https://doi.org/10.26565/2220-8089-2022-41-04
УДК 004.89:343.353(327)

Наталія Анатоліївна Вінникова
професор, доктор політ. наук, Харківський національний університет імені В.Н. Каразіна,
майдан Свободи, 4, 61022, м. Харків
vinnykova@karazin.ua, https://orcid.org/0000-0001-5941-7562

ЦИФРОВІ ТЕХНОЛОГІЇ У БОРОТЬБІ З ГЛОБАЛЬНОЮ КОРУПЦІЄЮ

Одним із феноменів сьогодення, породжених глобалізаційними процесами, є транснаціоналізація корупційних практик. Цьому «сприяють» можливості цифрових технологій. Зумовлюючи такі негативні явища, як глобальна корупція, цифровізація водночас забезпечує інструменти для боротьби з нею.

Увага зосереджується на оцінці потенціалу цифрових технологій, насамперед штучного інтелекту, в запобіганні корупційним практикам. Викладено характеристики феномена «глобальної корупції». На основі аналізу досвіду впровадження цифрових технологій у боротьбі з корупцією розкрито проблемні аспекти та перспективні напрями розвитку цифрових антикорупційних механізмів на національному рівні урядування. Особливу увагу приділено цифровим інструментам виявлення та відстеження транснаціональних корупційних схем у межах міжнародних журналістських розслідувань і технологіям антикорупційного контролю в Європейському Союзі. З'ясовано, що однією з критичних проблем у застосуванні штучного інтелекту для подолання транснаціональної корупції є відсутність консолідованого міжнародного регуляторного режиму доступу до даних. Продемонстровано, що штучний інтелект є амбівалентним інструментом, який можуть використовувати як для виявлення корупції, так і застосовувати в корупційних цілях. Наведено аргументи щодо перспективності технології розподіленого реєстру як інструменту запобігання корупції. Визначено фактори, які гальмують масштабне впровадження блокчейну і смарт-контрактів як механізмів зниження ризиків виникнення корупції. Акцентовано на необхідності напрацювання міжнародних стандартів використання технологій штучного інтелекту в боротьбі з корупційними практиками. Доведено, що гранично важливим у боротьбі з глобальною корупцією є створення профільної транснаціональної структури з відповідними нормотворчими та контрольними повноваженнями.

Ключові слова*: глобальна корупція, цифрові технології, штучний інтелект, блокчейн, смарт-контракти, глобальне управління, Європейський Союз.*

Як цитувати: Вінникова, Н.А. 2022. Цифрові технології у боротьбі з глобальною корупцією. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Питання політології»*. 41: 30-39. https://doi.org/10.26565/2220-8089-2022-41-04

In cites: Vinnykova, Nataliya. 2022. Digital Technologies in Combating Global Corruption. *The journal of V. N. Karazin Kharkiv National University. Series «Issues of Political Science»*. 41: 30-39. https://doi.org/10.26565/2220-8089-2022-41-04 (in Ukrainian)

Корупція – одна з системних суспільно-політичних проблем, – на жаль, не зникає з порядку денного політичного управління. З розвитком глобалізації цей феномен набуває більш комплексних форм. Журналістські викриття останніх років щодо офшорних збережень відомих політиків і знаменитостей шоу-бізнесу, як-от опублікування «Панамських документів» (ICIJ 2017) і «документів Пандори» (ICIJ 2021), є наочними прикладами глобального характеру сучасних корупційних процесів.

Поширення корупційних схем транснаціонального масштабу зумовлено також і використанням цифрових технологій. Цифровізація фінансового сектора глобальної економіки забезпечує надзвичайну оперативність транзакцій і широкий спектр каналів їх проведення. Це ускладнює виявлення маршрутів фінансових потоків. Крім того, різноманіття криптовалют і відсутність розвинутої міжнародної правової бази для їх регулювання додають опції для реалізації корупційних практик. Утім, саме до перспектив застосування цифрових технологій у боротьбі з корупцією привертають увагу урядовці, експертні та наукові кола.

Ця тема заслуговує на дослідницьку увагу і в Україні. Адже наша держава, демонструючи передові цифрові моделі запобігання корупції (наприклад, системи державних закупівель Prozorro й моніторинговий портал громадського контролю Dozorro), водночас, на жаль, стикається з репутаційними втратами через систематичне потрапляння в міжнародний інформаційний простір відомостей про корупційні практики політиків і представників бізнесу. Варто зауважити, що більшість публікацій розкривають окремі кейси цифровізації антикорупційних механізмів переважно на державному рівні урядування. Попри гостру актуальність проблематики, усе ще бракує наукових праць з комплексним аналізом можливостей застосування цифрових інструментів у подоланні корупційних практик у глобальному вимірі.

Отже, метою нашого дослідження є визначення пріоритетних напрямів впровадження цифрових технологій у боротьбі з глобальною корупцією. Для досягнення означеної цілі дослідження побудовано на виконанні таких завдань: 1) розкрити поняття глобальної корупції; 2) проаналізувати досвід впровадження цифрових технологій у боротьбі з корупцією; 3) окреслити перспективи та ризики застосування цифрових технологій у боротьбі з корупційними практиками в транснаціональному вимірі.

Корупцію зазвичай визначають як «зловживання довіреною владою для приватної вигоди» (Transparency International n.d.). З'являючись у різних формах, вона охоплює широкий спектр практик, як хабарництво, відкати, непотизм, рекет, саботаж, шахрайство, змова тощо. Означені прояви корупції не є нормативно еквівалентними: крадіжка або шахрайство можуть вважатися злочинними в більшості країн, однак «торгівля впливом» або хабарництво можуть толеруватися залежно від соціокультурного контексту, в якому ці практики відбуваються.

Конвенція ООН проти корупції містить перелік видів корупції в серії положень, спрямованих на її криміналізацію корупції: від підкупу національних та іноземних посадових осіб та посадових осіб публічних міжнародних організацій (ст. 15 і 16) до відмивання доходів, одержаних злочинним шляхом (ст. 23); приховування (ст. 24) та перешкоджання правосуддю (ст. 25) (UN Office on Drugs and Crime 2004).

Глобальний вимір корупції ще складніше ідентифікувати. Хоча, її наслідки відчутні по всьому світі. Згідно з даними ООН, приблизно 1 трильйон доларів щорічно виплачується у вигляді хабарів, а ще 2,6 трильйона доларів втрачається через корупційну діяльність у всьому світі (United Nations 2018).

Глобальну корупцію відносять до злочинної діяльності, розуміючи під нею ендемічні явища, які з'являються з регулярною частотою практично в усіх країнах, у різному ступені та пропорціях (Transparency International Hravatska 2020). Глобальний вимір корупції пов'язують з мережами, які використовують хабарі, щоб сприяти торгівлі людьми, наркотиками, зникаючими видами [тварин] та зброєю (UN Office on Drugs and Crime 2014). Глобальні форми корупції важко виявляти, оскільки вона здійснюється транскордонно, залучаючи численні юрисдикції та різноманітні цифрові інструменти для здійснення транзакцій.

Узагальнюючи найбільш поширені практики, можна стверджувати, що ключовою характеристикою глобальної корупції *є неформальне використання транснаціональних зв'язків для отримання незаконних прибутків шляхом зловживання владними ресурсами.* Транскордонний характер фінансових операцій і міжнародний склад учасників корупційних схем є атрибутами глобального виміру корупції. Крім того, наявний нормативно-інституційний арсенал інструментів боротьби з глобальною корупцією у міжнародних організацій та постійна увага до цього питання на світових форумах, зокрема зустрічах глав держав, є доказом масштабності та гостроти означеної проблеми. Серед найбільш відомих міжнародних платформ є Антикорупційний та інтеграційний форум Організації економічного співробітництва та розвитку (OECD 2022) та Міжнародна антикорупційна конференція, яка збирає представників зі 140 країн світу

(IACC 2022). Симптоматично, що пріоритетними темами обговорення на зустрічах Великої Двадцятки під головування Індонезії 2022 р. стали цифрова трансформація і посилення колективних зусиль у боротьбі з корупцією (Indonesia's G20 Presidency 2022) .

Наведені приклади свідчать не лише про увагу з боку міжнародних установ та організацій до проблем корупції, через її глобальний характер, а й про звернення до передових технологій, зокрема штучного інтелекту, як інструменту боротьби з нею.

Штучний інтелект (ШІ) визначають як «системи, які демонструють розумну поведінку, аналізуючи навколишнє середовище та вживаючи дій – з певним ступенем автономності – для досягнення конкретних цілей» (European Commission 2018). На відміну від «класичних» інформаційно-комунікаційних технологій (ІКТ), які дозволяють цифрувати процедури закупівель, надавати державні послуги онлайн і публікувати відкриті державні дані, унікальність штучного інтелекту полягає в його здатності до автономного навчання. Замість того, щоб програміст вказував курс дій машині для всіх можливих результатів, алгоритми ШІ можуть самостійно знаходити рішення. Використання ШІ як інструменту оброблення даних дозволяє виявляти інформацію про бенефіціарну власність з усього світу; відстежувати мережі зв'язків, розташування, використання підставних компаній, офшорні юрисдикції та банківську інформацію учасників тендерів (Sharma 2018). Потенціал ШІ є особливо перспективним у критичних для бізнесу бюрократичних процесах, таких як реєстрація землі та власності; управління соціальними трансфертами; перевірка персональних даних; оформлення державних контрактів тощо.

Вартим уваги для застосування цифрових технологій у глобальному вимірі боротьби з корупцією вбачається досвід Європейського Союзу. Обсяги фінансування програм, грантів і проєктів як у сфері внутрішніх спільних політик ЄС, так і в реалізації його зовнішньої діяльності вимагає транснаціонального механізму контролю за видатками і захисту від шахрайства. Крім того, попри високі позиції держав-членів ЄС зі сприйняття корупції, останні кроснаціональні дослідження виявили, що це явище залишається серйозною проблемою для громадян Євросоюзу: 68% респондентів у межах моніторингового проєкту Євробарометру (Special Eurobarometer 2022:8) та 62% з понад 40 000 учасників опитування Глобального барометру корупції (Transparency International 2021) вважають корупцію широко поширеною у їхній країні. Претензії громадян насамперед спрямовані на національні державні установи, де, на думку 74% респондентів, найбільше поширена корупція (Special Eurobarometer 2022:8). У цьому антирейтингу сприйняття корупції опинилися політичні партії (58%) і місцеві, регіональні та національні політики (55%) (Special Eurobarometer 2022:8).

Бізнес-сектор у країнах Європейського Союзу також вказує, що корупція є проблемою під час ведення справ: про це зазначили більше третини компаній в ЄС (34%). Більшість комерційних структур зазначили, що в їхній країні тісні зв'язки між бізнесом і політикою призводять до корупції (79%) і що фаворитизм і корупція перешкоджають бізнес-конкуренції (70%). Водночас 59% опитаних представників бізнесу в ЄС погоджуються з твердженням, що хабарництво та використання зв'язків часто є найлегшим способом отримати певні державні послуги (Flash Eurobarometer 2022:3).

Запущений Європейською Комісією цифровий інструмент ARACHNE аналізу даних у системі управлінського аудиту здійснював моніторинг використання коштів структурних фондів Європейського Союзу протягом реалізації бюджету ЄС 2014-2021 рр. (European Commission 2015).

ARACHNE збирає дані від органів управління Європейського соціального фонду та Європейського фонду регіонального розвитку, а також із зовнішніх джерел даних. Відповідними суб'єктами даних є юридичні та фізичні особи. ARACHNE аналізує дані та доповнює їх загальнодоступною інформацією, щоб визначити бенефіціарів, контракти та підрядників, які можуть бути вразливими до ризиків шахрайства, конфлікту інтересів і порушень. Цей цифровий інструмент обробляє інформацію про майже 400 мільйонів компаній у всьому світі (активних і неактивних); відомості про власність (акціонери, дочірні компанії, рівень участі, тощо); 41 мільйон компаній із детальною фінансовою інформацією (оборот, грошовий потік, коефіцієнт платоспроможності); адресні дані; інформацію про топ-менеджмент і пов'язаних осіб (директори, вище керівництво, ступінь спорідненості); кількість компаній і роль у компанії; показники щодо довіри та ризиків банкрутство (Neculcea and Ninka 2022:11).

Спочатку держави-члени вагалися із впровадженням цієї технології, посилаючись

на національні правила захисту даних. Однак під тиском наднаціональних установ цю технологію антикорупційного контролю починають застосовувати в державах-членах. У своїй пропозиції щодо переглянутого фінансового регламенту Європейська Комісія запропонувала зробити обов'язковим використання інтегрованого інструменту для аналізу даних і оцінки ризиків у виконанні бюджету ЄС (European Commission 2022a).

Оскільки основним дискусійним питанням щодо використання ARACHNE в національних системах фінансового контролю держав-членів був захист даних, компромісом стало рішення про заборону передачі даних за межі приміщень Європейської Комісії. Дані, завантажені державами-членами, більше не доступні постачальнику послуг. Повна обробка даних (включно з оцінкою та розрахунком ризиків) виконується в приміщеннях Європейської Комісії і керується працівниками IT ARACHNE та Генеральному директораті Європейської комісії з інформатики, відповідальному за надання цифрових послуг (European Commission 2022 b).

Окрім ARACHNE ЄС має у своєму розпорядженні Систему раннього виявлення та виключення (Early Detection and Exclusion System, EDES) і Систему управління невідповідностями (Irregularity Management System, IMS), що функціонують у межах Інформаційної системи боротьби з шахрайством (Anti-Fraud Information System, AFIS). Остання допомагає зберігати та аналізувати відповідні дані, зокрема вона містить відомості про понад 8500 кінцевих користувачів у майже 1400 профільних службах. До цих користувачів належать держави-члени, країни-партнери, що не входять до ЄС, міжнародні організації, Європейська Комісія та інші установи Європейського Союзу (European Anti-Fraud Office n.d.).

Система раннього виявлення та виключення (EDES) складається з комплексу заходів щодо ненадійних суб'єктів господарювання. Цей механізм дозволяє виявляти та виключати з фінансування ЄС економічних операторів, щодо яких доведена участь у шахрайстві. Цифровою основою EDES є база даних, яка містить список осіб або організацій, які не мають доступу до фінансування ЄС або на яких накладено фінансові санкції (European Commission 2022c).

Інший компонент цифрової системи боротьби Європейського Союзу з шахрайством – Система управління невідповідностями – створений для забезпечення повідомлень про порушення, зокрема шахрайство, у випадках, пов'язаних зі спільним управлінням та фондами допомоги перед вступом до ЄС (European Anti-Fraud Office n.d.). Держави-члени, країни-кандидати та інші країни, що не входять до ЄС, формують ієрархічну структуру звітності з різними рівнями відповідальності. Майже 700 організацій, що звітують, і понад 3000 користувачів цього цифрового механізму несуть відповідальність за своєчасне повідомлення про порушення (European Anti-Fraud Office n.d.).

Також варто додати, що попри суворі регуляторні вимоги щодо захисту даних і доволі поміркований підхід ЄС до впровадження штучного інтелекту, технології ШІ вже використовуються Європейським офісом боротьби з шахрайством. Головна антикорупційна служба ЄС розробила систему аналізу даних на основі моделі машинного навчання, щоб мати можливість знаходити «підозрілі» семантичні значення в електронному листуванні та соціальних медіа, зокрема в контексті організації тендерів і проведення закупівель (European Parliament 2021:54). Особливу увагу у використанні ШІ Європейський офіс боротьби з шахрайством приділяє програмному забезпеченню та персоналізації. Технології штучного інтелекту потребують великих обсягів даних. Водночас інформація, яку вони обробляють, має бути достовірною. Запущена Європейським офісом боротьби з шахрайством програма з виявлення ознак фінансового шахрайства в «Панамських документах» знайшла сім збігів з людьми, які працюють в установах ЄС, але деякі з них пізніше були визнані помилковими через характер неповних даних. Проблема також виникла під час спроби ідентифікувати одних і тих самих фінансових суб'єктів, що діють у різних країнах під різними назвами (European Parliament 2021:14).

Попри технічні виклики Європейський Союз планує активізувати впровадження цифрових технологій і розвиток систем оброблення даних в антикорупційній діяльності, що зазначено в звіті Європейської Комісії за 2021 рік щодо захисту фінансових інтересів Європейського Союзу і боротьби з шахрайством (European Commission 2022d: 44). І, хоча деталізованої інформації про конкретні корупційні випадки, виявлені за допомогою зазначених цифрових інструментів у звіті не представлено, однак загальний результат демонструє доцільність використання цифрових технологій в антикоруп-

ційній політиці ЄС. Так, у 2021 р. було повідомлено про 11 218 порушень на суму близько 3 мільярдів 24 мільйонів євро (European Commission 2022d: 31). Серед інших, найбільшим за обсягами шахрайськими порушенням було використання фінансів Європейських структурних та інвестиційних фондів на суму 1 мільярд 624 мільйонів євро (European Commission 2022d: 36).

Симптоматично, що для антикорупційних заходів Європейський Союз не шкодує матеріального підкріплення. У межах Програми боротьби з шахрайством з бюджетом у 181 мільйон євро на 2021-2027 рр. на Інформаційну систему боротьби з шахрайством виділено 60 мільйонів євро та 7 мільйонів євро – для реалізації Системи управління невідповідностями (European Anti-Fraud Office n.d.).

Ці приклади демонструють, як під впливом наднаціонального регулятора цифрові технології відстеження корупційних практик впроваджуються в системи управління та контролю за фінансами на державному рівні урядування. Водночас це забезпечує більше можливостей для удосконалення механізмів боротьби з транснаціональною корупцією.

І все ж, найбільш масштабними за обсягами опрацьованих даних і виявлених ознак ухилення від сплати податків стали викриття Міжнародному консорціуму журналістів-розслідувачів, здійснені за допомогою технологій штучного інтелекту. У взаємодії з технологічними стартапами Міжнародний консорціум журналістів-розслідувачів опрацював витік даних про понад 810 000 офшорних організацій, які є частиною розслідувань «Документів Пандори» (Pandora Papers), «Райські документи» (Paradise Papers), «Багамські витіки» (Bahamas Leaks), «Панамські документи» (Panama Papers) та «Офшорні витіки» (Offshore Leaks). Дані пов’язані з людьми та компаніями з понад 200 країн і територій. Наразі зібрана база даних про компанії та трасти, зареєстровані в податкових гаванях, імена їхніх справжніх власників. Загалом інтерактивний додаток містить понад 750 000 імен людей і компаній, які стоять за офшорними структурами (ICIJn.d.).

Цифрові технології стали ключовим інструментом у реалізації глобальних антикорупційних розслідувань. Так, технологічні розробки компаній Linkurious та Neo Technology допомогли міжнародній мережі з 370 журналістів опрацювати понад 11,5 млн. зашифрованих документів панамської юридичної фірми Mossack Fonseca, що забезпечувала офшорне розміщення капіталу відомих політиків, державних діячів і знаменитостей шоу-бізнесу. Вони містили майже 2,6 терабайт даних, задокументувавши 214 488 офшорних структур, створені та адміністровані Mossack Fonseca між 1977 і 2015 роками (Linkurious 2016). Дешифрування даних та перетворення витоку файлів на придатні для аналізу документів здійснювалося за допомогою технологій розпізнавання й опрацювання текстів Apache Solr, Apache Tika та Nuix (Linkurious 2016). Зрештою це призвело до глобального викриття, відомого як «Панамські документи».

Більшого резонансу набув проєкт «Документи Пандори», для реалізації якого 600 журналістів з 150 медіа-організацій опрацювали 11,9 млн. записів, що становило 2,94 терабайта даних про офшорну діяльність понад 27 000 компаній і 29 000 власників-бенефіціарів (Linkurious 2021). У розслідуванні фігурують 330 політиків і 130 мільярдерів Forbes, а також знаменитості, члени королівських родин та ін. (Linkurious 2021).

Для автоматизації вилучення та структурування даних, що містять інформацію про бенефіціарну власність в цьому проєкті використана мова програмування Python, а також інструменти, такі як програмне забезпечення Fonduer і Scikit-learn (Linkurious 2021). Після фільтрації та структурування даних за допомогою платформи розслідувань Linkurious Enterprise і графічної бази даних Neo4j журналісти-учасники розслідування змогли проаналізувати цю величезну кількість інформації. Завдяки візуалізації даних вдалося виявити зв’язки між усіма учасниками офшорних схем.

Результати реалізації проєктів Міжнародного консорціуму журналістів-розслідувачів були сприйняті вкрай суперечливо: від обурених гучних заяв політиків і селебритіс, які опинилися в «чорних» списках учасників офшорних схем, до запровадження більш жорстких режимів контролю фінансових операцій як на національному рівні урядування, такі і в транснаціональному вимірі, зокрема в Європейському Союзі. Утім, важливо, що найбільші за всю історію розслідування податкових гаваней і фінансових злочинів не лише змінили глобальну дискусію про необхідність консолідації міжнародних зусиль у боротьбі з корупційними практиками глобального масштабу, а й привернули увагу до ролі цифрових технологій у вирішенні цієї проблеми. Водночас принципове питання щодо надійності та

достовірності даних, які потрапляють в опрацювання цифрових інструментів, залишається неврегульованим. Застосування технологій штучного інтелекту також характеризується дилемою між доступом до інформації та посиленням нормативних вимог до захисту персональних даних. Різні типи джерел даних містять різні проблеми щодо доступності та якості даних. Записи дзвінків і дані про окремі транзакції є конфіденційними даними, тим більше біометрична ідентифікаційна інформація. У деяких країнах довіра до приватних компаній може перевищувати довіру до уряду щодо збереження такої інформації в безпеці та захисту від зловживання. Порушення прав на конфіденційність, навіть потенційних корупціонерів, не лише ставить під загрозу законність використання таких даних, але й підриває сприйману легітимність таких антикорупційних зусиль.

Крім того, небажані побічні ефекти таких систем можуть виникати через недостовірні чи викривлені дані, які використовуються для навчання ШІ, або в розробці алгоритму. Непрозорі алгоритми і, отже, непрозорі системи ухвалення рішень є проблемою, відомою як «проблема чорної скрині». Непрозорість багатьох систем машинного навчання робить їх уразливими для тих, хто хоче використовувати їх у корупційних цілях.

Експерти Transparency International визначили кілька опцій, за яких технології штучного інтелекту стають інструментом корупції:

1) система ШІ навмисно розроблена для корупційних цілей;

2) кодом або навчальними даними систем штучного інтелекту маніпулюють для досягнення корупційних цілей;

3) система штучного інтелекту використовується корумпованим способом (Köbis, Starke, Edward-Gill 2022:7).

Технології ШІ можуть бути налаштовані для обслуговування партикулярних групових інтересів. Такі випадки маніпулювання моделями штучного інтелекту для систематичного сприяння певній групі називаються «алгоритмічним захопленням» (Köbis, Starke, Edward-Gill 2022:8). Наприклад, пошкодження електронних закупівель потребує лише одноразової маніпуляції з системою штучного інтелекту, щоб отримати вигоду протягом тривалого періоду.

Ключовою особливістю штучного інтелекту, важливою для розуміння його потенціалу як інструменту корупції є унікальне поєднання персоналізації та масштабованості. Масштабування за допомогою штучного інтелекту часто вимагає низьких граничних витрат і дозволяє персоналізувати контент для конкретного одержувача. Корумповані актори можуть у такий спосіб зі стрімкою швидкістю охопити велику аудиторію з одночасним наданням персоналізованого контенту. Ці функції роблять технології ШІ привабливими для вико ристання зловмисниками. Вони пропонують вищі винагороди, надаючи при цьому ефективні маніпулятивні інструменти одночасно зменшуючи ризик виявлення через їх непрозору роботу та анонімність.

Серед суперечливих аспектів застосування технологій штучного інтелекту в розкритті корупційних схем є проблема інтерпретації результатів їх роботи. Відсутність пояснення призведе до того, що мережеві адміністратори та експерти не зможуть обґрунтувати певні рішення штучного інтелекту. Прикладом стала відмова від функціонування антикорупційної технології Zero Trust, впровадженої урядом КНР. Програма переглядала дані банків, об'єктів нерухомості та будівництва та навіть супутникові дані, щоб виявити ознаки корупції, зокрема підозрілий переказ грошей або нову машину чи майно, зареєстроване на ім'я родини чи друзів державного чиновника. Хоча вона працювала лише в кількох десятках регіонів і міст, Zero Trust вдалося виявити 8721 порушника (або тих, кого система вважала такими). Однак через деякий час роботу системи вирішили припинити, оскільки вона виявилася проблемною з точки зору обґрунтування фактів корупції (Chen 2019). Система вказувала на порушника, але не могла пояснити, чому ця людина є корупціонером. До розслідування кожної справи доводилося залучати багато людей, які не завжди давали однозначний висновок.

Отже, хоча потенціал штучного інтелекту щодо виявлення корупції в різних сферах влади є високим, розвиток правової бази для його застосування має не лише передувати, а й супроводжувати весь процес. Крім того, найкращим способом боротьби з корупційними практиками є впровадження інструментів їх запобіганню. Таким інструментом можуть виступати технології розподіленого реєстру.

Блокчейн-технології забезпечують створення захищених від корупції публічних записів (таких як адміністративні реєстри) та державних транзакцій. Блокчейн також дозволяє автоматизувати управлінські проце-

си за участю акторів з державного, приватного та громадського секторів. Передовий функціонал технології блокчейну – смарт-контракти – підвищує ефективність і зменшує невизначеність транзакцій. Смарт-контракти дозволяють контролювати та адмініструвати процеси на основі різних можливих непередбачених обставин, які можуть формуватися користувачами або зовнішніми факторами. Ця технологія застосовується для цільових соціальних виплат, сприяння економічним операціям на ринках власності та підтримки нормативного прогнозування й адміністрування фінансових систем.

Блокчейн також забезпечує фактичну децентралізацію влади: шляхом зміщення від центрального посередника до екосистеми. За допомогою блокчейну можна сприяти підвищенню прозорості державних установ у таких сферах, як державні фінанси, або розширення контролю громадян над виборчими процедурами. Пілотні проєкти запуску блокчейну демонструють, що ця технологія може підвищити ефективність і надійність систем фінансового контролю, транзакцій за участі багатьох сторін (Allessie, Sobolewski, Vaccari, 2019). Наприклад, Національне агентство державного реєстру Грузії використовує технологію блокчейн для надання своїм громадянам цифрового сертифікату прав власності на землю. Перевірка сертифікатів здійснюється на публічному блокчейні, який знаходиться поза контролем будь-якого учасника або групи учасників. Незалежний і непідкупний механізм Exonum допомагає боротися з шахрайством і запобігати суперечкам щодо прав власності на землю (National Agency of Public Registry 2016).

Технології розподіленого реєстру – це нові можливості для державних та міжнародних структур у регуляторному нагляді: миттєвий доступ до фактичної інформації про ділові операції забезпечує спектр інструментів, за допомогою яких можуть протидіяти шахрайству чи ухиляннню від сплати податків. Найбільшу зацікавленість у використанні блокчейну в транснаціональному вимірі демонструє Європейський Союз. Прагнучи лідерства в цій сфері, ЄС ставить за мету перетворитися на осередок для платформ, програм і компаній і центр розроблення стандартів для технології блокчейн. Європейська інфраструктура блокчейн-сервісів, запущена в 2021 році, має сприяти реалізації антикорупційних заходів у ЄС (European Commission 2021).

Однак такі трансформаційні застосування блокчейну як нового механізму управління наразі розглядаються концепттуально. Для втілення цієї функції блокчейну потрібні системні напрацювання. Більшість проаналізованих цифрових сервісів усе ще не готові до розширення в застосуванні. Це спричинено недостатньою технічною зрілістю або невідповідністю правовому середовищу, наприклад, щодо законності цифрових підписів і нотаріального посвідчення за допомогою криптографічних доказів. У разі складних проєктів широка адаптація до місцевих інституційних умов є ще однією перешкодою для масштабування. Крім того, бюрократичні структури можуть бути не зацікавлені в обмеженні своєї влади на користь означеного механізму.

На глобальному рівні управління роботу з узгодження підходів до нормативного регулювання електронних підписів і цифрових транзакцій розпочато в межах запропонованого ООН Модельного закону про електронні передавальні записи (United Nations 2017) та Ініціативи цифрових стандартів Міжнародної торгової палати (International Chamber of Commerce 2020). Створення міжнародної правової матриці може сприяти розгортанню блокчейну в транснаціональних форматах надання послуг, зокрема й фінансових. Проте міжнародні рекомендації корисні лише в тій мірі, в якій вони перетворюються на конкретні дії на національному рівні. Прийняття законодавства на основі цих інструментів поки що залишається обмеженим.

Отже, обидві технології – штучного інтелекту та систем блокчейну – мають свої недоліки. У той час як блокчейн-системи демонструють проблеми, пов’язані з масштабованістю та ефективністю даних, ШІ має недоліки в таких сферах, як пояснення, конфіденційність даних і надійність. Коли дві технології використовуються разом, вони покривають недоліки одна одної, утворюючи потужну комбінацію. Блокчейн забезпечує пояснюваність і конфіденційність у системах штучного інтелекту, а останній дає змогу системам блокчейну досягти більшої масштабованості, що може бути корисним для підвищення продуктивності, управління та персоналізації.

Висновки. Цифрові технології набувають все більшого поширення в боротьбі та запобіганні корупції. У виявленні корупційних схем транснаціонального масштабу свою ефективність продемонстрував штучний інтелект. Однак, як будь-яке техноло-

гічне застосування на початковій стадії впровадження, штучний інтелект має свій набір проблем.

1. *Доступ та надійність даних, що підлягають опрацюванню алгоритмами.* Наразі проблемою є винайдення балансу між існуючими нормами з захисту даних і тим фактом, що процеси ШІ базуються на великому обсязі даних. Водночас не менш гострим є питання достовірності інформації, яку опрацьовують технології штучного інтелекту. Алгоритми, навчені на необ'єктивних наборах даних, відтворюють і ще більше посилюють існуючі упередження в суспільстві. Для забезпечення транскордонних розслідувань гранично важливим є обмін інформацією про наявні ресурси. Поки що не існує глобальної мапи всіх доступних баз даних та інструментів їхнього моніторингу. Впроваджені проєкти з використанням ШІ як антикорупційного інструменту в різних країнах виявляються дуже схожими за принципами функціонування. Картографування цих баз даних допомогло б посилити потенціал технологій штучного інтелекту в боротьбі з корупцією в глобальному масштабі.

2. *Відсутність систем верифікації результатів роботи ШІ з виявлення ознак корупції.* Привабливість «великих даних» спокусила багатьох повірити, що кількісне збільшення даних подолає всі проблеми. Натомість потрібні ефективніші практики збору, моделювання даних і нормативних рамок з перевірки та інтерпретації результатів роботи технологій ШІ для отримання достовірних результатів без шкоди для права громадян на конфіденційність.

3. *Відсутність розвинутої міжнародно-правової бази з регулювання питань застосування технологій штучного інтелекту в боротьбі з корупцією.* Технології розвиваються швидше, ніж законодавство, і тому працюють у нерегульованому глобальному контексті. Уряди та бізнес-сектор мають гарантувати безпеку та конфіденційність персональних даних, які їм довірено, а також надійність публічних даних. Необхідно невідкладно напрацьовувати глобальні стандарти управління даними як у державному, так і в приватному секторах та нормативні механізми контролю за їх дотриманням. Це вимагає багатосторонніх підходів і щільнішої міжнародної співпраці.

Цифрові технології чи їх використання не обов'язково мають антикорупційний ефект. Натомість використовуватися в корупційних цілях. під час розроблення та впровадження зацікавлені особи можуть обмежити антикорупційний потенціал технології або налаштувати алгоритми на обслуговування лише своїх інтересів.

Варто також зважати на роль криптоактивів у транснаціональній корупції. Платформи обміну криптовалютою відіграють все більшу роль у схемах фінансового шахрайства. Криптовалюти функціонують на технології однорангового зв'язку, через що їх важко відстежити. Це вимагає активізації зусиль щодо регулювання криптоактивів як на внутрішньому, так і на міжнародному рівнях з точки зору незаконних угод, відмивання грошей та ухилення від сплати податків.

Перспективним механізмом запобігання корупції вбачають технології розподіленого реєстру. Пілотні проєкти впровадження блокчейну та смарт-контрактів у сферах надання адміністративних послуг, зокрема з високими ризиками корупції, як-от обслуговування майнових питань, продемонстрували ефективність і доцільність подальшого масштабування. Однак переведення управлінських процесів на принципи блокчейну потребує фактично парадигмальних змін в усталених моделях адміністрування. Побудова системи урядування на основі блокчейну може суттєво знизити рівень корупції, якщо не елімінувати її зовсім. Очевидно, що особи, зацікавленні в корупційних схемах, не вітатимуть такі технології та не сприятимуть їх впровадженню.

Корупція – глобальна проблема, яка потребує глобальних рішень. Досягнутого міжнародного консенсусу щодо масштабів шкоди від транснаціональних корупційних оборудок і визнання необхідності боротьби з ними недостатньо. Важливим є створення глобальної структури мережевого формату з функціональним призначенням виявлення та запобігання корупції.

Оскільки корупційні практики не обмежуються фінансовим шахрайством, нагальною є потреба розроблення нормативних основ з ідентифікації різних видів корупції за допомогою цифрових технологій. Отже, перспективним для подальших наукових розвідок вбачається дослідження в динаміці мультисекторального впровадження ШІ та блокчейну як інструментальних компонент боротьби з корупцією.

REFERENCES

1. International Consortium of Investigative Journalists. 2017. *Explore the Panama Papers Key Figures. Investigations.* URL: https://www.icij.org/investigations/panama-papers/explore-panama-papers-key-figures/

2. International Consortium of Investigative Journalists. 2021. *Pandora papers. Offshore havens and hidden riches of world leaders and billionaires exposed in unprecedented leak. Global Overview*. URL: https://www.icij.org/investigations/pandora-papers/
3. Transparency International. n.d. *What is Corruption?* URL: https://www.transparency.org/en/what-is-corruption
4. United Nations Office on Drugs and Crime. 2004. *United Nations Convention Against Corruption* (UNCAC). URL: https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf
5. United Nations. 2018. The costs of corruption: values, economic development under assault, trillions lost, says Guterres. *UN News* 9 December 2018. URL: https://news.un.org/en/story/2018/12/1027971
6. Transparency International Hravatska. 2020. What is Corruption? URL: https://www.transparency.hr/en/antikorupcija-detalji/what-is-corruption-390
7. United Nations Office on Drugs and Crime. 2014. *Addressing the Links between Corruption and Transnational Organized Crime.* URL: https://www.unodc.org/unodc/en/ngos/CN15-Addressing-the-links-between-corruption-and-transnational-organised-crime.html
8. Organisation for Economic Co-operation and Development (OECD). 2022. *OECD Global Anti-Corruption & Integrity Forum* 30 March - 1 April 2022 URL: https://www.oecd-events.org/gacif2022/
9. International Anti-Corruption Conference (IACC). 2022. *Uprooting Corruption, Defending Democratic Values*. Washington. URL: https://iaccseries.org
10. Indonesia's G20 Presidency 2022. *Priority Issues*. URL: https://www.g20.org/g20-presidency-of-indonesia/#priorities
11. European Commission. 2018. *A Definition of AI: Main Capabilities and Scientific Disciplines*. High-Level Expert Group on Artificial Intelligence. B-1049 Brussels. URL: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf
12. Sharma, V. 2018. Can artificial intelligence stop corruption in its tracks? *World Bank Blogs.* URL: https://blogs.worldbank.org/governance/can-artificial-intelligence-stop-corruption-its-tracks
13. Special Eurobarometer. 2022. *Corruption*. Report. March-April 2022. 523. European Union. http://dx.doi.org/10.2837/110098
14. Transparency International. 2021. *European Union. Global Corruption Barometer*. URL: https://www.transparency.org/en/gcb/eu/european-union-2021
15. Flash Eurobarometer. 2022. Businesses' attitudes towards corruption in the EU. April. *Ipsos European Public Affairs.* Luxembourg: Publications Office of the European Union. http://dx.doi.org/10.2837/474493
16. European Commission. 2015. *Charter for the Introduction and Application of the Arachne Risk Scoring Tool in the Management Verifications*. URL: https://ec.europa.eu/social/BlobServlet?docId=14836&langId=en
17. Neculcea Florin L. and Ninka, Besiana. 2022. *Arachne Interreg survey 2022* URL: https://www.interact-eu.net/download/file/fid/25780
18. European Commission. 2022a. *Regulation of the European Parliament and of the Council on the financial rules applicable to the general budget of the Union (recast)*. Brussels, 16.5.2022. COM(2022) 223 final. 2022/0162(COD). URL: https://eur-lex.europa.eu/legal-content/EN/ TXT/HTML/?uri=CELEX:52022PC0223
19. European Commission. 2022b. *Arachne. What is new in Arachne V2.3?* 18 January 2022. URL: https://ec.europa.eu/social/BlobServlet?docId=25636&langId=en
20. European Anti-Fraud Office. n.d. *Union Anti-Fraud Programme – AFIS component*. URL: https://anti-fraud.ec.europa.eu/policy/union-anti-fraud-programme-uafp/union-anti-fraud-programme-afis-component_en
21. European Commission. 2022c. *Early Detection and Exclusion System (EDES). Anti-fraud measures.* URL: https://commission.europa.eu/strategy-and-policy/ eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/edes_en
22. European Anti-Fraud Office. 2022. *Union Anti-Fraud Programme – IMS component.* URL: https://anti-fraud.ec.europa.eu/policy/union-anti-fraud-programme-uafp/union-anti-fraud-programme-ims-component_en
23. European Parliament. 2021. Proceedings of the workshop on Use of big data and AI in fighting corruption and misuse of public funds - good practice, ways forward and how to integrate new technology into contemporary control framework. *Workshop: Use of big data and AI in fighting corruption and misuse of public funds.* Policy Department D for Budgetary Affairs. Directorate General for Internal Policies of the Union. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/691722/IPOL_STU(2021)691722_EN.pdf
24. European Commission. 2022d.*33rd Annual Report on the Protection of the European Union's financial interests and the Fight against fraud 2021*. Luxembourg: Publications Office of the European Union. URL: https://anti-fraud.ec.europa.eu/system/files/2022-09/pif-report-2021_en_0.pdf
25. European Anti-Fraud Office. n.d. *Union Anti-Fraud Programme (UAFP)*. URL: https://anti-fraud.ec.europa.eu/policy/union-anti-fraud-programme-uafp_en
26. International Consortium of Investigative Journalists. n.d. *Offshore Data Leaks*. URL: https://offshoreleaks.icij.org/pages/about
27. Linkurious. 2016. Panama Papers: *How Linkurious enables ICIJ to investigate the massive Mossack Fonseca leaks*. URL:

https://linkurious.com/blog/panama-papers-how-linkurious-enables-icij-to-investigate-the-massive-mossack-fonseca-leaks/
28. Linkurious. 2021. *A "tsunami of data": the investigative technology behind the Pandora Papers*. URL: https://linkurious.com/blog/technology-pandora-papers-investigation/
29. Köbis, N. C., Starke, C. Edward-Gill, J. 2022. The corruption risks of artificial intelligence. *Transparency International. Working Paper*. URL: https://knowledgehub.transparency.org/assets/uploads/kproducts/The-Corruption-Risks-of-Artificial-Intelligence.pdf
30. Chen, S. 2019. Is China's corruption-busting AI system 'Zero Trust' being turne doff for being too efficient? *Tech in Asia* URL: https://www.techinasia.com/chinas-corruptionbusting-ai-system-trust-turned-efficient
31. Allessie, D., Sobolewski, M., Vaccari, L. 2019. *Blockchain for digital government*. F. Pignatelli (ed.). EUR 29677 EN, Publications Office of the European Union, Luxembourg. doi:10.2760/942739, JRC115049
32. National Agency of Public Registry. 2016. *Improving the security of a government land registry*. Georgia. URL: https://exonum.com/story-georgia
33. European Commission. 2021. *European Blockchain Services Infrastructure*. URL: https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure
34. United Nations. 2017. *UNCITRAL Model Law on Electronic Transferable Records*. Date of adoption: 13 July 2017. New York. URL: https://uncitral.un.org/sites/uncitral.un.org/files/media-
35. International Chamber of Commerce. 2020. *Digital Standards Initiative*. URL: https://www.dsi.iccwbo.org/

Стаття надійшла до редакції 5.05.2022
Стаття рекомендована до друку 16.05.2022.

Nataliya Vinnykova
Professor in Political Science Department V.N. Karazin Kharkiv National University
Maidan Svobody, 4 Kharkiv 61022, Ukraine,
vinnykova@karazin.ua, https://orcid.org/0000-0001-5941-7562

DIGTIAL TECHNOLOGIES IN COMBATING GLOBAL CORRUPTION

A transnationalization of corruption practices, born by globalization processes, is one of nowadays negative phenomenon that deserves intensive studying. Digital technologies smooth the pathways for transnational corruption. On the other hand, digitalization also provides tools for building up respective countermeasures. This article examines the potential of digital technologies, primarily artificial intelligence (AI), in preventing corruption practices.

Firstly, the characteristics of the «global corruption» phenomenon are outlined. The experience of implementing digital technologies in the corruption countermeasures has been analysed that revealed problems and prospective trends in the development of digital anti-corruption mechanisms at the supra-national level of governance. Digital tools for detecting and tracking of transnational corruption schemes were described in the framework of international journalistic investigations or anti-corruption control technologies in the European Union. One of key factors preventing the effective application of AI against the transnational corruption is the lack of the consolidated international regulatory regime for data evaluation. However, AI is ambivalent for both fighting corruption and creation new corruption pathways. Arguments in support of the distributed ledger technologies as the promising corruption-preventing techniques are provided. The study discloses factors inhibiting the scaling of the implementation of blockchain or smart contracts as mechanisms of reducing the risks of corruption. The need to develop international standards for the use of AI technologies in the fight against corruption practices is emphasized. The creation of a transnational structure with appropriate rule-making and control powers in this area becomes extremely important.

Keywords**:** *global corruption, digital technologies, artificial intelligence, blockchain, smart-contracts, global governance, European Union.*

The article was received by the editors 5.05.2022.
The article is recommended for printing 16.05.2022.