УДК 342.951
DOI https://doi.org/10.32782/2709-9261-2026-1-17-22

**Ковальова Ольга Вікторівна,**
доктор юридичних наук, доцент,
помічник ректора
*(Донецький державний університет внутрішніх справ, м. Кропивницький)*
*ORCID: https://orcid.org/0000-0003-4555-0172*

**Батрак Костянтин Миколайович,**
аспірант науково-дослідної лабораторії
з проблем запобігання кримінальним правопорушенням
Навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної поліції імені Е. О. Дідоренка
*(Донецький державний університет внутрішніх справ, м. Кропивницький)*
*ORCID: https://orcid.org/0009-0000-4071-4321*

# МІЖНАРОДНО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

*У статті здійснено комплексний аналіз міжнародно-правових засад інформаційного забезпечення правоохоронної діяльності в Україні в контексті цифрової трансформації публічного управління та зростання транснаціональних загроз безпеці. Проаналізовано роль інформаційного забезпечення як ключового елементу управління в правоохоронних органах та його значення для реалізації стратегічних завдань реформування сектору безпеки і оборони України, орієнтованих на забезпечення безпеки людини, дотримання прав і свобод та підвищення довіри до державних інституцій. Значну увагу приділено аналізу міжнародного досвіду правового регулювання інформаційних відносин. Зроблено висновок, що адаптація міжнародних та європейських стандартів інформаційного забезпечення правоохоронної діяльності є необхідною умовою подальшої цифрової трансформації України, підвищення ефективності правоохоронної діяльності та інтеграції національної правової системи до європейського правового та інформаційного простору.*

***Ключові слова:*** *правоохоронні органи, інформаційне забезпечення, правоохоронна діяльність, міжнародно-правові засади, європейські стандарти, нормативно-правові акти, міжнародне співробітництво, євроінтеграція.*

**Постановка проблеми.** У сучасному світі, що характеризується глобалізацією, інформація є ключовим фактором у забезпеченні ефективної правоохоронної діяльності. В умовах поширення транснаціональної злочинності, загроз в кіберпросторі, тероризму та інших викликів міжнародного масштабу, критично важливим є створення правових механізмів, що сприяють належному обміну, обробці та захисту інформації між правоохоронними органами України та міжнародними партнерами. Співпраця в галузі інформаційного забезпечення правопорядку будується на міжнародних правових принципах, які регулюють доступ до інформаційних ресурсів, їх обмін та використання відповідно до принципів прав людини, державного суверенітету та міжнародної безпеки.

Україна, як активний гравець на міжнародній арені, дотримується основних принципів міжнародного права в сфері інформаційного забезпечення роботи правоохоронних органів, що включає імплементацію міжнародних норм та стандартів, співробітництво з такими організаціями, як Інтерпол, Європол, ООН, Рада Європи та Європейський Союз. Зокрема, важливими аспектами є забезпечення кібербезпеки, боротьба з організованою злочинністю, протидія корупції та обмін оперативною інформацією в рамках двосторонніх та багатосторонніх угод. Ключову роль у цьому процесі відіграють між-

народні правові акти, зокрема Конвенція ООН проти транснаціональної організованої злочинності (2000), Конвенція Ради Європи про кіберзлочинність (2001), Глобальний антитерористичний стратегічний документ ООН, а також нормативні документи Європейського Союзу. Україна також активно працює над удосконаленням нормативно-правової бази для інтеграції в європейську систему безпеки, що є важливим етапом на шляху до євроінтеграції.

Окрім міжнародних зобов'язань, актуальним залишається питання національного регулювання інформаційного забезпечення правоохоронної діяльності, що охоплює законодавчі акти щодо доступу до інформації, її захисту, персональних даних, а також спеціальні нормативні документи, які визначають діяльність Національної поліції, Служби безпеки України, Державного бюро розслідувань та інших органів.

Таким чином, дослідження міжнародно-правових основ інформаційного забезпечення діяльності правоохоронних органів в Україні є важливим як з теоретичної, так і з практичної точки зору. Воно дозволяє оцінити ступінь інтеграції національного законодавства в глобальну систему правових норм, визначити ключові проблеми та перспективи розвитку ефективної співпраці між правоохоронними органами України та міжнародними організаціями в сфері інформаційного обміну та безпеки.

**Аналіз останніх досліджень і публікацій.** Серед наукових робіт присвячених інформаційному забезпеченню правоохоронної діяльності варто виділити наукові доробки Ю. Битяка, В. Білоуса, О. Безпалової, С. Брателя, С. Гречанюка, Р. Калюжного, В. Колпакова, Т. Коломоєць, М. Лошицького, Є. Соболя, О. Фролової та ін. Водночас, в умовах євроінтеграції та модернізації правоохоронного сектору, вельми актуальним питанням постало дослідження міжнародно-правових засад інформаційного забезпечення правоохоронної діяльності в Україні

**Виклад основного матеріалу.** Сьогодні наша країна переживає епоху активного використання інтернету, а перехід до електронних інформаційних систем суттєво сприяє розвитку держави. Разом з цим, виникають негативні явища, такі як кіберзлочинність, включаючи (крадіжки з банкоматів шляхом встановлення спеціальних накладок, несанкціоноване списання коштів з банківських рахунків через системи дистанційного банківського обслуговування, шахрайство через інтернет-аукціони, інтернет-магазини та сайти, а також протиправний контент, що пропагує екстремізм, тероризм, наркоманію та культ насильства) [1].

У багатьох випадках пріоритетна роль інформаційного забезпечення у процесі здійснення ефективного управління в органах Національної поліції та функціонування усієї правоохоронної системи підтверджується на практиці боротьби зі злочинністю. Важлива роль системи інформаційного забезпечення управління в правоохоронних органах підтверджується на нормативному рівні, зокрема наказами та розпорядженнями МВС України [2, с. 55].

Указом Президента України від 11 травня 2023 року № 273/2023 було схвалено Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки [3], в якому закріплено цифровізацію як один із ключових векторів модернізації правоохоронної системи та реагування на виклики воєнного часу й післявоєнної відбудови. Змістовно інформаційний блок реформ сконцентрований у напрямі «Комплексна цифрова трансформація», який передбачає: (1) консолідовану поетапну цифрову трансформацію органів правопорядку та прокуратури на основі інструментів стратегічного менеджменту й кращих практик Європейського Союзу; (2) впровадження інноваційних технологічних рішень для гнучкості процесів та цифрової спроможності реагування; (3) поетапне запровадження електронної системи управління кримінальними провадженнями із модернізацією обладнання, забезпеченням сумісності ІТ-систем, безперебійності роботи, інтероперабельності та доступу всіх учасників кримінального провадження; (4) підвищення ефективності через «більшу доступність і повноту інформації» та розвиток сервісів на Єдиному державному веб-порталі електронних послуг.

Водночас реалізація зазначених орієнтирів висвітлює низку проблемних аспектів інформаційного забезпечення правоохоронної діяльності. По-перше, «консолідована» цифрова трансформація вимагає подолання фрагментарності відомчих ІТ-ландшафтів, уніфікації довідників/класифікаторів, стандартизації даних та усунення дублювання інформаційних потоків; без цього ризики «несумісності» систем і низької якості даних можуть нівелювати очікуваний ефект від електронного управління кримінальними провадженнями. По-друге, розширення доступу до державних реєстрів і баз даних потребує чіткого правового режиму: визначення підстав, меж, процедур аудиту доступів, пропорційності втручання у приватність, а також належної відповідальності за порушення режиму інформації. Поставлене Планом завдання імплементації стандартів Європейського Союзу щодо захисту персональних даних актуалізує проблему балансу між ефективністю розслідування та гарантіями прав людини. По-третє, упровадження біометричної ідентифікації, штучного інтелекту та хмарних рішень підвищує вимоги до кіберстійкості, управління ризиками, прозорості алгоритмічних рішень і запобігання дискримінаційним ефектам, що вимагає як технічних, так і процедурних запобіжників у діяльності органів правопорядку.

Зазначені процеси цифровізації та впровадження електронних інформаційних систем, з одного боку, істотно підвищують ефективність функціонування правоохоронних органів, а з іншого – зумовлюють появу нових форм і способів злочинної діяльності, які за своїм характером дедалі частіше виходять за межі національної юрисдикції. Кіберзлочинність, транснаціональні фінансові махінації, поширення протиправного контенту та використання мережевих технологій у терористичній діяльності об'єктивно потребують не лише вдосконалення внутрішніх механізмів інформаційного забезпечення правоохоронної діяльності, а й активної міжнародної взаємодії у сфері обміну, обробки та захисту інформації.

Водночас реалізація стратегічних завдань реформування органів правопорядку, орієнтованих на забезпечення безпеки людини, підвищення рівня довіри до державних інституцій і дотримання стандартів верховенства права, неможлива без урахування міжнародно-правових зобов'язань України та імплементації загальновизнаних міжнародних стандартів у сфері інформаційної безпеки та правоохоронної діяльності. Саме міжнародне право формує універсальні підходи до регламентації доступу до інформації, транскордонного інформаційного обміну, захисту персональних даних і координації дій правоохоронних органів у протидії сучасним загрозам.

У зв'язку з цим логічним і необхідним є звернення до аналізу міжнародно-правових засад інформаційного

забезпечення правоохоронної діяльності, які визначають правові рамки співробітництва держав, міжнародних організацій та правоохоронних інституцій у сфері забезпечення правопорядку в умовах цифрової трансформації та глобалізації злочинності.

На теперішній час, на рівні органів публічного управління України відбувається процес упровадження цифрових технологій, однак, як зазначає С. А. Квітка «...у сьогоднішньому вигляді структурні підрозділи (відділи, управління, сектори) нездатні задовольнити сучасні потреби щодо інформатизації органів влади та запровадження «електронного урядування» [4]. Тому, шлях України у Європейське інформаційне суспільство має супроводжуватись, на нашу думку, пошуком найкращих практик цифрової трансформації публічного управління у Європейському Союзі та адаптації його до вимог українського суспільства.

Одними із перших кроків цифрової трансформації публічного управління спрямованим на окреслення інформації як сучасного ресурсу сталого розвитку в Європейському Союзі були:

– затвердження Директиви 95/46/ЄС Європейського Парламенту та Ради Європи від 24 жовтня 1995 року «Про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних» [5];

– затвердження Директиви 97/66/ЄС Європейського Парламенту та Ради Європи від 15 грудня 1997 року «Про обробку персональних даних та захист конфіденційності в телекомунікаційному секторі» [6].

Директива 95/46/ЄС була видана для ліквідації бар'єрів на шляху вільного потоку інформації, приведення до спільного знаменника національних норм у цій сфері та забезпечення однакового захисту прав громадян у межах Співтовариства. Ця Директива охоплює «будь-яку дію чи серію дій, які здійснюються з використанням особистих даних», що позначається терміном «обробка» даних. До таких дій відносяться: збирання особистої інформації; її збереження; розголошення; та інше. Цей акт застосовується до інформації, яка обробляється автоматизованими засобами (наприклад, комп'ютерною базою клієнтів), а також до відомостей, що становлять частину неавтоматизованих «систем подачі заявок» або призначені бути ними. Доступ до таких систем може бути різним, наприклад, система подачі може містити традиційні паперові картки з інформацією, впорядкованою за алфавітом. Ця Директива не поширюється на дані, оброблені винятково з особистих міркувань чи у побутових цілях (наприклад, електронний щоденник чи файл з даними про сім'ю та друзів).

Директива 97/66/ЄС стосується захисту приватності інформації в телекомунікаціях. У цій Директиві вказано, що країни-члени повинні гарантувати секретність спілкування шляхом відповідних національних законів. Будь-яке несанкціоноване підслуховування, перехоплення або моніторинг телекомунікаційних розмов є незаконним. Також Директива встановлює, що у випадках, коли існують друковані або електронні каталоги телекомунікацій, особи мають, в принципі, право безкоштовно видаляти свою інформацію зі списку.

На додачу, 12 липня 1999 року Рішенням № 1719/1999/ЄС Європейського Парламенту та Ради Європи «Щодо низки вказівок, які включають визначення проектів, що становлять спільний інтерес, для транс'європейських мереж електронного обміну даними між адміністраціями» [7].

У статті 1 цього документу зазначено наступні цілі:

– забезпечення високого рівня взаємодії між телематичними мережами, що створені державами-членами, а також між Співтовариством та державами-членами у різних адміністративних сферах і, за потреби, з приватним сектором. Мета полягає у підтримці розбудови економічного та валютного союзу;

– узгодження зазначених мереж із загальним телематичним інтерфейсом між Співтовариством та державами-членами;

– надання значних переваг для адміністрацій держав-членів та Співтовариства завдяки оптимізації операцій, зменшенню витрат на обслуговування, прискоренню впровадження нових мереж та покращень, а також досягнення спільного безпечного та надійного обміну даними;

– поширення переваг таких мереж на промисловість Співтовариства та громадян Європейського Союзу;

– сприяння поширенню кращого досвіду та стимулювання розробки інноваційних телематичних рішень в адміністраціях.

Заходи, визначені у рішенні № 1720/1999/ЄС, спрямовані на:

– визначення технічних вимог та загальних послуг для галузевих мереж, які мають відповідати вимогам користувачів Співтовариства (стаття 4);

– забезпечення скорочення витрат на прикладні програми галузевих мереж, оптимізацію та вдосконалення технічних рішень, скорочення часу, необхідного для впровадження операційних систем, а також раціоналізацію системного обслуговування (стаття 5);

– забезпечення сумісності щодо контенту інформації, якою обмінюються в адміністративних секторах та між ними, а також із приватним сектором (стаття 6).

Стрімкий прогрес цифрових технологій і поява нових проблем у сфері інформаційної безпеки викликали потребу у модернізації законодавства у сфері інформаційного забезпечення публічних адміністрацій. Відтак, 25 травня 2018 року набрав чинності Загальний регламент про захист даних (далі – GDPR, Регламент) [8].

У першому пункті цього документа викладено такі завдання:

– Досягти значного рівня взаємодії між телематичними мережами, розгорнутими в країнах-учасницях, у різних адміністративних галузях, та, за потреби, з приватним сектором; а також між Співтовариством та країнами-учасницями для підтримки розбудови економічного та валютного союзу.

– Спрямувати ці мережі до спільного телематичного інтерфейсу між Співтовариством та країнами-учасницями.

– Забезпечити значні переваги для державних адміністрацій країн-учасниць та Співтовариства шляхом оптимізації операцій, мінімізації обслуговування, прискорення впровадження нових мереж та вдосконалень, та досягнення загального безпечного та надійного обміну даними.

– Поширити переваги таких мереж на промисловість Співтовариства та громадян Європейського Союзу.

– Сприяти розповсюдженню найкращих практик та заохочувати розробку інноваційних телематичних рішень в адміністративних структурах.

Заходи, передбачені у рішенні № 1720/1999/ЄС, зосереджені:

– На визначенні технічних вимог та загальних послуг галузевих мереж, які повинні відповідати потребам користувачів Співтовариства (стаття 4);

– На забезпеченні зменшення витрат на застосунки галузевих мереж, раціоналізації та покращенні технічних рішень, скороченні часу на впровадження операцій-

них систем та оптимізації системного обслуговування (стаття 5);

– На забезпеченні сумісності в контексті інформації, якою обмінюються в адміністративних галузях та між ними, а також з приватним сектором (стаття 6).

Динамічний розвиток цифрових технологій та виникнення нових викликів у сфері інформаційної безпеки обумовили необхідність оновлення законодавства у сфері інформаційного забезпечення державних адміністрацій. Отже, 25 травня 2018 року набув чинності Загальний регламент про захист даних (далі – GDPR, Регламент) [9], що замінив Директиву 95/46/ЄС [10] та запровадив більш жорсткі норми обробки персональних даних. GDPR має безпосередню дію в усіх країнах-членах Європейського Союзу та поширюється на обробку персональних даних громадян і резидентів Європейського Союзу незалежно від локації оператора. Документ суттєво розширив права суб'єктів даних, закріпив у ст. 25 принцип «конфіденційність за призначенням» та посилив санкції за порушення вимог захисту персональних даних. Згідно зі ст. 5 Регламенту, основоположними принципами обробки персональних даних визначено: законність, справедливість і прозорість; цільове обмеження; мінімізацію даних; точність; обмеження зберігання; цілісність і конфіденційність. У розділі 3 GDPR також закріплює низку прав суб'єктів даних: доступ до інформації, виправлення, видалення («право бути забутим»), обмеження обробки, перенесення даних і заперечення проти обробки. Документ встановлює суворі вимоги до згоди на обробку персональних даних, яка має бути добровільною, конкретною, інформованою та недвозначною [11]. Ключовим новаторством GDPR є поява посади уповноваженого із захисту даних (далі − DPO) для організацій, котрі здійснюють широкомасштабну обробку особистої інформації. DPO наглядає за дотриманням вимог Регламенту, надає консультації з питань захисту даних та взаємодіє з контролюючими органами. Також GDPR передбачає створення Європейської ради із захисту даних (European Data Protection Board) для забезпечення однакового застосування Регламенту в усіх державах-членах Європейського Союзу. Система захисту персональних даних спирається не лише на GDPR, але й на інші нормативно-правові акти. Серед них значну роль відіграє Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [12], прийнята Радою Європи у 1981 році. Конвенція встановлює міжнародні стандарти захисту персональних даних та сприяє гармонізації законодавства європейських країн. Її модернізована версія адаптувала принципи захисту даних до сучасних технологічних викликів.

Міжнародний досвід, зокрема досвід Європейського Союзу, демонструє, що успішна цифрова трансформація можлива за умови системного підходу, який включає в себе розробку чіткої стратегії, створення необхідної законодавчої бази, інвестиції в розвиток інфраструктури та людських ресурсів, а також тісну співпрацю з міжнародними партнерами. Україна може скористатися цим досвідом для прискорення своєї цифрової трансформації та наближення до європейських стандартів.

**Висновки.** Таким чином, інформаційне забезпечення правоохоронної діяльності в сучасних умовах цифровізації набуває стратегічного значення для ефективного функціонування системи правопорядку та забезпечення безпеки людини, суспільства і держави. Активне впровадження електронних інформаційних систем істотно підвищує управлінські та оперативні можливості правоохоронних органів, водночас породжуючи нові виклики, пов'язані з кіберзлочинністю, транснаціональними фінансовими правопорушеннями та поширенням протиправного контенту. Такі загрози за своєю природою виходять за межі національної юрисдикції, що зумовлює об'єктивну потребу у формуванні ефективних міжнародно-правових механізмів інформаційної взаємодії правоохоронних органів. Саме міжнародне право відіграє ключову роль у встановленні універсальних стандартів доступу до інформації, транскордонного обміну даними, захисту персональної інформації та забезпечення інформаційної безпеки.

Аналіз нормативно-правових актів Європейського Союзу засвідчив, що європейська модель інформаційного забезпечення публічних адміністрацій і правоохоронних органів базується на поєднанні технологічної інтеграції, високого рівня сумісності інформаційних систем та жорстких гарантій захисту прав людини, насамперед права на приватність і захист персональних даних. Директиви ЄС, рішення щодо транс'європейських мереж електронного обміну даними, а також Загальний регламент про захист даних (GDPR) сформували комплексну правову основу, яка забезпечує баланс між потребами безпеки та дотриманням демократичних стандартів.

Імплементація міжнародних стандартів у сфері інформаційного забезпечення правоохоронної діяльності є важливою складовою цифрової трансформації публічного управління в Україні та реалізації стратегічних завдань реформування сектору безпеки і оборони. Водночас національна практика свідчить про наявність інституційних і організаційних проблем, зокрема недостатню адаптованість існуючих структур до сучасних вимог інформатизації та електронного урядування. Відтак, подальший розвиток інформаційного забезпечення правоохоронної діяльності в Україні має ґрунтуватися на системному запозиченні та адаптації кращих міжнародних практик, удосконаленні нормативно-правової бази, підвищенні рівня міжвідомчої та міжнародної координації, а також забезпеченні реального захисту прав і свобод людини в інформаційній сфері. Реалізація цих завдань сприятиме підвищенню ефективності правоохоронної діяльності, зміцненню довіри суспільства до державних інституцій та наближенню України до європейського інформаційного простору.

**Список використаних джерел**

1. Що таке кіберполіція? *Трибуна*. 2019. URL: https://tribuna.pl.ua/news/shho-take-kiberpolitsiya/

2. Фролова О. Г. Проблеми правового регулювання інформаційно-методичного управління в органах внутрішніх справ. *Проблеми правознавства та правоохоронної діяльності*. 2002. № 1. С. 53–62.

3. 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 р. № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733

4. Квітка С. А. Державне управління формуванням партнерських відносин між владою та бізнесом у умовах соціальних перетворень. Дніпро: Грані, 2017. 268 с.

5. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *European Parliament and the Council*. Official Journal. URL: https://eur-lex.europa.eu/

6. Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector (European Parliament and the Council). Official Journal. URL: https://eur-lex.europa.eu/

7. 1719/1999/EC: Decision on a series of guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA). *European Parliament and the Council*. Official Journal. URL: https://eur-lex.europa.eu/

8. 1720/1999/EC: Decision adopting a series of actions and measures in order to ensure interoperability of and access to trans-European networks for the electronic interchange of data between administrations (IDA) (European Parliament and the Council). Official Journal. URL: https://eur-lex.europa.eu/

9. General Data Protection Regulation : Regulation (EU) of 25.05.2018 no. 2016/679. URL: https://gdpr-info.eu/

10. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» : Директива Європейського Союзу від 24.10.1995 р. № 95/46/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text

11. General Data Protection Regulation : Regulation (EU) of 25.05.2018 no. 2016/679. URL: https://gdpr-info.eu/

12. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

**References**

1. Shcho take kiberpolitsiia? [What is cyberpolice?] *Trybuna*. 2019. URL: https://tribuna.pl.ua/news/shho-take-kiberpolitsiya/ [in Ukrainian]

2. Frolova, O. H. (2002). Problemy pravovoho rehuliuvannia informatsiino-metodychnoho upravlinnia v orhanakh vnutrishnikh sprav. [Problems of legal regulation of information and methodological management in internal affairs bodies]. *Problemy pravoznavstva ta pravookhoronnoi diialnosti*. № 1. S. 53–62 [in Ukrainian].

3. Pro Kompleksnyi stratehichnyi plan reformuvannia orhaniv pravoporiadku yak chastyny sektoru bezpeky i oborony Ukrainy na 2023–2027 roky [On the Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as Part of the Security and Defense Sector of Ukraine for 2023–2027] : Ukaz prezydenta Ukrainy vid 11.05.2023 r. № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733 [in Ukrainian].

4. Kvitka, S. A. (2017). Derzhavne upravlinnia formuvanniam partnerskykh vidnosyn mizh vladoiu ta biznesom u umovakh sotsialnykh peretvoren. [State management of the formation of partnership relations between government and business in the context of social transformations]. Dnipro: Hrani [in Ukrainian].

5. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *European Parliament and the Council*. Official Journal. URL: https://eur-lex.europa.eu/

6. Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector (European Parliament and the Council). Official Journal. URL: https://eur-lex.europa.eu/

7. 1719/1999/EC: Decision on a series of guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA). *European Parliament and the Council*. Official Journal. URL: https://eur-lex.europa.eu/

8. 1720/1999/EC: Decision adopting a series of actions and measures in order to ensure interoperability of and access to trans-European networks for the electronic interchange of data between administrations (IDA) (European Parliament and the Council). Official Journal. URL: https://eur-lex.europa.eu/

9. General Data Protection Regulation : Regulation (EU) of 25.05.2018 no. 2016/679. URL: https://gdpr-info.eu/

10. Dyrektyva 95/46/IeS Yevropeiskoho Parlamentu i Rady «Pro zakhyst fizychnykh osib pry obrobtsi personalnykh danykh i pro vilne peremishchennia takykh danykh»: Dyrektyva Yevropeiskoho Soiuzu vid 24.10.1995 r. № 95/46/IeS. [Directive 95/46/EC of the European Parliament and of the Council "On the protection of individuals with regard to the processing of personal data and on the free movement of such data": European Union Directive of 24.10.1995 No. 95/46/EC]. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text [in Ukrainian].

11. General Data Protection Regulation : Regulation (EU) of 25.05.2018 no. 2016/679. URL: https://gdpr-info.eu/

12. Konventsiia pro zakhyst osib u zviazku z avtomatyzovanoiu obrobkoiu personalnykh danykh vid 28.01.1981 r. [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.1981]. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text [in Ukrainian].

**Kovalova Olha,**
Doctor of Law, Associate Professor,
Rector Assistant
*(Donetsk State University of Internal Affairs, Kropyvnytskyi)*
*ORCID: https://orcid.org/0000-0003-4555-0172*

**Batrak Kostiantyn,**
Postgraduate Student at the Research Laboratory on the Problems
of Preventing Criminal Offenses,
Educational and Scientific Institute for Training Specialists for Criminal Police Units named after E. O. Didorenko
*(Donetsk State University of Internal Affairs, Kropyvnytskyi)*
*ORCID: https://orcid.org/0009-0000-4071-4321*

# INTERNATIONAL LEGAL PRINCIPLES OF INFORMATION SUPPORT OF LAW ENFORCEMENT ACTIVITIES IN UKRAINE

*The article provides a comprehensive analysis of the international legal principles of information support of law enforcement activities in Ukraine in the context of the digital transformation of public administration and the growth of transnational security threats. The emphasis is on the fact that the active implementation of electronic information systems and the development of Internet technologies significantly increase the efficiency of law enforcement agencies, while at the same time causing the emergence of new forms of crime, in particular cybercrimes, cross-border financial offenses, the use of information resources in terrorist and extremist activities.*

*The role of information support as a key element of management in law enforcement agencies and its importance for the implementation of strategic tasks of reforming the security and defense sector of Ukraine, focused on ensuring human security, respecting rights and freedoms, and increasing trust in state institutions, is analyzed. It is substantiated that effective counteraction to modern threats requires not only the improvement of national information mechanisms, but also active international interaction in the field of information exchange, processing and protection.*

*Considerable attention is paid to the analysis of international experience in the legal regulation of information relations, in particular, the regulatory legal acts of the European Union in the field of personal data protection, telecommunications and electronic exchange of information between public administrations. The evolution of legal regulation from the European Union directives to the implementation of the General Data Protection Regulation (GDPR), which established enhanced guarantees of the rights of personal data subjects, the principles of confidentiality and liability for their violation, is revealed. The significance of the Council of Europe Convention as a universal international legal instrument for the harmonization of legislation in the field of personal data protection is separately analyzed.*

*It is concluded that the adaptation of international and European standards for information support for law enforcement activities is a necessary condition for the further digital transformation of Ukraine, increasing the efficiency of law enforcement activities and integrating the national legal system into the European legal and information space.*

***Key words:*** *law enforcement agencies, information support, law enforcement activities, international legal principles, European standards, regulatory legal acts, international cooperation, European integration.*

Дата першого надходження статті до видання: 26.02.2026
Дата прийняття статті до друку після рецензування: 24.03.2026
Дата публікації (оприлюднення) статті: 11.05.2026