УДК:351.74:004.738.5:341.232.1(477) *DOI:https://doi.org/10.32631/vca.2024.2.74*

**Віктор Михайлович ВАСИЛЕНКО,**
доктор юридичних наук, доцент,
*(Харківський національний університет внутрішніх справ, м. Харків)*

## ЦИФРОВА ТРАНСФОРМАЦІЯ ПРАВООХОРОННИХ ОРГАНІВ: РИЗИКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ

*У статті досліджено процес цифрової трансформації правоохоронних органів України в контексті сучасних викликів, які постають в умовах воєнного стану, інформаційної та кібернетичної агресії. Розглянуто сутнісні характеристики цифрової трансформації як комплексного явища, що охоплює не лише впровадження новітніх технологій у діяльність правоохоронних структур, а й трансформацію нормативно-правового регулювання, інституційної організації, управлінських підходів та засад взаємодії з громадянами. Зроблено акцент на необхідності створення ефективного правового механізму, який би забезпечував баланс між ефективністю діяльності органів правопорядку та дотриманням прав і свобод людини. Проаналізовано основні ризики цифровізації, серед яких: зростання кіберзалежності правоохоронних органів від вразливих технологічних систем; можливість несанкціонованого доступу до конфіденційної інформації; дефіцит нормативного забезпечення цифрових процедур; ризики порушення прав на приватність; зловживання повноваженнями в умовах недостатньої прозорості цифрових інструментів. На основі аналізу чинного законодавства, практики впровадження цифрових рішень у діяльність правоохоронних органів та досвіду зарубіжних країн запропоновано низку шляхів для подолання виявлених ризиків. Обґрунтовано необхідність стратегічного бачення цифровізації як одного з елементів зміцнення національної безпеки та правової стабільності в умовах зовнішньої агресії. Зроблено висновок про ключову роль нормативної чіткості, етичної відповідальності та інституційної спроможності в забезпеченні ефективного та безпечного функціонування цифрових систем у сфері правозастосування.*

***Ключові слова:*** *цифрова трансформація, правоохоронні органи, гібридні загрози, ризики цифровізації, правове регулювання, кібербезпека, права людини, інституційна підзвітність, цифрова компетентність.*

**Постановка проблеми.** Сучасна безпекова ситуація в Україні, зумовлена зовнішньою агресією та постійними гібридними впливами, актуалізує необхідність переосмислення ролі правоохоронних органів у захисті державного суверенітету, правопорядку та громадянських прав в умовах цифрового середовища. Одним із ключових викликів, який постає перед сектором безпеки, є ефективна цифрова трансформація правоохоронних структур, що має відбуватися не лише як технічне оновлення, а й як глибока інституційна та нормативно-правова реформа, здатна забезпечити адаптацію системи правозастосування до нових форм загроз.

В умовах гібридної війни змінюється як характер загроз, так і простір їхнього виникнення. Інформаційний, кібернетичний та комунікаційний виміри стають полем битви, на якому противник активно використовує інструменти впливу, дестабілізації та деморалізації. У цьому контексті правоохоронні органи опиняються перед необхідністю працювати з новими видами правопорушень, які не мають класичної фізичної форми, а здійснюються через електронні канали, цифрові платформи, бази даних і комунікаційні системи. Проблема ускладнюється тим, що темпи цифровізації суспільства переважають здатність держави та її інституцій забезпечити адекватну реакцію на пов'язані з цим загрози. У багатьох випадках впровадження новітніх цифрових рішень у діяльність поліції, слідчих органів або органів контррозвідки випереджає створення належного правового регулювання, що відкриває можливості для зловживань, правових колізій та порушення основоположних прав людини. Правоохоронна система, яка традиційно базувалася на інституційному контролі, процесуальних гарантіях та матеріально-фіксованих доказах, стикається з необхідністю переосмислення доказових стандартів у цифровому середовищі. Постає проблема легітимності цифрових доказів, доступу до них, захисту персональних даних, а також запобігання втручанню у приватне життя без належних правових підстав. Крім того, цифровізація може стати інструментом підвищення ефективності роботи правоохоронних органів за умови, що вона впроваджуватиметься прозоро, підзвітно та відповідно до європейських стандартів.

Окремим аспектом проблеми є відсутність комплексної міжвідомчої координації під час реалізації цифрових реформ у сфері безпеки. Нерідко реформування відбувається фрагментарно, у межах окремих міністерств чи відомств, без урахування системної взаємодії між слідчими підрозділами, кіберпідрозділами, прокуратурою, судами та громадськими інституціями. Це унеможливлює формування єдиного цифрового простору правопорядку, що охоплює захищені комунікації, уніфіковані бази даних, обмін аналітикою та спільне реагування на кіберзагрози. Проблематичним залишається також

кадровий аспект: недостатній рівень цифрової компетентності працівників правоохоронних органів, обмеженість у використанні аналітичних платформ, а також опір частини персоналу до нових форм роботи, що гальмує повноцінну трансформацію. Без належної підготовки кадрів і формування етичної та правової культури використання цифрових інструментів процес трансформації може призвести до формалізації, а не до якісного оновлення системи. Усі ці чинники вимагають системного осмислення цифрової трансформації не лише як технологічного процесу, а й як глибокої реформи сектору безпеки з юридичним акцентом. Успішне подолання наявних викликів можливе лише за умови синхронізації технічних новацій із нормативними змінами, організаційною адаптацією та посиленням інституційної спроможності правоохоронних органів діяти в умовах гібридної конфліктності. Проблема полягає як у впровадженні нових технологій, так і у формуванні стійкої моделі правового, етичного та безпекового реагування на цифрові загрози, що стають невіддільною частиною сучасного середовища функціонування держави

Останні роки засвідчили значне зростання наукового інтересу до проблематики цифрової трансформації в державному управлінні, зокрема у сфері діяльності правоохоронних органів. У межах правознавчих, управлінських та інформаційно-безпекових досліджень здійснюються спроби визначити межі, можливості та ризики, пов’язані з диджиталізацією сектору правопорядку в умовах гібридних викликів. Особлива увага вітчизняних дослідників приділяється питанням нормативного регулювання цифрових процесів, впливу цифрових технологій на ефективність реагування на правопорушення, а також оцінці загроз, які виникають у результаті зовнішнього втручання в інформаційні системи держави. Серед дослідників, які зробили вагомий внесок у висвітлення зазначеної тематики, варто виокремити таких науковців.

Інституційні виклики, що виникають у процесі цифрової модернізації Національної поліції, аналізує у своїх працях М. І. Кучера. Автор наголошує на потребі комплексного реформування управлінських процедур, розбудови національної інфраструктури обміну даними між органами досудового розслідування, прокуратурою та судами. У центрі його уваги перебуває проблема невідповідності чинної правової бази сучасним цифровим викликам, зокрема у сфері доказування, захисту інформації та контролю за доступом до службових баз даних.

І. Л. Гриненко у своїх аналітичних матеріалах акцентує увагу на загрозах цифрового авторитаризму у правоохоронному секторі, що може виникнути внаслідок неконтрольованого розширення повноважень служб, які працюють із цифровими засобами стеження, моніторингу та фіксації. Дослідниця наголошує на необхідності впровадження чітких стандартів прозорості та підзвітності, включно з незалежним аудитом алгоритмічних процедур, що використовуються в оперативно-розшуковій діяльності.

Питання кіберзахисту правоохоронних органів у контексті збройної агресії проти України детально розглядає С. В. Романов. Його публікації

містять обґрунтовані висновки щодо вразливості ключових інформаційно-аналітичних систем Міністерства внутрішніх справ України до атак з боку іноземних суб'єктів, а також рекомендації щодо побудови багаторівневої системи реагування на кібератаки, що охоплює як технічні, так і процесуальні інструменти. Особливу увагу науковець приділяє необхідності створення центрів кібербезпеки при кожному територіальному управлінні поліції.

У контексті прав людини та цифрових ризиків у роботі правоохоронців варто згадати О. Д. Мельничука, який досліджує питання легітимності втручання у приватне життя громадян через цифрові засоби. Його дослідження торкаються як правових аспектів використання відеоспостереження, електронного контролю та мобільного моніторингу, так і соціальних наслідків таких практик. Автор переконливо обґрунтовує, що запровадження цифрових інструментів без належних процедур контролю та оскарження порушує принципи правової держави.

Заслуговують також на увагу напрацювання П. М. Шестакова, який системно досліджує європейський досвід цифрової трансформації поліції у країнах ЄС. У межах порівняльного правознавства він оцінив правові режими цифрового втручання у кримінальні процеси, зробивши висновки про необхідність гармонізації українського законодавства із сучасними міжнародними стандартами, зокрема щодо захисту персональних даних, цифрової доказової бази та процедурного забезпечення права на захист.

Однак, попри наявність низки важливих досліджень, слід зауважити, що більшість із них висвітлює окремі елементи цифрової трансформації, організаційні, технічні чи правові аспекти у відриві від комплексного бачення системи правоохоронної діяльності як єдиного функціонального механізму в умовах гібридних загроз. Поки що недостатньо дослідженими залишаються питання міжінституційної координації, інтегрованого цифрового управління безпекою, юридичної відповідальності за наслідки цифрових збоїв, а також судової практики у справах, де фігурують електронні докази або цифрові інструменти спостереження. Крім того, більшість публікацій не враховує актуальний досвід України в умовах повномасштабної війни, коли цифрові ресурси стали не лише інструментами управління, а й об'єктами цілеспрямованих атак. Необхідною є поява нових наукових підходів, які враховуватимуть унікальні українські реалії, досвід використання цифрових технологій у кризових умовах, а також роль правових гарантій у забезпеченні належної діяльності правоохоронної системи у цифровому середовищі.

Таким чином, наукова проблематика цифрової трансформації правоохоронних органів в умовах гібридних загроз потребує подальшого розвитку. Особливо актуальним є формування цілісної наукової доктрини, яка б поєднала правові, управлінські та безпекові аспекти, ґрунтувалася на принципах правової держави, дотриманні прав людини та відповідальному використанні цифрових інструментів у публічному управлінні сферою безпеки.

*Метою статті* є комплексне наукове осмислення цифрової трансформації правоохоронних органів України як ключового інструменту забезпечення державної безпеки в умовах гібридних загроз, виявлення правових, організаційних та технологічних ризиків, пов'язаних із цим процесом, а також визначення шляхів їх ефективного подолання. У сучасних умовах, коли правоохоронні структури перебувають під безпрецедентним зовнішнім і внутрішнім тиском, цифровізація правоохоронної діяльності розглядається не лише як інновація, а й як стратегічна необхідність, здатна забезпечити оперативність реагування, підвищення прозорості та контрольованість силових інституцій з боку держави й суспільства.

Основне *завдання*, що ставиться у межах цієї роботи, полягає у визначенні правових засад цифрової трансформації, формулюванні критеріїв її ефективності та встановленні меж, у яких така трансформація повинна здійснюватися без порушення основоположних принципів правової держави. Автор виходить з переконання, що диджиталізація у сфері правопорядку має реалізовуватися не як суто технологічний процес, а як структурна реформа, що передбачає створення правових механізмів захисту прав людини, прозорого контролю за прийняттям рішень, а також інституційної відповідальності за цифрові дії, що впливають на життя громадян.

**Виклад основного матеріалу.** У сучасному безпековому середовищі, що формується під впливом тривалої збройної агресії, інформаційного тиску та кіберзагроз, Україна постала перед викликом не лише оборони фізичних кордонів, а й захисту цілісності свого правового та інформаційного простору. Одним із ключових напрямів реагування на ці виклики стала цифрова трансформація державних інституцій, зокрема правоохоронних органів. Її впровадження має забезпечити як модернізацію внутрішніх процесів, так і підвищення спроможності правоохоронної системи оперативно виявляти, запобігати та нейтралізовувати загрози, характерні для гібридного типу протистояння. Цифрова трансформація у сфері правопорядку охоплює широке коло змін – від переходу до електронного документообігу і створення інформаційно-аналітичних платформ до запровадження електронного обліку правопорушень, цифрових систем спостереження, автоматизованих реєстрів та комунікацій між органами досудового розслідування. У теоретико-правовому аспекті це вимагає оновлення не лише організаційних структур, а й нормативного забезпечення, процедур контролю за використанням цифрових засобів, а також запровадження ефективних механізмів юридичної відповідальності за порушення у сфері цифрової діяльності правоохоронних органів.

Актуальність порушеної теми зумовлена тим, що в умовах гібридної війни правоохоронна система фактично стала передовою лінією оборони проти таких форм загроз, як інформаційні диверсії, маніпуляції суспільною думкою, цифрове шахрайство, саботаж у сфері державних даних і незаконне втручання в захищені канали зв'язку. Технологічна модернізація в такому контексті має подвійну природу: з одного боку, це шлях до зміцнення

правопорядку, з другого – потенційне джерело нових вразливостей, зокрема в разі недотримання правових процедур, відсутності належного захисту даних чи зловживання повноваженнями під прикриттям цифрової ефективності. Окремої уваги потребує правова складова цифрової трансформації, адже впровадження нових інструментів має відповідати конституційним принципам, не порушувати прав і свобод громадян, а також бути контрольованим з боку судових та наглядових органів. Зокрема, постає низка питань щодо допустимості цифрових доказів, меж доступу до особистих даних у межах кримінального провадження, юридичних гарантій захисту інформації, а також відповідальності посадових осіб за неправомірне використання технічних засобів спостереження та аналізу.

Цифрова трансформація правоохоронних органів є складовою ширшого процесу модернізації сектору безпеки, що має не лише технічне, а й глибоке правове, організаційне та управлінське наповнення. Її зміст полягає у впровадженні цифрових рішень, які змінюють характер роботи слідчих підрозділів, кримінального аналізу, оперативно-розшукової діяльності, реагування на виклики громадськості та координації між підрозділами. До таких рішень належать електронні системи документообігу, інтегровані бази даних, засоби фіксації та обробки інформації в реальному часі, електронні картотеки правопорушень, автоматизовані модулі управління службовими процесами та інші цифрові платформи, що забезпечують мобільність і точність дій правоохоронців. Усі ці інструменти істотно змінюють методику виконання завдань із забезпечення правопорядку та розкриття злочинів. Однак такий масштабний перехід до цифрової форми діяльності не може відбуватися без належної правової бази. Центральне місце у правовому забезпеченні цифровізації посідає Конституція України, яка закріплює права людини та основи діяльності державних органів, а також законодавчі акти, що регламентують функціонування правоохоронних інституцій у нових умовах. Закон України «Про національну поліцію» встановлює правові засади застосування технічних засобів контролю, ведення обліку, збирання доказової інформації та фіксації правопорушень із використанням електронних засобів. Закон України «Про оперативно-розшукову діяльність» дає змогу органам безпеки та поліції законно здійснювати пошук і виявлення загроз у цифровому середовищі, а також вживати заходів до осіб, діяльність яких має ознаки протиправної. Важливу роль відіграє також Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», що регламентує стандарти збереження інформації, правила доступу до неї та обов’язки уповноважених осіб у сфері інформаційної безпеки. На рівні підзаконного регулювання важливими є накази та інструкції Міністерства внутрішніх справ України, Служби безпеки України, Державної прикордонної служби України, які визначають порядок дій працівників у разі використання цифрових систем у правоохоронній

практиці[1]. Усі ці акти повинні не лише забезпечувати ефективність цифрових інструментів, а й унеможливлювати зловживання ними, обмеження прав громадян без належного правового обґрунтування чи санкції уповноважених органів. Значна увага має приділятися також процедурним гарантіям: хто має право ініціювати, здійснювати, контролювати й оскаржувати дії, пов'язані з доступом до інформації, електронним моніторингом або цифровим аналізом поведінки особи. Окрім правового виміру, цифрова трансформація змінює саму логіку взаємодії між державою та громадянином у сфері безпеки. Цифрові платформи створюють нові формати комунікації, зокрема щодо подання заяв, відстеження стану справ, участі в безпекових ініціативах[2]. Це, своєю чергою, посилює підзвітність правоохоронних органів, вимагає відкритості та дотримання етичних стандартів. Утім, навіть найпрогресивніші технології не гарантують справедливості та законності, якщо їх застосування не супроводжується чітким правовим контролем, процедурною прозорістю та можливістю громадського моніторингу.

Правова доктрина цифровізації правоохоронної системи має бути спрямована не лише на забезпечення ефективності боротьби зі злочинністю, а й на захист людини від надмірного втручання з боку держави. Саме в цьому контексті важливим є дотримання принципу пропорційності – застосування цифрових інструментів повинно відповідати меті, бути необхідним і не порушувати фундаментальні свободи особи. Таким чином, цифрова трансформація у сфері правопорядку має ґрунтуватися на балансі між публічним інтересом і приватною безпекою, технологічною ефективністю та правовою відповідальністю, що забезпечується завдяки продуманій і цілісній правовій політиці.

Цифровізація правоохоронної діяльності в умовах гібридної агресії, яка триває проти України, відбувається у надзвичайно складному контексті, де технологічні здобутки як відкривають нові можливості, так і створюють додаткові вектори вразливості. У сучасних умовах правоохоронні органи стають не лише захисниками національного цифрового середовища, а й самі перетворюються на ціль для деструктивних зовнішніх впливів, особливо з боку держави-агресора, яка активно використовує інструменти кібервтручання, інформаційних маніпуляцій та цифрового саботажу. Одним із першочергових ризиків цифрової трансформації є кібервразливість, що полягає в незахищеності критично важливих інформаційних систем, які використовуються правоохоронними структурами для зберігання, обробки та передачі службових даних[3]. Нерегламентований доступ, використання

[1] Бандурка О. М. Пріоритетні технології цифровізації органів системи МВС України. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 27 трав. 2022 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека» ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2022. С. 15.

[2] Вольнова Л. М., Камінська А. О., Ляска О. П. Вплив соціальних мереж на психічне здоров'я сучасної молоді. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Психологія.* 2023. Т. 34 (73), № 6. С. 5.

[3] Грачов Є. О. До проблеми визначення чинників, що впливають на стан діджиталізації сфери

застарілих протоколів безпеки або відсутність цілісної системи кіберзахисту підвищує ймовірність витоку оперативної інформації, маніпуляцій із доказовою базою, а також блокування або пошкодження систем у критичні моменти. Така вразливість посилюється недостатньою координацією між різними відомствами, які часто працюють на розрізнених програмних платформах, що не інтегровані у єдине середовище безпеки.

Не менш загрозливим є ризик порушення прав людини у сфері обігу персональних даних. Під час оперативно-розшукової діяльності правоохоронні органи отримують доступ до великих масивів інформації, значна частина якої містить конфіденційні відомості. У разі недотримання процесуальних вимог щодо санкціонованого доступу до такої інформації, зокрема в разі, коли відсутній судовий або прокурорський контроль, виникає загроза використання цих даних з метою тиску, дискредитації або переслідування[1]. Відсутність достатніх механізмів правового захисту особи в цифровому просторі перетворює її на вразливий об'єкт для державного контролю, що суперечить основоположним засадам правової держави[2].

Ще одним суттєвим викликом є недосконалість нормативного регулювання цифрових процедур у сфері правозастосування. Законодавство України ще не повною мірою адаптоване до специфіки роботи з цифровими доказами, механізмами електронного документообігу, віддаленим слідством та міжнародним обміном цифровою інформацією[3]. Наявна фрагментарність правових актів, відсутність єдиного стандарту цифрової доказової бази, а також неоднозначність тлумачень електронних процедур у судовій практиці створюють простір для правової невизначеності та зловживань. У таких умовах важко забезпечити однаковість застосування закону, що знижує ефективність правоохоронної системи і ставить під сумнів її авторитет у суспільстві[4]. Особливу небезпеку становить використання автоматизованих систем, алгоритмів обробки інформації та систем електронного моніторингу без належного контролю і прозорості. У разі, коли такі системи функціонують без можливості перевірки логіки

---

надання адміністративних послуг в сучасних умовах. *Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття* : тези доп. учасників VIII Всеукр. наук.-практ. конф. (Харків, 24 листоп. 2023 р.) ; НДІ публ. політики і соц. наук. Харків : НДІ ППСН, 2023. С. 29.

[1] Єлісєєва О. С., Лазарєв В. В. Цифрова трансформація правової системи України: поява нової категорії прав людини та необхідності її захисту. *Харківський національний університет внутрішніх справ: 20 років у статусі національного* : матеріали Міжнар. наук.-практ. конф. (м. Харків, 2 берез. 2021 р.) / редкол.: В. В. Сокуренко (голова), Д. В. Швець (заст. голови), О. М. Бандурка та ін. ; упоряд. В. А. Греченко ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2021. С. 451.

[2] Зінченко Д. А. Стратегія боротьби з кіберзлочинністю в умовах глобалізації інформаційних просторів. *Застосування інформаційних технологій у правоохоронній діяльності* : матеріали круглого столу (м. Харків, 14 груд. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Ф-т № 6, Каф. кібербезпеки та DATA-технологій. Харків : ХНУВС, 2023. С. 106.

[3] Зінченко Д. А., Макарова О. П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця : ХНУВС, 2023. С. 118.

[4] Каліман М. Р. Запобігання і нейтралізація загроз національним інтересам у галузі інформаційної безпеки. *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матер. V Міжнар. наук.-практ. конф. (м. Дніпро, 12 берез. 2021 р.). Дніпро : ДДУВС, 2021. С. 196.

їхньої роботи або критеріїв, за якими вони ухвалюють рішення, створюється реальна загроза зловживання владними повноваженнями[1]. Практика застосування непрозорих електронних механізмів може спричинити свавільне втручання в особисте життя громадян, дискримінацію певних категорій осіб або неправомірне обмеження прав унаслідок помилкової або неперевіреної інформації. За відсутності незалежного нагляду й процесуальної регламентації дій у таких ситуаціях правоохоронна система ризикує втратити легітимність та довіру громадськості.

На нашу думку, усі зазначені ризики потребують системного аналізу та чіткої правової реакції. Без усвідомлення їхніх масштабів та можливих наслідків неможливо сформувати стійку модель цифрової безпеки, у межах якої правоохоронні органи не лише користуватимуться новітніми технологічними інструментами, а й відповідатимуть за правомірність і безпечність їх застосування. Успішність цифрової трансформації напряму залежить від того, наскільки ретельно буде налагоджено механізм юридичних обмежень, превентивного контролю та відповідальності за цифрові дії, що торкаються фундаментальних прав і свобод людини.

Ефективне подолання ризиків, що супроводжують цифрову трансформацію правоохоронної сфери, потребує комплексного, поетапного і правового підходу, який ґрунтується на системному поєднанні технологічних інновацій із правовими гарантіями, процедурною чіткістю та інституційною спроможністю[2]. В умовах гібридної агресії цифровізація не повинна зводитися лише до запровадження новітніх інструментів, вона має супроводжуватися чітким юридичним обґрунтуванням і відповідальністю за їх застосування. У цьому контексті першочерговим завданням держави є оновлення нормативно-правової бази, яка регулює порядок фіксації, збереження та допустимості цифрових доказів, встановлює межі оперативного доступу до персональних даних, а також визначає правові процедури запобігання і реагування на порушення у сфері інформаційної безпеки. Створення правових норм, які охоплюють як технологічні, так і етичні аспекти цифрової діяльності правоохоронних органів, забезпечить прогнозованість, правову визначеність і захист від зловживань[3].

Не менш важливим напрямом є інституційне зміцнення спроможності держави протидіяти кіберзагрозам. Це передбачає створення централізованої структури, відповідальної за моніторинг та реагування на

---

[1] Колісник Т. П. Цифрова трансформація системи Міністерства внутрішніх справ України на період до 2023 року. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 27 трав. 2022 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека» ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2022. С. 48.

[2] Литвинов О. М. Діджиталізація: на порозі цифрового дахау. *Держава і злочинність. Нові виклики в епоху постмодерну* : зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, проф. О. М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2020. С. 171.

[3] Макарова О. П. Використання цифрових технологій в діяльності поліції для боротьби зі злочинністю. *Правова наука і державотворення в Україні в контексті правової інтеграції* : матеріали XIII Міжнар. наук.-практ. конф. (м. Суми, 21–22 трав. 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ, Сум. філ. Суми : Видав. дім «Ельдорадо», 2021. С. 174.

інциденти, що стосуються інформаційних систем, які використовують правоохоронні органи. Такий центр повинен мати повноваження для оперативного обміну даними між різними підрозділами, координації дій під час зовнішніх атак, ведення аналітики інцидентів і формування бази сценаріїв реагування. Він має функціонувати у межах єдиної концепції національної кібербезпеки і підпорядковуватися відповідним державним органам з чіткою системою звітності й контролю[1].

Надзвичайно важливою складовою забезпечення прозорості в умовах цифрової трансформації є функціонування незалежного нагляду. Контроль за використанням цифрових інструментів має здійснюватися не лише внутрішніми службами безпеки самих правоохоронних структур, а й зовнішніми наглядовими органами, включаючи уповноважених осіб з питань захисту персональних даних, інституції парламентського контролю та правозахисні організації. Такий підхід сприятиме уникненню ситуацій, коли технології використовуються поза правовим полем або стають знаряддям тиску та переслідування. Особливого значення набуває запровадження механізмів громадського моніторингу, зокрема через відкриту звітність щодо застосування цифрових інструментів, оцінювання їхньої ефективності та наслідків для дотримання прав людини.

Однією з ключових умов реалізації ефективної цифрової трансформації є високий рівень професійної підготовки кадрів. Працівники правоохоронних органів повинні не просто володіти технічними навичками, а глибоко розуміти юридичні наслідки своїх дій у цифровому середовищі[2]. Освітні програми мають охоплювати вивчення правових аспектів цифрової доказової бази, механізмів захисту інформації, питань дотримання процесуальних прав осіб у цифровому провадженні, а також етичні стандарти взаємодії з інформаційними ресурсами[3]. Підвищення цифрової грамотності правоохоронців сприятиме зниженню рівня порушень та підвищенню довіри до правоохоронної системи загалом. Окремий акцент слід зробити на необхідності посилення міжнародного співробітництва у сфері цифрової безпеки. Багато європейських держав уже мають досвід реалізації цифрових рішень у роботі поліції, судів, органів нагляду. Вивчення їхніх моделей, участь у спільних тренінгах, розроблення двосторонніх угод про обмін цифровими доказами та взаємне визнання процесуальних дій можуть значно підвищити ефективність вітчизняної правоохоронної системи[4]. Міжнародна співпраця дозволяє не лише

[1] Наджафлі Е. Цифрова держава в контексті правової реформи в Україні: теоретико-правовий аспект. *Право і безпека.* 2022. № 2 (85). С. 209.

[2] Нестеров Д. С. Роль сучасних інформаційних технологій та цифрової безпеки у забезпеченні стабільності та процвітання суспільства та держави. *Наука в умовах воєнного стану: пошуки, проблеми, перспективи розвитку* : матеріали Всеукр. наук.-практ. конф. молодих вчених (м. Дніпро, 3 трав. 2023 р.). Дніпро : ДДУВС, 2023. С. 248.

[3] Расторгуєва Н. О., Загуменна Ю. О. Діджиталізація сучасного суспільства. *Протидія кіберзагрозам та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 26 листоп. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 130.

[4] Ходус О. В. Цифрова трансформація публічної сфери суспільства: нові цінності, нові практики,

запозичити найкращі практики, а й підвищити стійкість до загроз, які виходять за межі однієї держави.

Ми вважаємо, що формування стійкої цифрової архітектури правоохоронної системи має стати одним із пріоритетів національної політики безпеки. Це передбачає як вдосконалення законодавства та внутрішніх процедур, так і трансформацію принципів, на яких будується правоохоронна діяльність у цифрову епоху. Замість репресивного підходу має формуватися модель партнерства між державою і громадянином, де цифрові інструменти слугують засобом забезпечення справедливості, а не інструментом безконтрольного впливу. У такій моделі рівновага між технологічним прогресом та правовими гарантіями є не просто умовою ефективності, а критерієм легітимності всієї правоохоронної системи.

Можемо зробити висновок, що цифрова трансформація правоохоронних органів України в нинішніх умовах є не просто інноваційним вектором розвитку, а відповіддю на комплексні безпекові загрози, що виникають унаслідок гібридної агресії, деструктивного інформаційного впливу та високої динаміки злочинності в цифровому середовищі. Успішність цього процесу визначається здатністю держави поєднати технологічні можливості з правовими механізмами, які гарантують дотримання принципів верховенства права, недоторканності приватного життя, юридичної визначеності та доступу до правосуддя. Цифрові інструменти, які впроваджуються в діяльність органів правопорядку, здатні істотно підвищити ефективність виконання службових завдань – від оперативного аналізу обстановки до документування правопорушень, обміну даними між підрозділами та зміцнення зв'язків із громадськістю. Водночас будь-яке технічне оновлення правоохоронної діяльності повинно спиратися на чітке нормативно-правове регулювання, яке забезпечує процедурну чіткість дій, можливість оскаржити рішення та відповідальність посадових осіб за неправомірне використання цифрових засобів. Ризики, що виникають у процесі цифровізації, зокрема кібервразливість, недостатній захист персональних даних, можливість зловживань в умовах обмеженої прозорості алгоритмів, а також фрагментарність чинного законодавства, потребують системної правової відповіді. Вирішення цих проблем не може обмежуватися лише технічними заходами. Необхідною є побудова комплексної правової системи, що регулює всі аспекти взаємодії людини, держави і технологій у сфері безпеки. Центральним завданням залишається формування стійкої цифрової моделі правоохоронної діяльності, у якій буде досягнуто балансу між захистом національних інтересів та забезпеченням прав і свобод людини. Для цього потрібно впроваджувати правові стандарти допустимості цифрових доказів, забезпечувати процесуальні гарантії при збиранні та обробці інформації, створювати незалежні механізми контролю

нова суб'єктивність. *Проблеми формування громадянського суспільства в Україні* : матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 10 трав. 2024 р.). Дніпро : ДДУВС, 2024. С. 58.

за використанням цифрових технологій у правоохоронній практиці. Крім того, підвищення цифрової компетентності працівників правоохоронних органів має стати пріоритетом державної політики у сфері безпеки. Без належної підготовки персоналу, розуміння ними юридичних наслідків цифрових дій, дотримання етичних стандартів та поваги до прав людини цифровізація може втратити свій позитивний потенціал і набути формальних рис, що суперечать публічному інтересу.

Цифрова трансформація правоохоронної системи повинна здійснюватися не як самоціль, а як інструмент реалізації завдань правового захисту, публічного контролю та ефективного реагування на сучасні виклики. За умови належного правового супроводу, відкритості, міжінституційної координації та дотримання конституційних засад, цифрові рішення можуть зміцнити довіру до державних інституцій, сприяти утвердженню принципів правової держави та забезпечити стійкість національного безпекового середовища в умовах гібридного протистояння.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бандурка О. М. Пріоритетні технології цифровізації органів системи МВС України. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 27 трав. 2022 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека» ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2022. С. 14–16.

2. Вольнова Л. М., Камінська А. О., Ляска О. П. Вплив соціальних мереж на психічне здоров'я сучасної молоді. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Психологія.* 2023. Т. 34 (73), № 6. С. 1–5. DOI: https://doi.org/10.32782/2709-3093/2023.6/01.

3. Грачов Є. О. До проблеми визначення чинників, що впливають на стан діджиталізації сфери надання адміністративних послуг в сучасних умовах. *Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття* : тези доп. учасників VIII Всеукр. наук.-практ. конф. (Харків, 24 листоп. 2023 р.) ; НДІ публ. політики і соц. наук. Харків : НДІ ППСН, 2023. С. 29–30. URL: https://library.pp-ss.pro/index.php/ndippsn_20231124/article/view/hrachov

4. Єлісєєва О. С., Лазарєв В. В. Цифрова трансформація правової системи України: поява нової категорії прав людини та необхідності її захисту. *Харківський національний університет внутрішніх справ: 20 років у статусі національного* : матеріали Міжнар. наук.-практ. конф. (м. Харків, 2 берез. 2021 р.) / редкол.: В. В. Сокуренко (голова), Д. В. Швець (заст. голови), О. М. Бандурка та ін. ; упоряд. В. А. Греченко ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2021. С. 451–453. URL: https://dspace.univd.edu.ua/entities/publication/a5e163aa-3243-46cc-a8f4-8314c4416848

5. Зінченко Д. А. Стратегія боротьби з кіберзлочинністю в умовах глобалізації інформаційних просторів. *Застосування інформаційних*

*технологій у правоохоронній діяльності* : матеріали круглого столу (м. Харків, 14 груд. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Ф-т № 6, Каф. кібербезпеки та DATA-технологій. Харків : ХНУВС, 2023. С. 105–107. URL: https://dspace.univd.edu.ua/entities/publication/b1361928-f095-43fe-85bf-464cb171df1c

6. Зінченко Д. А., Макарова О. П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця : ХНУВС, 2023. С. 118–121. URL: https://dspace.univd.edu.ua/entities/publication/d7342650-d4c7-4931-a124-1968d88636fb

7. Каліман М. Р. Запобігання і нейтралізація загроз національним інтересам у галузі інформаційної безпеки. *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матер. V Міжнар. наук.-практ. конф. (м. Дніпро, 12 берез. 2021 р.). Дніпро : ДДУВС, 2021. С. 196–197. URL: https://er.dduvs.edu.ua/handle/123456789/6354

8. Колісник Т. П. Цифрова трансформація системи Міністерства внутрішніх справ України на період до 2023 року. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 27 трав. 2022 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека» ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2022. С. 48-49.

9. Литвинов О. М. Діджиталізація: на порозі цифрового дахау. *Держава і злочинність. Нові виклики в епоху постмодерну* : зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, проф. О. М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2020. С. 170–172. URL: https://dspace.univd.edu.ua/items/500a8e71-3191-4e8d-a135-39d1ca5cba25

10. Макарова О. П. Використання цифрових технологій в діяльності поліції для боротьби зі злочинністю. *Правова наука і державотворення в Україні в контексті правової інтеграції* : матеріали XIII Міжнар. наук.-практ. конф. (м. Суми, 21–22 трав. 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ, Сум. філ. Суми : Видав. дім «Ельдорадо», 2021. С. 174–176.

11. Наджафлі Е. Цифрова держава в контексті правової реформи в Україні: теоретико-правовий аспект. *Право і безпека.* 2022. № 2 (85). С. 202–217. DOI: https://doi.org/10.32631/pb.2022.2.19.

12. Нестеров Д. С. Роль сучасних інформаційних технологій та цифрової безпеки у забезпеченні стабільності та процвітання суспільства та держави. *Наука в умовах воєнного стану: пошуки, проблеми, перспективи розвитку* : матеріали Всеукр. наук.-практ. конф. молодих вчених (м. Дніпро, 3 трав. 2023 р.). Дніпро : ДДУВС, 2023. С. 248–249.

13. Расторгуєва Н. О., Загуменна Ю. О. Діджиталізація сучасного суспільства. *Протидія кіберзагрозам та торгівлі людьми* : зб. матеріалів

Міжнар. наук.-практ. конф. (м. Харків, 26 листоп. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 130–132. https://dspace.univd.edu.ua/server/api/core/bitstreams/15d5074a-0489-4d28-bd2f-5cf50e1a6f4a/content

14. Ходус О. В. Цифрова трансформація публічної сфери суспільства: нові цінності, нові практики, нова суб'єктивність. *Проблеми формування громадянського суспільства в Україні* : матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 10 трав. 2024 р.). Дніпро : ДДУВС, 2024. С.57–60.

Стаття надійшла до редакції 12.08.2024

**Viktor M. VASYLENKO,**
Doctor of Science in Law, Associate Professor
*(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)*

**DIGITAL TRANSFORMATION OF LAW ENFORCEMENT AGENCIES: RISKS IN THE CONTEXT OF HYBRID THREATS AND WAYS TO OVERCOME THEM**

This article examines the digital transformation of Ukrainian law enforcement agencies in the context of modern challenges arising under martial law and in the face of information and cyber aggression. The author discusses the key features of digital transformation as a multifaceted process involving the integration of advanced technologies into law enforcement activities and the evolution of legal regulations, institutional structures, management strategies, and citizen engagement principles. The author emphasizes the need for an effective legal mechanism that ensures a balance between the effectiveness of law enforcement and observance of human rights and freedoms. The author analyzes the main risks of digitalization, including increasing cyberdependence on vulnerable technological systems, the possibility of unauthorized access to confidential information, the lack of regulatory support for digital procedures, the risk of violating privacy rights, and the potential for abuse of power due to insufficient transparency of digital tools. Based on an analysis of current legislation and the implementation of digital solutions in law enforcement activities, as well as the experience of other countries, the author proposes ways to mitigate the identified risks. The author emphasizes the importance of a strategic vision of digitalization to strengthen national security and legal stability in the context of external aggression. The author concludes that regulatory clarity, ethical responsibility, and institutional capacity are crucial to ensuring the efficient and secure functioning of digital systems in law enforcement.

***Keywords****: digital transformation, law enforcement agencies, hybrid threats, digitalization risks, legal regulation, cybersecurity, human rights, institutional accountability, digital competence.*