УДК 351:354:343.352
DOI https://doi.org/10.32782/2310-9653-2026-1.13

А. Поздєєв, аспірант кафедри публічного управління та митного адміністрування Університету митної справи та фінансів
https://orcid.org/0009-0009-7411-4194

О. О. Крітенко, кандидат наук з державного управління, доцент, доцент кафедри публічного управління та митного адміністрування Університету митної справи та фінансів
https://orcid.org/0000-0001-9582-3007

РОЛЬ ІНТЕГРОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ У ЗАБЕЗПЕЧЕННІ ПРОЗОРОСТІ ПУБЛІЧНОЇ СЛУЖБИ ТА МІНІМІЗАЦІЇ КОРУПЦІЙНИХ РИЗИКІВ

У статті досліджується фундаментальна роль інтегрованих інформаційних систем (ІІС) у процесі трансформації публічної служби України, забезпеченні її прозорості та нейтралізації корупціогенних факторів. Актуальність дослідження зумовлена безальтернативністю курсу України на європейську інтеграцію в умовах воєнного стану, що вимагає переходу від застарілого паперового документообігу до парадигми управління на основі даних (data-driven governance). У роботі ідентифіковано ключові вразливості традиційної моделі державного управління, які генерують корупційні ризики: надмірні дискреційні повноваження посадових осіб, інформаційну асиметрію, ручне управління даними та непрозорість кадрових і фінансових процесів.

Особливу увагу приділено функціональним можливостям Інформаційної системи управління людськими ресурсами (HRMIS) та системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта». Доведено, що їх впровадження дозволяє змінити філософію державного управління з «довіри до чиновника» на «довіру до алгоритму» (Trust in Data). Проаналізовано антикорупційний ефект автоматизації нарахування заробітної плати, автоматичного відстеження конфлікту інтересів через інтеграцію з реєстрами НАЗК та фіксації цифрового сліду (Audit Trail).

У статті також досліджено специфічні виклики процесу цифровізації: зростання кіберзагроз та інституційний опір (цифровий саботаж) з боку частини бюрократичного апарату. Запропоновано комплекс стратегічних рекомендацій для побудови стійкої антикорупційної інфраструктури, серед яких стовідсоткове підключення органів влади до систем інтероперабельності та впровадження алгоритмів штучного інтелекту (red flags) для превентивного виявлення зловживань.

Ключові слова: *публічна служба, корупційні ризики, інтегровані інформаційні системи, HRMIS, інтероперабельність, система «Трембіта», антикорупційний комплаєнс, електронне урядування, data-driven управління.*

A. Pozdieiev, O. O. Krytenko. The role of integrated information systems in ensuring transparency of public service and minimizing corruption risks

The article investigates the fundamental role of integrated information systems (IIS) in transforming the public service of Ukraine, ensuring its transparency, and neutralizing corruption-generating factors. The relevance of the study is driven by the lack of alternatives to Ukraine's European integration course amidst martial law, which requires a transition from outdated paper-based document management to a data-driven governance paradigm. The paper identifies key vulnerabilities of the traditional public administration model that generate corruption risks: excessive discretionary powers of officials, information asymmetry, manual data manipulation, and non-transparent HR and financial processes.

Special attention is paid to the functionality of the Human Resource Management Information System (HRMIS) and the "Trembita" system of electronic interaction of state electronic information resources. It has been proven that their implementation allows changing the philosophy of public administration from "trust in the official" to "trust in the algorithm" (Trust in Data). The anti-corruption effect of payroll automation, automatic tracking of conflicts of interest through integration with NACP registers, and recording of the digital footprint (Audit Trail) are analyzed.

The article also explores specific challenges of the digitalization process: the growth of cyber threats and institutional resistance (digital sabotage) from a part of the bureaucratic apparatus. A set of strategic recommendations for building a resilient anti-corruption infrastructure is proposed, including 100% connection of government authorities to interoperability systems and the implementation of artificial intelligence algorithms (red flags) for the preventive detection of abuses.

Key words: *public service, corruption risks, integrated information systems, HRMIS, interoperability, Trembita system, anti-corruption compliance, e-governance, data-driven governance.*

Постановка проблем. У контексті набуття Україною статусу кандидата на вступ до Європейського Союзу, реформування публічної служби на засадах доброчесності, прозорості та підзвітності перетворилося з внутрішньополітичного завдання на один із ключових маркерів інституційної зрілості держави на міжнародній арені.

Традиційні адміністративно-каральні методи боротьби з корупцією демонструють свою обмеженість, оскільки вони спрямовані на боротьбу з наслідками, а не з першопричинами зловживань. Державна антикорупційна програма на 2023–2025 роки чітко артикулює, що цифровізація процесів та мінімізація людського фактору є найбільш дієвими превентивними інструментами запобігання корупційним правопорушенням.

Проблема полягає в тому, що традиційні (переважно паперові або локально-цифрові) форми управлінської діяльності генерують системні корупційні ризики: від маніпуляцій з кадровими призначеннями до приховування публічної інформації. Вирішення цієї проблеми неможливе шляхом точкових змін; воно вимагає докорінної реінжинірингової трансформації – впровадження інтегрованих інформаційних систем (ІІС), які здатні забезпечити перехід до парадигми управління на основі даних (data-driven governance).

Аналіз останніх досліджень і публікацій. Проблематика впровадження інформаційно-комунікаційних технологій у державне управління та їх вплив на інституційну спроможність держави перебуває в центрі уваги багатьох вітчизняних науковців. Базові дефініції та концептуальні засади цифрового врядування в Україні закладено у працях В. Куйбіди та О. Карпенка [2]. Механізми публічного управління у сфері цифрових трансформацій ґрунтовно досліджувалися Т. Биркович [3] співавторами зі, які акцентували увагу на необхідності комплексного підходу до реінжинірингу управлінських процесів.

Сучасний стан та перспективи розвитку цифровізації публічного управління в умовах новітніх викликів розкрито в роботі Н. Бондарчук та Н. Дуброової [4], де доведено, що цифровізація покликана знизити адміністративні бар'єри та максимально усунути вплив суб'єктивних чинників в управлінні. 'Інституційні аспекти цифрової трансформації в умовах євроінтеграції глибоко проаналізовані А. Рачинським та О. Титаренком [5]. Крім того, інноваційні підходи до антикорупційної діяльності, зокрема щодо впровадження штучного інтелекту для мінімізації корупційних ризиків, розглядаються у новітніх дослідженнях Т. Штерми, А. Луківського та С. Луківського [6].

Виділення невирішених раніше частин загальної проблеми. Незважаючи на ґрунтовні дослідження феномену електронного урядування, більшість праць зосереджені на загальнотеоретичних аспектах цифровізації або на питаннях надання електронних послуг громадянам (фронт-офіс). Натомість недостатньо вивченим залишається інструментальний потенціал внутрішніх інтегрованих інформаційних систем (бек-офісу), таких як HRMIS та системи інтероперабельності, саме як механізмів антикорупційного комплаєнсу на публічній службі. В умовах воєнного стану та жорстких вимог ЄС щодо підзвітності державного апарату, питання переходу від фрагментарної автоматизації до створення екосистеми «управління на основі даних» (data-driven governance) потребує додаткового науково-практичного обґрунтування.

Мета статті полягає у теоретико-практичному обґрунтуванні ролі інтегрованих інформаційних систем як ключового механізму забезпечення прозорості публічної служби та усунення корупціогенних факторів, а також у розробці пропозицій щодо подолання інституційних бар'єрів на шляху їх впровадження в органах державної влади України.

Виклад основного матеріалу дослідження. Генезис корупціогенних ризиків у традиційній архітектурі публічної служби має свої особливості. Традиційна модель публічного управління, що історично сформувалася на засадах паперового документообігу та ієрархічної бюрократії, за своєю природою містить системні вразливості, які генерують корупційні ризики. Як слушно зазначають Н. Бондарчук та Н. Дуброва [4], головною проблемою традиційної взаємодії є наявність значної кількості адміністративних бар'єрів та критична залежність результату управлінського рішення від суб'єктивних чинників, пов'язаних із посадовою особою.

Аналіз функціонування публічної служби в її доцифровому або «частково цифровому» (коли комп'ютери використовуються лише як друкарські машинки) стані дозволяє виокремити три ключові групи корупціогенних факторів:

По-перше, інформаційна асиметрія та ручне управління даними. У традиційній системі чиновник виступає монополістом у володінні суспільно важливою інформацією. Це створює умови для так званої «корупції доступу», коли посадові особи можуть штучно приховувати, викривляти або знищувати службову інформацію, маніпулювати чергами або строками надання адміністративних послуг. Відсутність єдиної інтегрованої бази даних дозволяє існувати дублюванню інформації, що робить практично неможливим оперативний зовнішній аудит дій службовця.

По-друге, непрозорість кадрових (HR) та фінансових процесів. Відсутність єдиної системи обліку людських ресурсів породжує високий рівень суб'єктивізму. В українській практиці це роками призводило до ручного управління фондом оплати праці: непрозорого та нерівномірного призначення премій (часто за принципом лояльності до керівника, а не на основі KPI), стихійного просування по службі, а також створення умов для існування «мертвих душ» (фіктивно оформлених працівників, чию заробітну плату привласнювало керівництво).

По-третє, надмірні дискреційні повноваження. Відсутність жорстких алгоритмізованих процедур у традиційному управлінні надає можливість посадовцям різного рівня на власний розсуд трактувати норми закону. Дискреція сама по собі є необхідним елементом управління, проте без цифрових «запобіжників» і систем відстеження історії прийняття рішень (audit trail) вона швидко трансформується у можливість вимагання неправомірної вигоди за прийняття «вигідного» для суб'єкта звернення рішення.

Подолання цих ризиків виключно адміністративно-каральними методами (шляхом посилення відповідальності) є малоефективним. Зміна архітектури публічного управління потребує переходу до парадигми «довіри до алгоритму» (Trust in Data) через розгортання інтегрованих інформаційних систем, які не просто фіксують діяльність чиновника, а алгоритмічно унеможливлюють корупційне діяння.

Для зменшення впливу корупційних ризиків на публічній службі використовується Інформаційна система управління людськими ресурсами (далі HRMIS) як інструмент антикорупційного комплаєнсу в управлінні персоналом. Загалом, ця система у державному секторі традиційно розглядалася виключно як інструмент кадрового менеджменту. Проте, як зазначають фахівці Національного агентства України з питань державної служби (далі НАДС) та дослідники у сфері кадрової політики (зокрема, С. Хаджирадєва та В. Сороко [7]), в українських реаліях HRMIS набула чітко вираженої антикорупційної функції. Відповідно до Концепції, затвердженої Кабінетом Міністрів України [8], ця система є єдиною централізованою базою даних про державних службовців, що кардинально змінює логіку управління персоналом.

Антикорупційний потенціал HRMIS реалізується через три базові механізми, які усувають людський фактор із процесів прийняття рішень (табл. 1).

Отже, автоматизація нарахування заробітної плати (Payroll) позбавляє керівників можливості фінансового шантажу підлеглих або безпідставного преміювання лояльних співробітників. Відстеження конфлікту інтересів відбувається алгоритмічно, а безперервний цифровий слід (Audit Trail) виступає надійним доказовим інструментом для антикорупційних органів у разі проведення розслідувань.

Якщо HRMIS забезпечує внутрішню прозорість державного органу, то система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» (побудована на естонській технології X-Road) гарантує прозорість міжвідомчої взаємодії та надання послуг громадянам [9].

Згідно з аналітичними звітами проєкту міжнародної технічної допомоги USAID / UK aid «Прозорість та підзвітність у державному управлінні та послугах» (TAPAS), саме відсутність інтероперабельності (здатності баз даних «спілкуватися» між собою) історично була головним джерелом побутової корупції в Україні. Громадянин змушений був виконувати роль «кур'єра» між державними органами, збираючи паперові довідки, що створювало ідеальне середовище для вимагання хабарів за прискорення процесу. Тобто традиційна паперова модель – генерує можливість корупційних діянь. Впровадження системи «Трембіта» докорінно змінює цю архітектуру – вона усуває передумови корупції (рис. 1) та має чіткий алгоритм: *Громадянин → Дія → Трембіта → Реєстри*, що виключає вплив чиновника – посередника (рис 1)

З точки зору антикорупційного комплаєнсу, система «Трембіта» забезпечує такі безпрецедентні результати:

1. Знищення монополії чиновника на прийняття рішень. У традиційній моделі посадова особа одноосібно вирішувала, чи приймати довідку від громадянина. В інтегрованій моделі дані верифікуються криптографічно між серверами державних органів: якщо система підтверджує наявність права на послугу, чиновник не має технічної можливості відмовити.

2. Мінімізація фізичного контакту. «Трембіта» є бек-енд основою для порталу «Дія». Автоматичний обмін даними дозволяє надавати послуги проактивно та дистанційно, повністю виключаючи фізичний контакт між суб'єктом звернення та посадовою особою, що є класичним методом усунення умов для корупційної угоди.

Таким чином, інтероперабельність перестає бути суто технічним IT-терміном і перетворюється на базовий інститут превентивної антикорупційної політики держави.

Попри беззаперечну антикорупційну ефективність, впровадження інтегрованих інформаційних систем у систему публічного управління України стикається з двома фундаментальними групами викликів: зовнішніми (технологічними) та внутрішніми (інституційними) (рис. 2).

Таблиця 1

Порівняльний аналіз традиційного кадрового обліку та системи HRMIS у контексті антикорупційних запобіжників

Процес / Критерій	Традиційна модель (паперова/ локальна)	Модель на базі HRMIS (Data-driven)	Антикорупційний ефект
Нарахування заробітної плати (Payroll)	Ручне формування табелів. Розподіл премій на суб'єктивний розсуд керівника.	Автоматизований розрахунок на основі електронного табелювання та об'єктивних KPI.	Унеможливлення маніпуляцій з фондом оплати праці, ліквідація явища «мертвих душ».
Перевірка конфлікту інтересів	Здійснюється формально, постфактум, часто покладається на сумлінність самого службовця.	Автоматичний крос-чек баз даних (інтеграція з реєстрами НАЗК) на етапі підготовки кадрового наказу.	Превентивне блокування призначень за наявності прямого підпорядкування близьких осіб.
Історія змін документів (Audit Trail)	Можливість підміни сторінок в особовій справі, зміна наказів «заднім числом».	Будь-яка зміна фіксується незмінним цифровим слідом (час, IP-адреса, кваліфікований електронний підпис).	Повна підзвітність кадровиків та керівників; неможливість приховування неправомірних дій.

Джерело: складена автором

 ISSN 2521-6503 (Print), 2664-6145 (Online)

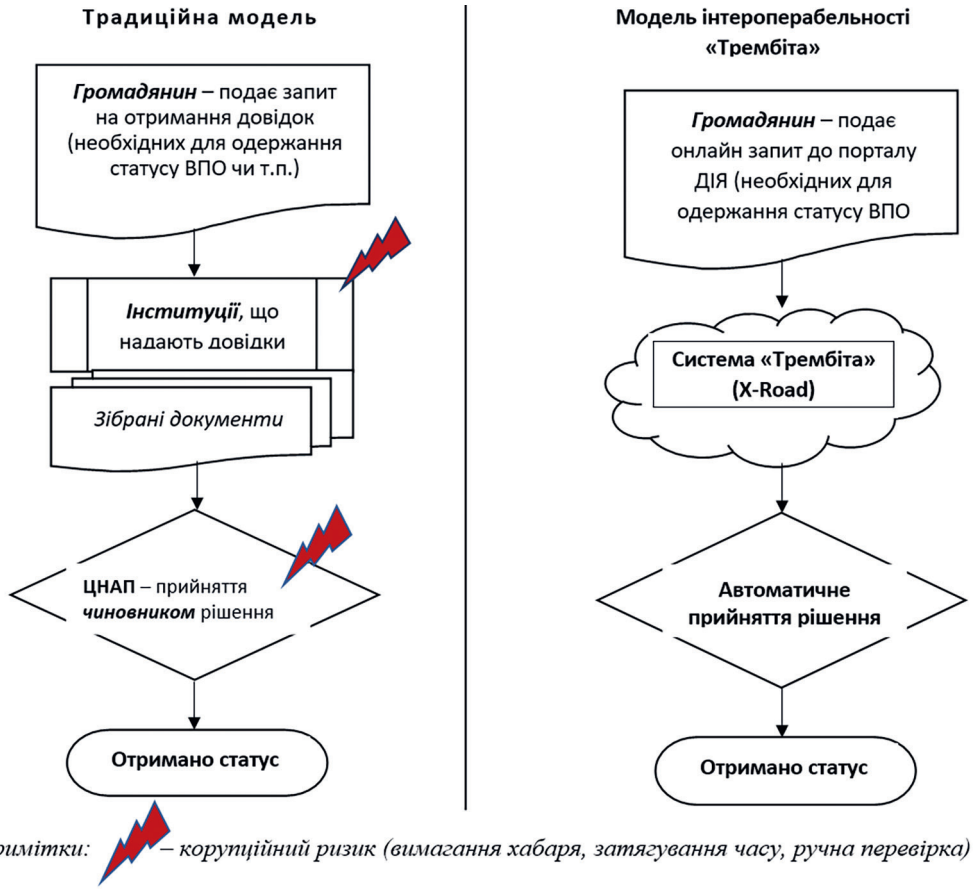

Рис. 1. Трансформація надання публічних послуг та усунення корупційних ризиків завдяки системі інтероперабельності «Трембіта»

Джерело: розроблено автором

ЗОВНІШНІ ВИКЛИКИ (Технологічні)	ВНУТРІШНІ ВИКЛИКИ (Інституційні)
Суть загрози. *Кібератаки з боку агресора, спроби викрадення масивів даних (з HRMIS чи реєстрів), DDoS-атаки на державні сервери.*	***Суть загрози.*** *«Цифровий саботаж», прихований опір бюрократії, симуляція «технічних проблем» через небажання втрачати дискреційні (ручні) повноваження та монополію на інформацію.*
Вектор протидії. *Перехід на хмарні технології (Cloud First), криптографічний захист, імплементація європейських стандартів безпеки (Директива ЄС NIS2).*	***Вектор протидії.*** *Жорстка політична воля, встановлення адміністративної відповідальності керівників за непідключення до ІІС, 100% обов'язковість використання цифрових систем (Data-driven).*

Рис. 2. Матриця ключових загроз упровадженню інтегрованих інформаційних систем в органах публічної влади

Джерело: розроблено автором

Перший виклик – кібербезпека в умовах воєнного стану. Акумуляція величезних масивів сенситивних даних (персональних даних посадовців у HRMIS, даних громадян у реєстрах, що взаємодіють через «Трембіту») робить їх пріоритетною мішенню для кібератак з боку держави-агресора. Як зазначають А. Рачинський та О. Титаренко [5], в умовах європейської інтеграції Україна має імплементувати жорсткі стандарти кіберзахисту, зокрема Директиву ЄС NIS2 (Directive (EU) 2022/2555) щодо заходів для високого спільного рівня кібербезпеки. Це вимагає відкритості даних для суспільства, але закритості та криптографічного захисту (архітектура Cloud First) від зовнішніх втручань. Злам системи може не лише паралізувати роботу державного органу, але й призвести до компрометації антикорупційних алгоритмів.

Другий виклик – інституційний опір або «цифровий саботаж». Це внутрішній фактор, який часто недооцінюється. Практика показує, що значна частина державного апарату чинить прихований опір повноцінному впровадженню систем прозорості.

– Саботаж рідко має відкриту форму. Зазвичай він маскується під:

– *«Технічні проблеми»* (затягування інтеграції баз даних через нібито несумісність форматів);

– *«Нормативні колізії»* (посилання на застарілі інструкції з діловодства, які вимагають паперового дублювання документів);

– *«Кадровий голод»* (відмова від використання ІІС через нібито низьку цифрову грамотність персоналу).

Проте, як свідчить аналіз Реєстру корупційних ризиків НАЗК [10], справжньою причиною такого опору є небажання бенефіціарів традиційної системи втрачати інструменти ручного управління фінансами, кадрами та повноваженнями. Подолання цифрового саботажу вимагає жорсткої політичної волі керівництва держави: підключення до HRMIS та «Трембіти» має бути не правом державного органу, а його безальтернативним обов'язком, невиконання якого повинно тягнути за собою управлінську відповідальність керівника.

Висновки і перспективи подальших розвідок у даному напрямі. Впровадження інтегрованих інформаційних систем є безальтернативним та найбільш дієвим інструментом реінжинірингу публічної служби України. Проведене дослідження дозволяє дійти висновку, що перехід від паперового та фрагментарного цифрового документообігу до парадигми управління на основі даних (data-driven governance) руйнує сам фундамент корупційних практик. Системи класу HRMIS та інтероперабельні платформи рівня «Трембіта» ліквідують монополію посадовців на інформацію, автоматизують процеси розподілу ресурсів та фіксують незмінний цифровий слід (Audit Trail), перетворюючи корупційні дії з «прихованої можливості» на «технологічну неможливість».

Водночас, цифровізація публічного управління не повинна зупинятися на етапі простої автоматизації наявних процесів. Перспективою подальших розвідок є дослідження переходу від реактивної до *проактивної (превентивної)* антикорупційної діяльності.

Як доводять у своєму новітньому дослідженні Т. Штерма, А. Луківський та С. Луківський [6], наступним еволюційним кроком у мінімізації корупційних ризиків має стати впровадження технологій штучного інтелекту (ШІ) в моделі державного управління. Інтегровані бази даних є ідеальним середовищем для машинного навчання. Алгоритми ШІ здатні в режимі реального часу аналізувати мільйони транзакцій, кадрових наказів та адміністративних послуг, автоматично виявляючи аномалії – так звані «червоні прапорці» (red flags). Наприклад, ШІ може миттєво сигналізувати про нетипове зростання преміального фонду в окремому департаменті або про систематичне пришвидшення видачі дозволів певним суб'єктам господарювання.

Отже, забезпечення стовідсоткової інтеграції органів публічної влади до єдиної екосистеми ІІС у поєднанні з аналітичними можливостями штучного інтелекту дозволить Україні не лише виконати антикорупційні вимоги щодо вступу до ЄС, але й створити одну з найбільш прозорих, стійких та ефективних моделей публічної служби у світі.

Список використаних джерел:

1. Державна антикорупційна програма на 2023–2025 роки : постанова Кабінету Міністрів України від 04.03.2023 № 220. URL: https://zakon.rada.gov.ua/laws/show/220-2023-%D0%BF#Text.

2. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні : базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України*. 2018. № 1. С. 5–10. URL: http://nbuv.gov.ua/UJRN/Vnadu_2018_1_3

3. Биркович Т. І., Биркович В. І., Кабанець О. С. Механізми публічного управління у сфері цифрових трансформацій. *Державне управління: удосконалення та розвиток*. 2019. № 9. DOI: https://doi.org/10.32702/2307-2156-2019.9.2

4. Бондарчук Н. В., Дуброва Н. П. Цифровізація публічного управління: стан та перспективи розвитку. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління.* 2023. Том 34 (73), № 1. С. 38–43. DOI: https://doi.org/10.32782/TNU-2663-6468/2023.1/38

5. Рачинський А. П., Титаренко О. М. Цифрова трансформація публічного управління. *Державне будівництво.* 2024. № 2 (36). DOI: https://doi.org/10.26565/1992-2337-2024-2-38

6. Штерма Т. В., Луківський А. С., Луківський С. Д. Впровадження штучного інтелекту у моделі економічного управління для мінімізації корупційних ризиків. *Здобутки економіки: перспективи та інновації.* 2025. № 3. DOI: https://doi.org/10.5281/zenodo.14959270

7. Сталий розвиток і цифрові інновації : колективна монографія / за заг. ред. Б. В. Буркинського, О. А. Назаренка, О. І. Лайка, С. К. Хаджирадєвої. Одеса : ДУ ІРЕЕД НАНУ, 2024. 416 с.

8. Про схвалення Концепції впровадження інформаційної системи управління людськими ресурсами в державних органах : розпорядження Кабінету Міністрів України від 01.12.2017 № 844-р (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/844-2017-%D1%80#Text

9. Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта»: Офіційний портал. URL: https://trembita.gov.ua/

10. Реєстр корупційних ризиків // Офіційний сайт Національного агентства з питань запобігання корупції. URL: https://nazk.gov.ua/uk/reestr-korupcijnih-rizikiv/

11. Одарченко Роман, Фесенко Андрій Роль інформаційних технологій та проблеми забезпечення кібербезпеки громад в умовах кібервійни. Сталий розвиток і цифрові інновації: колективна монографія / За заг. ред. академіка НАН України Б.В.Буркинського, О. А. Назаренка, О.І. Лайка,. С.К. Хаджирадєвої; Одеса: ДУ ІРЕЕД НАНУ, 2024. С. 262–273

References:

1. Cabinet of Ministers of Ukraine. (2023, March 4). *Derzhavna antykoruptsiina prohrama na 2023–2025 roky* [State anti-corruption program for 2023-2025] (Resolution No. 220). Retrieved from: https://zakon.rada.gov.ua/laws/show/220-2023-%D0%BF#Text

2. Kuibida, V. S., Karpenko, O. V., & Namestnik, V. V. (2018). *Tsyfrove vriaduvannia v Ukraini: bazovi definitsii poniatiino-katehorialnoho aparatu* [Digital governance in Ukraine: basic definitions of the conceptual and categorical apparatus]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy*, (1), 5–10. Retrieved from: http://nbuv.gov.ua/UJRN/Vnadu_2018_1_3

3. Byrkovych, T. I., Byrkovych, V. I., & Kabanets, O. S. (2019). *Mekhanizmy publichnoho upravlinnia u sferi tsyfrovykh transformatsii* [Mechanisms of public administration in the field of digital transformations]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, (9). https://doi.org/10.32702/2307-2156-2019.9.2

4. Bondarchuk, N. V., & Dubrova, N. P. (2023). *Tsyfrovizatsiia publichnoho upravlinnia: stan ta perspektyvy rozvytku* [Digitalization of public administration: State and prospects of development]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Derzhavne upravlinnia*, 34(73)(1), 38–43. https://doi.org/10.32782/TNU-2663-6468/2023.1/38

5. Rachynskyi, A. P., & Tytarenko, O. M. (2024). *Tsyfrova transformatsiia publichnoho upravlinnia* [Digital transformation of public administration]. *Derzhavne budivnytstvo*, (2). https://doi.org/10.26565/1992-2337-2024-2-38

6. Shterma, T. V., Lukivskyi, A. S., & Lukivskyi, S. D. (2025). *Vprovadzhennia shtuchnoho intelektu u modeli ekonomichnoho upravlinnia dlia minimizatsii koruptsiinykh ryzykiv* [Implementation of artificial intelligence in economic management models to minimize corruption risks]. *Zdobutky ekonomiky: perspektyvy ta innovatsii*, (3). https://doi.org/10.5281/zenodo.14959270

7. Burkynskyi, B. V., Nazarenko, O. A., Laiko, O. I., & Khadzhyradieva, S. K. (Eds.). (2024). *Stalyi rozvytok i tsyfrovi innovatsii* [Sustainable development and digital innovations]. DU IREED NANU.

8. Cabinet of Ministers of Ukraine. (2017, December 1). *Pro skhvalennia Kontseptsii vprovadzhennia informatsiinoi systemy upravlinnia liudskymy resursamy v derzhavnykh orhanakh* [On approval of the Concept for the implementation of the human resource management information system in state bodies] (Order No. 844-r). Retrieved from: https://zakon.rada.gov.ua/laws/show/844-2017-%D1%80#Text

9. Systema elektronnoi vzaiemodii derzhavnykh elektronnykh informatsiinykh resursiv "Trembita" ["Trembita" system of electronic interaction of state electronic information resources]. (n.d.). Retrieved from: https://trembita.gov.ua/

10. National Agency on Corruption Prevention. (n.d.). *Reiestr koruptsiinykh ryzykiv* [Register of corruption risks]. Retrieved from: https://nazk.gov.ua/uk/reestr-korupcijnih-rizikiv/

11. Odarchenko, R., & Fesenko, A. (2024). *Rol informatsiinykh tekhnolohii ta problemy zabezpechennia kiberbezpeky hromad v umovakh kiberviiny* [The role of information technologies and the problems of ensuring the cybersecurity of communities in the context of cyber warfare]. In B. V. Burkynskyi, O. A. Nazarenko, O. I. Laiko, & S. K. Khadzhyradieva (Eds.), *Stalyi rozvytok i tsyfrovi innovatsii* (pp. 262–273). DU IREED NANU.

Дата першого надходження статті до видання: 05.02.2026
Дата прийняття статті до друку після рецензування: 09.03.2026
Дата публікації (оприлюднення) статті: 30.04.2026