорушень:

- проводити оперативно-розшукові заходи щодо попередження своєчасного виявлення і припинення кримінальних правопорушень (кіберзлочинів) та викриття причин та умов, які спричиняють їх вчиненню;
- виконувати гласні та негласні оперативно-розшукові дії;
- встановлювати зв’язки, канали поширення злочинної інформації;
- брати участь у проведенні слідчих дій.

Трудова функція 4. Здійснювати оцінку оперативної обстановки, ризик-аналіз та аналітичну розвідку:

– проводити збір інформації про оперативну обстановку;
– застосовувати аналітичну розвідку (ILP) та прогнозно-аналітичну діяльність для ухвалення рішень;
– проводити ідентифікацію загроз та ризиків з подальшим ризик-аналізом та типізацією загроз.

Трудова функція 5. Вживати заходи, які спрямовані на попередження та протидію злочинам і правопорушенням (механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку) у сфері комп'ютерних систем:
– здійснювати ідентифікацію кіберзагроз у межах оперативної обстановки;
– моніторити кіберпростір та виявляти кіберзагрози на предмет виявлення ознак підготовки або вчинення кіберзлочинів;
– проводити слідчі (розшукові) дії та негласні (розшукові) дії у сфері комп'ютерних систем;
– проводити інформаційно-профілактичні заходи в сфері комп'ютерних систем.

Трудова функція 6. Здійснювати моніторинг та аналіз відкритих джерел з метою подальших аналітичних досліджень, у тому числі руху віртуальних активів:
– ідентифікувати релевантні відкриті джерела;
– застосовувати інструменти OSINT для дослідження, у тому числі криптоактивів;
– встановлювати первинні характеристики об'єктів дослідження та документувати результати моніторингу;
– ідентифікувати гаманці/адреси, кластеризувати транзакції, здійснювати запити до VASP/бірж щодо збереження й надання даних, ініціювати арешт активів і документувати ланцюжок володіння електронними доказами з подальшою інтеграцією *on-chain* та *off-chain* матеріалів у доказову базу;
– виявляти та документувати використання міксерів, cross-chain bridges і криптоанонімайзерів;
– застосовувати та валідувати моделі ШІ для аналітичної підтримки розслідувань і реагування, тобто будувати пайплайни виявлення аномалій і класифікації (фішинг, бот-мережі та інше), забезпечує прозорість і відтворюваність (логування даних/версій, оцінка похибок та упередженості).

Трудова функція 7. Набуття нових або вдосконалення раніше набутих знань, умінь, навичок своєї професійної діяльності або галузі знань:
– регулярно проходити тренінги, семінари, курси підвищення кваліфікації, перевірки знань в системі службової підготовки;
– здійснювати поточне вивчення та систематизацію змін у законодавстві, нормативно-правовій базі й спеціалізованій літературі з метою вдосконалення професійної компетентності.

Таким чином, по-перше, перехід до інтелектуально-керованої моделі робить аналітичні спроможності оперуповноваженого системоутворювальними; без ILP-циклу функції залишаються фрагментарними. По-друге, нормативна база України забезпечує достатні рамки (Нацполіція, ОРД, КПК, кібербезпека), однак професійний стандарт доцільно деталізувати: включити ILP-компетентності, електронні докази, криптоактиви, NIS2-сумісну взаємодію та KPI ризик-орієнтованого типу. По-третє, кіберкомпоненти трудових функцій кіберполіцейського формують наступну взаємодоповнювану систему: аналітика дає змогу приймати обґрунтовані рішення; реагування – трансформувати події у процесуально значущі кейси; процесуальне забезпечення та цифрова криміналістика – перетворювати технічні знахідки на допустимі докази; робота з критичною

інфраструктурою – зберігати стійкість життєво важливих послуг; компетентність у криптоактивах – протидіяти фінансовим і технологічним зловживанням у цифровій економіці.

**Список використаних джерел:**

1. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Бутко Р., Денисенко Б., Ісмайлов К.Ю. та ін., за заг. ред. Користіна О.Є. Київ: «ВАТЕ», 2024. 444 с.

2. Про заходи для високого спільного рівня кібербезпеки на всій території Союзу: Директива Європейського Парламенту і Ради (ЄС) від 14 грудня 2022 року № 2022/2555. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text

3. Про штучний інтелект: закон ЄС. URL: https://artificialintelligenceact.eu/ai-act-explorer/

4. Конституція України: Закон України 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

5. Про Національну поліцію: закон України від 02.07.2015 № 580-VIII. URL : https://zakon.rada.gov.ua/laws/show/580-19#Text

6. Про оперативно-розшукову діяльність: закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

7. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-VI. *Офіційний вісник України*. 2012. № 37. Ст. 1307.

8. Про основні засади забезпечення кібербезпеки України: закон Україні від 05.10.2017 № 2163-VIII. URL**:** https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

10. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

11. Другий додатковий протокол до Європейської конвенції про взаємну допомогу у кримінальних справах. Конвенція Ради Європи від 08.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_518#Text

12. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: наказ МВС України від 07.07.2017 № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text

13. Про затвердження Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: наказ МВС України від 27.04.2020 № 357. URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text

14. Стандарт вищої освіти України: другий (магістерський) рівень вищої освіти, галузь знань 26 «Цивільна безпека», спеціальність 262 «Правоохоронна діяльність». Затверджено і введено в дію наказом Міністерства освіти і науки України від 22.10.2020 р. № 1294. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/262-Pravookhor.diyaln-mag.31.01.22.pdf

15. Стандарт вищої освіти України: перший (бакалаврський) рівень вищої освіти, галузь знань 26 Цивільна безпека, спеціальність 262 Правоохоронна діяльність. Затверджено і введено в дію наказом Міністерства освіти і науки України від 28 05 2024 р. № 769. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/28.05.2024/262-Pravookhor.Diyaln-bak.769.V%C3%ADd.28.05.24.pdf

16. Державний освітній стандарт з професії 5162 «Поліцейський (за спеціалізаціями)». Затверджено наказом МОН від 07.11.2024 № 1592. URL: https://mon.gov.ua/static-objects/mon/sites/1/pto/standarty/2024/11/07/nakaz-mon-1592-vid-07-11-2024-politseyskyy-za-spetsializatsiyamy.pdf

17. Професійний стандарт «Слідчий (поліція)». Затверджено накахом Національною поліцією України від 28.06.2024 № 724 URL: https://register.nqa.gov.ua/uploads/0/629-profesijnij_standart_slidcij_policia.pdf

18. Професійні стандарти «Суддя» та «Прокурор» внесені до Реєстру кваліфікацій. URL: https://court.gov.ua/press/news/1735928/?utm_source=chatgpt.com

19. Про організацію розроблення проєкту професійного стандарту: наказ Національної поліції України від 2.9 05.2025 № 610.

20. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110–113.

21. Ismailov K.Y. Peculiarities of human rights and freedom while applying intelligence-led policing (ILP). *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2019. Special Issue № 1. P. 36–37.

Дата надходження статті до редакції: 19.06.2025
Дата затвердження статті до друку: 03.07.2025
Дата публікації статті: 03.10.2025