2026 년 3월 13일;
서울, 대한민국

섹션 6.
LAW AND INTERNATIONAL LAW

DOI 10.36074/logos-13.03.2026.012

МІЖНАРОДНІ ПІДХОДИ ТА КРАЩІ ПРАКТИКИ ЦИФРОВІЗАЦІЇ У СФЕРІ РОЗБУДОВИ ДОБРОЧЕСНОСТІ В ОБОРОННОМУ СЕКТОРІ

Калітник Максим Сергійович[1], Шевчук Андрій Олександрович[2]

1. начальник відділу наукового центру проблем виховання доброчесності та запобігання корупції у секторі безпеки та оборони
Національний університет оборони України, УКРАЇНА
ORCID ID: 0000-0002-7897-9138

2. науковий співробітник наукового центру проблем виховання доброчесності та запобігання корупції у секторі безпеки та оборони
Національний університет оборони України, УКРАЇНА
ORCID ID: 0000-0003-2838-0159

У сучасних умовах цифрова трансформація державного управління дедалі більше розглядається як один із ключових інструментів підвищення прозорості, підзвітності та ефективності публічних інституцій. Особливого значення цей процес набуває у секторі безпеки та оборони, де складність управлінських процедур, значні обсяги фінансових ресурсів і обмежений рівень відкритості створюють підвищені корупційні ризики. Міжнародна практика свідчить, що використання цифрових технологій — зокрема систем електронного управління, аналізу великих масивів даних та автоматизованого моніторингу управлінських процесів — може істотно знизити можливості для зловживань і забезпечити системне підвищення рівня інституційної доброчесності.

Водночас, попри значну кількість досліджень, присвячених антикорупційній політиці та цифровій трансформації державного управління, питання використання цифрових технологій як інструменту розбудови доброчесності саме в оборонному секторі залишається недостатньо дослідженим. Зокрема, потребує подальшого наукового аналізу досвіду впровадження цифрових інструментів управління ризиками, алгоритмічного моніторингу контрактних процедур, систем управління даними та цифрового комплаєнсу у сфері оборонного управління.

Метою даних тез є узагальнення міжнародних підходів та кращих практик цифровізації, що застосовуються для підвищення рівня доброчесності в оборонному секторі, а також визначення ключових напрямів їх можливого застосування у процесі цифрової трансформації системи управління сектором безпеки та оборони України.

Цифрова трансформація оборонного сектору в сучасних умовах розглядається міжнародною спільнотою як структурний інструмент забезпечення прозорості, підзвітності та інституційної стійкості. На відміну від традиційних контрольних механізмів, цифровізація дозволяє інтегрувати принципи доброчесності безпосередньо в архітектуру управлінських процесів, мінімізуючи вплив людського фактору та дискреційних рішень. У цьому контексті цифрові технології сприяють формуванню нової моделі управління публічними ресурсами, де контроль за використанням коштів та прийняттям управлінських рішень здійснюється на основі аналізу даних і автоматизованих алгоритмів.

Ключову роль у формуванні міжнародних стандартів з розбудови доброчесності відіграє NATO, зокрема через програму Building Integrity (BI), яка визначає доброчесність як складову оборонної спроможності держави [1]. Підхід НАТО передбачає інституційну самооцінку вразливостей, зовнішню експертну перевірку, впровадження стандартів прозорості та системне навчання персоналу. Важливо, що цифрові інструменти в цій моделі виконують не допоміжну, а системоутворюючу функцію — забезпечують електронний аудиторський слід, автоматизований моніторинг та управління ризиками.

Одним із найбільш уразливих до корупційних ризиків напрямів є оборонні закупівлі. За висновками Organisation for Economic Co-operation and Development, повна цифровізація циклу закупівель (від планування до виконання контракту) істотно знижує можливості для зловживань шляхом забезпечення прозорості процедур та зменшення неформальних контактів між замовником і постачальником [2]. Застосування аналітики даних, автоматизованого ризик-скорингу та інтеграції закупівельних і фінансових систем дозволяє переходити від формального контролю до превентивного управління ризиками.

Дослідження практик моніторингу публічних закупівель свідчать, що цифрові системи можуть виявляти ранні ознаки корупційних ризиків. До таких індикаторів належать аномалії ціноутворення, несподівані стрибки витрат, нерегулярні процедури тендерів, використання єдиного постачальника або непрозорі фінансові перекази підрядникам. Використання алгоритмів аналізу даних дозволяє виявляти такі сигнали на ранніх етапах реалізації контрактів та оперативно реагувати на потенційні порушення.

World Bank наголошує на потенціалі використання цифрових технологій — зокрема алгоритмів виявлення аномалій та інструментів аналізу великих масивів даних — для своєчасного ідентифікування підозрілих операцій [5]. Такий підхід сприяє формуванню risk-based governance, коли ресурси внутрішнього контролю спрямовуються насамперед на процеси з підвищеним рівнем ризику.

Важливим теоретичним елементом сучасної цифрової антикорупційної політики є концепція алгоритмічної підзвітності (algorithmic accountability). Її сутність полягає у використанні автоматизованих систем аналізу даних для моніторингу управлінських рішень та фінансових операцій із можливістю перевірки логіки алгоритмів, що приймають або оцінюють такі рішення. У сфері оборонного управління алгоритмічна підзвітність дозволяє здійснювати постійний моніторинг контрактних процедур, бюджетних транзакцій і логістичних операцій, виявляючи аномалії на основі попередньо визначених індикаторів ризику. На відміну від традиційних механізмів контролю, що залежать від людського фактору, алгоритмічні системи здатні обробляти значні масиви даних у режимі реального часу, що суттєво підвищує ймовірність раннього виявлення корупційних схем.

Важливе значення має впровадження цифрових систем комплаєнсу та внутрішнього контролю. Рекомендації United Nations Office on Drugs and Crime передбачають використання технологічних рішень для моніторингу конфлікту інтересів, управління повідомленнями про правопорушення, створення цифрових реєстрів ризиків та забезпечення прозорості прийняття рішень [4]. У сучасних умовах такі механізми дедалі частіше інтегруються у концепцію цифрового комплаєнсу (Digital Compliance), яка передбачає використання алгоритмів аналізу даних для постійного моніторингу фінансових і контрактних операцій.

Окремим напрямом міжнародної практики є управління даними (data governance) та баланс між режимністю інформації й підзвітністю. Дослідження Transparency International Defence and Security підкреслюють необхідність впровадження чіткої класифікації інформації, рольових моделей доступу, журналювання дій користувачів і цифрового аудиту [3]. Водночас ефективність таких механізмів значною мірою залежить від доступності відкритих даних, регулярного аудиту та забезпечення простежуваності інформаційних потоків. Дані повинні бути придатними для машинного зчитування, доступними без обмежень та публікуватися відповідно до встановлених графіків.

Показовим прикладом використання цифрових технологій для запобігання корупції є система електронних закупівель KONEPS у Південній Кореї, яка використовує алгоритми аналізу даних для автоматичного

виявлення аномалій у контрактах. Система дозволяє ідентифікувати випадки завищення цін, участі фіктивних компаній або інших ознак зловживань на ранніх етапах укладання контрактів, що значно підвищує ефективність державного контролю.

Таким чином, міжнародні підходи свідчать про те, що цифровізація оборонного сектору виступає структурним механізмом забезпечення доброчесності, прозорості та підзвітності управлінських процесів. Найбільш ефективними напрямами є цифрова трансформація оборонних закупівель, управління фінансами, кадрових процедур та внутрішнього контролю на основі ризик-орієнтованої моделі. Впровадження інтегрованих інформаційних систем, формування цифрового сліду рішень, автоматизація контрольних тригерів та управління доступом до даних створюють інституційні запобіжники корупції та підвищують стійкість оборонних відомств.

Наукова новизна дослідження полягає у концептуалізації цифровізації оборонного сектору не лише як інструменту адміністративної модернізації, а як системного механізму інституційного забезпечення доброчесності. У роботі обґрунтовується підхід до розбудови цифрової екосистеми доброчесності, що поєднує алгоритмічну підзвітність, ризик-орієнтоване управління та інтегроване управління даними. Такий підхід дозволяє трансформувати антикорупційну політику від моделі постфактумного реагування до превентивної моделі управління ризиками на основі аналізу даних.

Отримані результати можуть слугувати теоретичною основою для подальшого дослідження імплементації міжнародних практик цифровізації у секторі безпеки та оборони України, а також для розробки концептуальних засад цифрової трансформації системи забезпечення доброчесності у Міністерстві оборони України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] NATO. (2023). *Building integrity programme: Practical tools and self-assessment framework*. NATO;
[2] Organisation for Economic Co-operation and Development. (2025). *Digital transformation of public procurement*. OECD Publishing;
[3] Transparency International Defence and Security. (2024). *Information governance and integrity in defence sectors*. Transparency International Defence and Security;
[4] United Nations Office on Drugs and Crime. (2022). *Guidelines on the use of technology to combat corruption in public procurement*. UNODC;
[5] World Bank. (2020). *Disruptive technologies in public procurement*. World Bank.