



УДК: 342.951: 004.89

ORCID id 0000-0003-2991-3236

DOI <https://doi.org/10.32703/2663-6352/2023-1-13-98-106>**Матвійчук Анатолій Васильович**

доктор юридичних наук, доцент кафедри,

в.о. завідувача кафедри Правосуддя

Юридичного факультету

Інституту управління, технологій та права

Державного університету інфраструктури та технологій,

м. Київ, Україна

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПРОТИДІЇ КОРУПЦІЙНИМ ПРАВОПОРУШЕННЯМ В УМОВАХ СУЧАСНОСТІ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Анотація. Статтю присвячено дослідженню сучасних підходів до протидії корупції, що передбачають застосування новітніх інформаційних технологій, таких як електронне урядування, електронні закупівлі та розробки в галузі штучного інтелекту.

Автор позитивно оцінює результати масового впровадження інформаційних технологій у державний механізм та економічну діяльність, оскільки це дозволило реалізувати можливості дистанційної роботи в умовах заходів щодо протидії пандемії COVID-19 та війни в Україні. Здобутки Міністерства цифрової трансформації України, зокрема у сфері електронізації надання ряду адміністративних послуг та відповідно – зменшення корупційних ризиків, також не викликають сумнівів. Водночас, він наголошує на потребі раціонально оцінювати не лише позитивні, але й негативні аспекти масового впровадження сучасних інформаційних технологій.

Ключовою проблемою, яка призводить до генерації нових корупційних ризиків, на базі впровадження сучасних інформаційних технологій у державний механізм, залишається людський фактор. Навіть технології штучного інтелекту не позбавлені цього недоліка, оскільки розробка програмних комплексів здійснюється людьми, що мають власні інтереси. А необхідність контролю за програмами, що мають потенціал розвитку штучного інтелекту, формує високі повноваження контролюючих осіб, що вже несе в собі нові корупційні ризики.

Акцентовано увагу на особливій небезпеці поширених у програмній та ігровій спільноті «закладок», так званих «Великодніх яєць», що зазвичай мають розважальну природу. Потенціал такого роду «артефактів» несе в собі колосальні корупційні і безпекові ризики, в контексті реалізації проєктів електронного урядування, електронних закупівель і електронного судочинства. Натомість, на прикладі наявних у законодавстві прогалин доведено складність передбачення появи таких загроз.

Запропоновано зосередити увагу на проблематиці прогнозування нових корупційних ризиків у ході законотворчого процесу. Наголошено на необхідності розробки дієвого механізму такого прогнозування.

Ключові слова: протидія корупції; корупційні ризики; інформаційні технології; штучний інтелект; правове регулювання; державна політика; електронне урядування; електронні закупівлі, прогнозування корупційних ризиків.

***Annotation.** The article is devoted to the study of modern approaches to combating corruption, which involve the use of the latest information technologies, such as e-government, e-procurement and developments in the field of artificial intelligence.*

The author positively evaluates the results of the mass introduction of information technologies into the state mechanism and economic activity, as it allowed to realize the possibilities of remote work in the conditions of measures to combat the COVID-19 pandemic and the war in Ukraine. The achievements of the Ministry of Digital Transformation of Ukraine, in particular in the field of electronic provision of a number of administrative services and, accordingly, the reduction of corruption risks, also do not cause doubts. At the same time, he emphasizes the need to rationally evaluate not only positive, but also negative aspects of the mass introduction of modern information technologies.

The key problem that leads to the generation of new corruption risks, based on the introduction of modern information technologies into the state mechanism, remains the human factor. Even artificial intelligence technologies are not without this drawback, since the development of software complexes is carried out by people with their own interests. And the need to control programs that have the potential to develop artificial intelligence creates high powers of controlling persons, which already carries new corruption risks.

Attention is focused on the special danger of "bookmarks", so-called "Easter eggs", which are common in the software and game community, and are usually of an entertainment nature. The potential of this kind of "artifacts" carries enormous corruption and security risks in the context of the implementation of e-government, e-procurement and e-judicial projects. On the other hand, the difficulty of predicting the appearance of such threats has been proven on the example of existing gaps in the legislation.

It is proposed to focus attention on the problem of forecasting new corruption risks during the law-making process. The need to develop an effective mechanism for such forecasting is emphasized.

Keywords: anti-corruption; corruption risks; Information Technology; Artificial Intelligence; legal regulation; state policy; electronic governance; electronic procurement, prediction of corruption risks.

Актуальність теми дослідження. Україна, незважаючи на численні фінансово-економічні та безпекові проблеми, належить до кола держав, які активно впроваджують інформаційні технології не лише у економічні процеси, але і в державний механізм. Діяльність Міністерства цифрової трансформації України (зокрема – в рамках створення та розвитку Порталу «Дія») спрямована не лише на забезпечення доступності цифрового формату отримання ряду адміністративних послуг, але й поступове впровадження повноцінного електронного урядування [1]. Не менше уваги привертають і перспективи розвитку системи державних закупівель ProZorro, покликаної, вперше за історію України, зробити цю галузь доступною для громадського нагляду. Зазначене, відкриває широку палітру

можливостей для збільшення інформаційної відкритості державного управління і реального, а не декларативного, перетворення його на повноцінне публічне адміністрування. Зростають і можливості антикорупційної діяльності як для уповноважених органів, так і для численних представників громадськості.

Не в останню чергу, стрибок у глобальному впровадженні нових інформаційних (і зокрема – телекомунікаційних) технологій відбувся в ході реалізації (з 2020 року) ряду заходів, спрямованих на протидію поширенню COVID-19. Саме нові технології дозволили перевести значну частину роботи у дистанційний формат без втрати (або принаймні – без суттєвої втрати) функціональності. Наразі ж, в Україні, саме вони надають можливість для продовження діяльності в різних галузях економіки в умовах війни.

Водночас, будь-які технології, які створюються, налаштовуються, чи застосовуються за участі людини, залишаються залежними від людського фактору. Тому, чи варто розглядати сучасні інформаційні технології як панацею у реформуванні державного механізму, чи тим більше – у справі протидії корупції? Це та інші питання, і обумовлюють актуальність даного дослідження.

Аналіз досліджень і публікацій щодо обраної тематики. Правова проблематика інформаційного суспільства електронного урядування вже не перший рік є предметом дослідження вітчизняних науковців. Її розглядали у своїх працях: В. Брижко, А. Новицький, В. Цимбалюк та ін. Особливої уваги заслуговують праці таких авторів як С. Шевченко, Н. Сидоренко, які досліджували саме особливості застосування сучасних інформаційних технологій, у якості інструментів протидії корупції.

У процесі дослідження, знайшли своє використання окремі напрацювання таких вітчизняних вчених як О. Амелін, Г. Белінська, О. Вихренко, О. Лусевич, М. Любимов, Д. Чернуха та ряду інших. Автор також торкався окремих аспектів досліджуваної тематики у своїх попередніх працях [2]. Водночас, динаміка розвитку інформаційних технологій обумовлює потребу нових досліджень перспектив їх застосування для протидії корупційним правопорушенням у сучасних умовах.

Мета дослідження: узагальнення проблем правового регулювання застосування інформаційних технологій для протидії корупційним правопорушенням.

Основний зміст дослідження. Корупція, як суспільний феномен, нерозривно пов'язана з державою, її розвитком і трансформацією. Навіть застосування найсучасніших технологій не зменшує важливості системного дослідження феномену корупції та розробки дедалі новіших способів протидії цьому явищу. Автор уже наголошував на доречності вести мову саме про протидію корупції, а не виключно її запобігання, чи боротьбу з нею (на чому аж надто часто акцентує увагу законодавець) [2]. Відповідно до Закону України «Про запобігання корупції» (від 14 жовтня 2014р. № 1700-VII), корупція являє собою «використання особою, (зазначеною у частині першій статті 3 цього ж закону), наданих їй службових повноважень чи пов'язаних з ними можливостей з метою одержання неправомірної вигоди або прийняття такої вигоди чи прийняття обіцянки/пропозиції такої вигоди для себе чи інших осіб або відповідно обіцянка/пропозиція чи надання неправомірної вигоди особі, ... або на її вимогу

іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень чи пов'язаних з ними можливостей». Відтак, ключовими точками генерації корупційних ризиків можна вважати управлінські рішення різного рівня. І саме на цю висхідну точку й орієнтовано більшість антикорупційних заходів.

Якою мірою впровадження цифрових технологій дозволяє зменшити корупційні ризики? І чи дійсно зменшує їх? Не лише технології штучних нейронних мереж (Artificial Neural Network, ANN), штучного інтелекту (Artificial Intelligence, AI) але й технології інтернету речей (Internet of Things, IoT) та великих даних (Big Data Driven, BDD) вже сьогодні набувають тотального застосування. І якщо такі діячі як Ілон Маск (Elon Musk) застерігають, щодо небезпеки неконтрольованого застосування технології штучного інтелекту (AI) з точки зору їх впливу на працевлаштування і національну безпеку [3], то чи враховується їх роль у формуванні нових можливостей для корупції? Адже, за принципом діалектичної суперечності, розвиток та тотальне впровадження інформаційних технологій несе в собі не лише переваги та нові інструменти для протидії корупції, але й нові корупційні ризики.

В умовах дедалі ширшого застосування сучасних технологій генерування, передачі, обробки та збереження інформації в усіх сферах суспільних відносин, у тому числі – в діяльності органів державної влади, формується й нове коло корупціогенних факторів. Як уже зазначалося, підвищення інтенсивності застосування інформаційних технологій колосально розширює комунікативні можливості, що набуває особливої гостроти у форматі дистанційної роботи. І нормотворець враховує цей момент, передбачаючи можливість використання засобів телекомунікаційного зв'язку в ряді процедур, де раніше вимагалася фізична присутність посадової особи, або наявність фізичних носіїв інформації. Звісно, такий підхід розширює можливості практичної діяльності посадових осіб, що було особливо актуально в умовах заходів, спрямованих на подолання пандемії COVID-19, і є не менш актуальним сьогодні в Україні, як країні, де йде війна. Та водночас – законотворець не завжди може врахувати тенденції розвитку технологій, а отже і функціонал, який не будучи достатньо унормованим, відкриває перед потенційним правопорушником нечувані раніше можливості для зловживань.

До прикладу, вітчизняний дослідник інформаційно-правового регулювання діяльності органів прокуратури О. Амелін, уже звертав увагу на особливості тлумачення норм «Порядку фіксації доведення інформації або документів до відома державного службовця шляхом використання засобів телекомунікаційного зв'язку» (затвердженого Постановою Кабінету Міністрів України від 11 грудня 2019 р. № 1042), покликаного визначити процедуру фіксації доведення інформації або документів до відома державного службовця шляхом використання засобів телекомунікаційного зв'язку відповідно до вимог Закону України «Про державну службу» (від 10 грудня 2015р № 889-VIII).

Серед іншого, дослідник наполягав на потребі оптимізації чинних норм «Порядку фіксації доведення інформації або документів до відома державного службовця шляхом використання засобів телекомунікаційного зв'язку», з огляду на технічну можливість зловживань (з боку керівництва) функціональними особливостями деяких месенджерів (Telegram, Viber), які, зважаючи на надійне

шифрування та зручність користування (надсилання текстової, фото- та відеоінформації), набувають дедалі більшої популярності. Він доволі детально обґрунтовує це тим, що у зазначених сервісах є доступною функція знищення надісланого повідомлення не лише у відправника, але й у адресата. Така технічна можливість дозволяє надіслати повідомлення, зробити «копію знімку екрану засобу телекомунікаційного зв'язку», скласти «протокол про доведення інформації або документів до відома державного службовця», а потім видалити повідомлення (у тому числі – у адресата). Наведений порядок дій дає змогу відправнику підтвердити факт надсилання повідомлення, при цьому – унеможливити його отримання адресатом [4]. Такий варіант зловживання був технічно неможливий при застосуванні e-mail листування (за винятком варіанту видалення листа у адресата при фізичному чи програмному доступі до його пристрою). І це лише один приклад, коли оновлення технології відкриває лазівку, яка не була передбачена в ході нормотворчості, а отже, не могла бути обмежена в принципі.

Ще одним із важливих секторів електронного урядування та водночас електронного бізнесу, який містить значні корупційні ризики, можна вважати сектор «Business to Government» (або ж – B2G). B2G – це бізнес-модель, за якої компанія продає продукти, послуги або інформацію державним або місцевим органам влади (переважно – за тендерною системою).

На практиці, модель B2G передбачає взаємодію бізнесу та адміністрації і включає ділові зв'язки комерційних структур із державними організаціями, починаючи від місцевої влади й закінчуючи міжнародними організаціями. Доволі поширений у Західній Європі та США, цей вид взаємодії бізнесу і держави з 2016 року почав важливий етап розвитку в Україні, з введенням у дію системи електронних державних закупівель ProZorro (дорогу якій відкрив Закон України «Про публічні закупівлі» від 25 грудня 2015 р. № 922-VIII). З того часу торги здійснюються через авторизовані електронні майданчики системи ProZorro, і їх кількість постійно зростає [5]. Доволі красномовним свідченням обсягів діяльності системи є свіжа інформація про закупівлі для Міністерстві оборони України, що відбулися вперше з початку повномасштабного вторгнення. За даними представниць Громадської антикорупційної ради при Міністерстві оборони Дани Ярової і Тетяни Ніколаєнко, попередньо сума, на яку проторгували, складає 18,3 млрд гривень. При цьому заощаджені державні кошти склали 6,3 млрд гривень, або 25,6% [6]. І звісно ж, такі результати можна сприймати виключно позитивно. Збільшення прозорості державних закупівель однозначно зменшує певну категорію корупційних ризиків. Однак, останніми роками неодноразово мали місце скандальні ситуації у цій сфері, що свідчить про наявність у діяльності системи закупівель серйозних проблем, незважаючи на запроваджені технології.

Недоліки в системі публічних закупівель уже розглядали в своїх працях ряд вітчизняних дослідників – Г. Белінська, О. Вихренко, М. Лусевич, М. Любимов, Д. Чернуха та ін. Тому детально зупинятися на них немає сенсу. Зазначимо лише, що серед проблем, пов'язаних із конкретними етапами процесу закупівлі, Г. Белінська виокремлює: проблему планування закупівель (оскільки вже

під час планування обсягу закупівель та їх номенклатури з'являється можливість лобіювати конкретне рішення, як наслідок – закупівельники приймають рішення про купівлю товарів чи послуг на користь «зацікавлених» осіб, не враховуючи вигід або втрат держави); проблему предмета закупівлі; проблему кваліфікаційної відповідності учасників; проблему прозорості процедури проведення тендера; проблему непрозорості процедури підписання договору; проблему оплати за виконаним договором; проблему прийняття товару [7]. Нескладно помітити, що система електронних державних закупівель ProZorro вирішує лише частину перелічених проблем.

Натомість, М. Любимов, О. Вихренко, М. Лусевич, окрім зазначених проблем, пов'язаних із конкретними етапами процесу закупівлі, акцентують увагу на загальних проблемах здійснення публічних закупівель в Україні. До таких вони відносять, у першу чергу, низький рівень кваліфікації учасників. Наслідками цього може стати некоректно складена тендерна пропозиція, яка містить некоректну специфікацію або неадекватну ціну, що може або унеможливити виконання тендерних вимог, або ж призведе до закупівлі за завищеними цінами [5]. Ще один дослідник проблем функціонування системи закупівель, Д. Чернуха, ретельно проаналізувавши саме діяльність системи ProZorro, додає до цього переліку такі недоліки функціонування системи як: демпінг цін, саботування тендерів, зловживання правом замовника і акцентування уваги лише на ціні товару [8]. На жаль, комп'ютерна програма, сама по собі, не здатна надавати раціональну оцінку. «Кібероптимістам», які переконані, що розвиток систем штучного інтелекту (AI) «вирішить всі проблеми», варто звернути увагу на реалії функціонування вже існуючих систем, які наближаються до рівня AI. Всесвітньо відомий проєкт корпорації OpenAI «ChatGPT» (у якому багато оглядачів вбачають зародження реального AI), в ході спілкування відверто визнає, що не послуговується жодними законами і правилами крім тих, які закладаються його розробниками. При цьому, наївно заявляє, що його розробники – «неодмінно законослухняні громадяни, і не будуть примушувати його порушувати закон» [9].

В цьому моменті криється ще один вагомий ризик – ризик прихованого неправомірного впливу на діяльність будь-якого програмного комплексу, з боку розробників і модераторів. І якщо в когось є ілюзії, що цьому завадить існуюча правоохоронна система – їх очікує страшне розчарування. В галузі програмування та ігрової індустрії доволі давно (щонайменше – з 1980-х років) існує поняття «Великодніх яєць» (від англ. Easter egg), «закладок», що є прихованими секретами у медійному або програмному продукті (програмному забезпеченні, відеоіграх, сайтах тощо) [10]. Зазвичай така «закладка» слугує своєрідною винагородою для уважних користувачів. Вона не є важливою чи обов'язковою для цих продуктів і використовується лише задля жарту. Найчастіше «закладки» є зовсім відмінними від змісту продукту, чи навіть виглядають безглуздо. Щоб «отримати» таке «Великоднє яйце», потрібно зробити щось нестандартне, нетривіальне в контексті гри або задіяти непередбачувану комбінацію клавіш у програмному забезпеченні.

Але що заважає розробнику застосувати корисливу «закладку», знаючи, що її ніхто не знайде, а коли настане час і будуть виконані умови, вона спрацює? Виключно його совість? А хто може гарантувати, що такі закладки (які почасти дуже складно виявити, з огляду на першопочаткову невизначеність інформації навіть щодо їх наявності) вже не вбудовані в програмне забезпечення електронного уряду, чи електронних закупівель? Адже, з огляду на унікальність таких систем і складність аналізу їх коду сторонньою особою (чи навіть іншою програмою), можливість оперативного виявлення таких «Easter egg» (наприклад – правоохоронцями, чи тим більше – громадськістю) наближається до нуля. І які загрози вони в собі можуть приховувати – питання риторичне.

Відтак, доволі наївно було б розглядати інформаційні технології, виключно у якості перспективного інструменту протидії корупції. З огляду на колосальну динаміку розвитку цієї галузі та її трансформаційний потенціал, і з урахуванням домінування у ній (щонайменше – у короткостроковій перспективі) ролі людського фактору, вона несе в собі нечувані раніше корупційні ризики. Підступність цих корупційних ризиків обумовлена особливостями якісного переходу у сфері розвитку інформаційних технологій та зростання обсягів їх застосування.

Як уже зазначалося, з приводу неврахування авторами «Порядку фіксації доведення інформації або документів до відома державного службовця шляхом використання засобів телекомунікаційного зв'язку» (затвердженого Постановою Кабінету Міністрів України від 11 грудня 2019 р. № 1042) технічних можливостей нових месенджерів, законотворцю складно протидіяти принципово новим можливостям зловживання, без належного їх розуміння, прогнозування їх появи та усвідомлення корупційного потенціалу. Якщо й не неможливо, то щонайменше – дуже складно протидіяти тому, чого ще немає, і тим більше тому, що ти навіть не можеш собі уявити.

Звісно, декому може спасти на думку, що держава здатна просто заборонити абсолютно всі потенційно шкідливі прояви інформаційних технологій. До речі, історія знає чимало прикладів введення тих чи інших заборон не лише на рівні державного управління, але і в науковій сфері (яка, здавалося б, мала бути найбільш динамічною і відкритою для розуміння інновацій). Французькі науковці XVIII ст. забороняли визнавати падіння метеоритів, а більшовицькі адміністратори у середині XX століття – забороняли визнавати науками генетику і кібернетику. Та всі вони програли суд історії. І навряд чи цю проблему на практиці можна вирішити повністю. Однак, є шляхи її раціонального обмеження. Наприклад – шляхом впровадження перспективних механізмів прогнозування корупційних ризиків.

Висновки. В результаті узагальнення досліджуваної теми, варто визнати, що доцільно вести мову радше не про проблематику застосування інформаційних технологій для протидії корупції, а про проблематику правового регулювання застосування інформаційних технологій, в контексті протидії корупції.

Це обумовлено не лише невпинністю та невідоротністю подальшого розвитку інформаційних технологій, впровадженням таких складових електронної держави як електронне урядування,

електронні закупівлі тощо, але й невід'ємністю людського фактору, що формує нові корупційні ризики на системній основі.

Окрім безпосередніх недоліків електронізації державного механізму, таких як наявність програмних помилок, збоїв, відсутність розуміння програмою ситуації, відсутність у програми емпатії (що в сукупності може призвести до суперечності між діяльністю програми електронного урядування, закупівель, чи судочинства і реалізацією норм Конституції України), загрозу становлять потенційні умисні дії розробників програмного забезпечення.

Проблема ж протидії корупційним ризикам, які несуть у собі нові інформаційні технології, це є концептуальна проблема системного характеру, яка тягне за собою нагальну потребу перегляду існуючого механізму законотворчості. У даному контексті, перспективним видається просування ідеї розвитку у законотворчому механізмі прогностичної складової, орієнтованої на врахування (у межах можливого) всіх потенційних загроз та песимістичних сценаріїв використання прогалін у законодавстві, з метою майбутнього зловживання можливостями, що відкривають інформаційні технології, в корупційних цілях.

Дана проблематика заслуговує окремої уваги науковців, як і проблематика впровадження цифровізації судочинства в Україні. При цьому, зазначені питання ще очікують своїх дослідників як у галузі інформаційних технологій, так і в галузі публічного адміністрування і права.

Література:

1. Портал Дія. Цифрова держава. URL : <https://plan2.diia.gov.ua/> (дата звернення: 01.06.2023)
2. Матвійчук А. В. Сучасні інформаційні технології, як інструмент протидії корупційним правопорушенням. «Глобалізація українського законодавства як результат війни Російської Федерації проти України»: Матеріали XIII Міжнародної науково-практичної конференції. Київ. ДУІТ, 2023. С. 171-176.
3. Elon Musk among experts urging a halt to AI training. BBC News. 30 March 2023. URL : <https://www.bbc.com/news/technology-65110030> (Дата звернення 01.06.2023р.)
4. Амелін О. Ю. Інформаційне забезпечення діяльності органів прокуратури України: адміністративно-правовий аспект: монографія. Науково-теоретичне видання. Київ: Видавництво Людмила, 2021. 224 с. URL:http://library.iapm.edu.ua/free_books/Mono_Amelin2021.pdf
5. Любимов М. О., Вихренко О. А., Лусевич М. С. та ін. Актуальні проблеми й напрями оптимізації публічних закупівель в Україні. Науковий вісник Полтавського університету економіки і торгівлі. 2020. № 4 (100). С. 33-39. URL: <http://journal.puet.edu.ua/index.php/nven/article/viewFile/1795/1848> (дата звернення: 07.06.2023)
6. Гліб Іванов. Перші торги на Prozorro для Міноборони зекономили державі 6 мільярдів грн, – Ярова. Obozrevatel. 06.06.2023. Вилучено з URL : <https://news.obozrevatel.com/ukr/society/pershi-torgi-na-prozorro-dlya-minoboroni-zekonomili-derzhavi-6-milyardiv-grn.htm> (дата звернення: 07.06.2023)

7. Белінська Г. В. Актуальні проблеми державних закупівель в Україні в умовах реформування. Вісник Кременчуцького національного університету імені Михайла Остроградського. 2016. Вип. 5. С. 125–131. URL: http://nbuv.gov.ua/UJRN/Vkdpu_2016_5_20. (дата звернення: 07.06.2023)
8. Чернуха Д. В. Проблеми функціонування та перспективи розвитку системи державних закупівель ProZorro. Молодий вчений. № 11 (63). листопад, 2018 р. С. 1231-1234. URL : <http://molodyvcheny.in.ua/files/journal/2018/11/282.pdf> (дата звернення: 01.06.2023)
9. Introducing ChatGPT. OpenAI. URL : <https://openai.com/blog/chatgpt> (дата звернення: 01.06.2023)
10. Kabay, M. E. (27 March 2000). "Easter eggs and the Trusted Computing Base". Network World. Archived from the original on 15 June 2006. Retrieved 4 November 2017. URL : <https://www.networkworld.com/article/2309980/bill-addresses-consumer-privacy-protection.html> (дата звернення: 01.06.2023).