

# ПРОБЛЕМИ ПРИВАТНОГО ПРАВА

УДК 347.1:[004.8+334.7]

DOI: <https://doi.org/10.31359/1993-0909-2026-33-1-220>

**Оксана Мар'янівна Вінник**

*Національна академія правових наук України  
Харків, Україна*

*Інститут правотворчості та науково-правових експертиз  
Національної академії наук України  
Київ, Україна  
<https://orcid.org/0000-0002-9397-5127>*

**Марина Миколаївна Великанова**

*Інститут правотворчості та науково-правових експертиз  
Національної академії наук України  
Київ, Україна,*

*Київський національний університет імені Тараса Шевченка  
Київ, Україна  
<https://orcid.org/0000-0003-1845-6500>*

## РИЗИКИ ЦИФРОВІЗАЦІЇ ТА ПАРТНЕРСТВА: ПРАВОВИЙ АСПЕКТ

**Анотація.** *Стаття присвячена дослідженню категорії ризику в сучасних суспільних відносинах, що суттєво ускладнилися під впливом глобальної цифровізації та повномасштабної агресії РФ проти України. У статті наголошується на необхідності розробки нового правового інструментарію для управління ризиками, які загрожують національній безпеці та економічній стабільності. Метою статті є розробка пропозицій щодо напрямів удосконалення законодавства України для мінімізації негативних наслідків ризиків, пов'язаних із запровадженням штучного інтелекту та реалізацією проєктів публічно-приватного партнерства в період війни та повоєнного відновлення. У роботі використано комплекс загальнонаукових та спеціальних методів, зокрема: діалектичний – для розкриття сутності ризику; порівняльно-правовий – для аналізу відповідності українського законодавства Регламентом ЄС (AI Act та Регламент 2021/2085); прогностичний – для моделювання ефектів від запровадження нових форм інвестування. Авторами обґрунтовано необхідність адаптації європейського досвіду (AI Act) до українських реалій шляхом запровадження класифікації систем штучного інтелекту за рівнем ризику та закріплення «цифрових прав» особи в Цивільному кодексі України. Вказано на недосконалість чинного Закону України «Про публічно-приватне партнерство», який обмежується лише договірною формою партнерства. Доведено переваги інституційної форми публічно-при-*

ватного партнерства (створення спільних підприємств), що дозволить залучати дружні держави як публічних партнерів. Це забезпечить прозорість, посилить контроль за цільовим використанням коштів та мінімізує корупційні ризики. Зроблено висновок, що мінімізація сучасних ризиків потребує системного оновлення законодавства. Запропоновано розширити суб'єктний склад публічних партнерів у проєктах публічно-приватного партнерства та запровадити механізми розподілу відповідальності за шкоду, завдану автономними системами штучного інтелекту.

**Ключові слова:** приватне право; публічно-приватне партнерство; євроінтеграція; штучний інтелект; ризик; відповідальність; приватноправові відносини; захист прав; інвестиції.

**Oksana M. Vinnyk**

National Academy of Legal Sciences of Ukraine  
Kharkiv, Ukraine

Institute of Lawmaking and Scientific and Legal Expertise  
National Academy of Sciences of Ukraine  
Kyiv, Ukraine  
<https://orcid.org/0000-0002-9397-5127>

**Maryna M. Velykanova**

Institute of Lawmaking and Scientific and Legal Expertise  
National Academy of Sciences of Ukraine  
Kyiv, Ukraine

Taras Shevchenko National University of Kyiv  
Kyiv, Ukraine  
<https://orcid.org/0000-0003-1845-6500>

## RISKS OF DIGITALIZATION AND PARTNERSHIP: LEGAL ASPECTS

**Abstract.** *The article explores the category of risk within modern social relations, which have become significantly more complex under the influence of global digitalization and the full-scale aggression of the Russian Federation against Ukraine. The study emphasizes the necessity of developing a new legal toolkit for risk management that poses threats to national security and economic stability. The purpose of the article is to develop proposals for improving Ukrainian legislation to minimize the negative consequences of risks associated with the implementation of artificial intelligence (AI) and the execution of public-private partnership (PPP) projects during the period of war and post-war reconstruction. The research employs a complex of general scientific and specialized methods, in particular: the dialectical method – to reveal the essence of risk; the comparative-legal method – to analyze the alignment of Ukrainian legislation with EU Regulations (the AI Act and Regulation 2021/2085); and the predictive method – to model the effects of introducing new investment forms. The authors justify the necessity*

*of adapting European experience (the AI Act) to Ukrainian realities by introducing a classification of artificial intelligence systems based on their risk level and enshrining individual «digital rights» within the Civil Code of Ukraine. The study points out the deficiencies of the current Law of Ukraine «On Public-Private Partnership,» which is limited solely to the contractual form of partnership. The advantages of the institutional form of public-private partnership (the creation of joint ventures) are proven, which would allow for the involvement of friendly states as public partners. This approach will ensure transparency, strengthen control over the targeted use of funds, and minimize corruption risks. It is concluded that minimizing modern risks requires a systemic update of legislation. It is proposed to expand the composition of public partners in public-private partnership projects and to introduce mechanisms for the allocation of liability for damage caused by autonomous artificial intelligence systems.*

**Keywords:** private law; public-private partnership; European integration; artificial intelligence; risk; liability; private law relations; protection of rights; investments.

## ВСТУП

Ризик, супроводжуючи будь-яку діяльність суб'єктів, так чи інакше впливає на суспільні відносини, створюючи ймовірність небажаного перебігу справ у приватних, публічних або змішаних – публічно-приватних відносинах.

Ризик характеризують: його причина (подія, ймовірність якої може бути врахувана, а час та місце її виникнення точно визначити неможливо, оскільки вона зумовлена зовнішніми (навколишнє середовище) та внутрішніми (суб'єктивні особливості осіб, що її визначають) чинниками; джерела ризику (ними можуть бути: певні явища, предмети, процеси, що зумовлюють ризики (через неможливість передбачення ймовірності певного результату, зумовлених складністю соціально-економічних та технологічних процесів): суперечливість інтересів і тенденцій (наприклад, конкуренція), інформаційна обмеженість (неповнота чи недостатня якість/суперечливість інформації); неможливість повного пізнання об'єктів, процесів та явищ; різноманітність соціально-психологічних установок та оцінок осіб у процесі прийняття рішень; наслідки (негативні, що можуть становити небезпеку, та позитивні [1]). Тому категорія ризиків (особливо тих, що можуть породити вкрай небезпечні наслідки), кількість яких у сучасному світі зростає, потребує відповідного дослідження та напрацювання ефективного правового інструментарію для обмеження обсягу ризиків або встановлення правил оптимального їх розподілу. На жаль, до останнього часу на цьому належним чином не акцентувалася увага законодавця, попри низку випадків, серед яких: покладення ризику випадкового знищення або пошкодження майна на власника, якщо інше не передбачено договором або законом [2, ст. 323], ризики в підрядних та деяких інших відносинах [2, статті 837, 842, 879, 880 та ін.; 3, ч. 4 ст. 12].

Об'єктивна категорія ризику, «зміст якої полягає в можливості настання несприятливих наслідків незалежно від поведінки осіб» [4], у сучасних умовах зростання загроз, у тому числі пов'язаних із цифровізацією, війною, досі злободенною проблемою корупції та інших зловживань у процесі інвестування [5; 6; 7] та необхідністю подолання їх наслідків, потребує системного підходу до обме-

ження обсягу ризиків або оптимального їх розподілу за допомогою правових інструментів, про що, зокрема, свідчить реакція ЄС на ризики цифровізації та необхідність мінімізації як самих ризиків, так їх наслідків [8].

Проблемі ризиків присвячено чимало наукових праць, серед яких:

– дисертаційні дослідження з аналізом стану та перспектив формування правового механізму обмеження та розподілу ризиків у приватних відносинах (М. Великанової [9]), з акцентом на проблему ризиків у договірних відносинах (О. Андрєєвої [10]);

– наукові статті, в яких акцентується увага на ризиках у підрядних договірних відносинах (А. Іванов, А. Іванюк та ін. [11]), співвідношенню ризиків та відповідальності в приватному праві (Н. Дубицька [12]), економічній складовій ризику в підприємницькій діяльності (Р. Скриньковський, Ю. Тиркало [13]), необхідності ширшого віддзеркалення категорії ризиків у цивільному праві в умовах цифровізації (М. Великанова [14]) тощо;

– матеріалів конференцій (О. Вінник [15]) та ін.

Разом із тим складність і динамізм сучасних суспільних відносин зумовлюють необхідність системного підходу до встановлення загальних правил та закріплення належного інструментарію для виявлення, оцінки та мінімізації ризиків із огляду на збільшення негативних проявів ризиків, що призводять до завдання шкоди суспільним інтересам і основоположним правам людини. Це стосується, зокрема, таких надбань цифровізації, як штучний інтелект, широке й неконтрольоване застосування якого може призвести до критичних для людства наслідків. У зв'язку з цим низка визнаних у світі вчених закликають навіть до заборони його застосування, вказуючи на ймовірність втрати над ним контролю збоку людства [16]. Євросоюз одним із перших відреагував на ризики використання технологій штучного інтелекту, прийнявши Регламент 2024/1689 [8]. Реакцією України на цей акт ЄС стала розробка відповідного законопроекту, з урахуванням не лише зазначеного Регламенту, а й український реалій [17; 18].

Другою проблемою, пов'язаною з потребою мінімізації ризиків в умовах війни і повоєнної відбудови, є корупційні й інвестиційні ризики у відносинах публічно-приватного партнерства (далі – ППП) в Україні.

Нагальність впливу на такі ризики з метою їх зменшення зумовлена не лише їх «традиційністю» для нашої країни, яку дехто пов'язує з нібито національними традиціями вдячності, а й умовами війни, отриманням Україною донорської допомоги від дружніх держав, відносинами публічно-приватного партнерства, на яке покладаються великі надії. Нецільове (або псевдо цільове) використання допомоги та інвестицій знецінює їх ефективність, шкодить репутації нашої держави, а головне – зменшує ефект від добрих починань, завдаючи шкоди державі та її громадянам.

Використання економіко-правового механізму ППП, на яке покладаються великі надії щодо залучення коштів на повоєнну відбудову, має забезпечуватися відповідними правовими засобами запобігання зловживань, зокрема передбаче-

ними в Регламенті ЄС 2021/1689 [19], а також правовими засобами, що забезпечать залучення дружніх держав як публічних партнерів за інституційною/корпоративною формою ППП з відповідними вимогами до неї.

Проте в українському законодавстві, попри необхідність урахування євроінтеграційної складової, передбачено лише договірну форму ППП [20, ст. 5] з досить поміркованими можливостями контролю за цільовим та ефективним використанням коштів партнерів, а також донорської допомоги. Відтак *метою цієї статті* є напрацювання пропозицій щодо вдосконалення правових механізмів запобігання або мінімізації негативних наслідків ризиків цифровізації (зокрема пов'язаних із застосуванням штучного інтелекту (ШІ) та ризиків у відносинах публічно-приватного партнерства. Це особливо важливо в надскладних умовах війни, повесної відбудови, а в підсумку – для посилення всіх складових національної безпеки та забезпечення добробуту громадян України.

Для досягнення поставленої мети необхідно проаналізувати чинні правові інструменти впливу на ризик, що виникає в суспільних відносинах у нинішніх умовах війни, розв'язаної російською державою, наслідки реалізації ризиків та нагальні проблеми, що заважають їхньому подоланню чи мінімізації; з'ясувати особливості сучасних ризиків (з акцентом на ризики цифровізації та інвестування у формі ППП) в суспільних відносинах та пов'язаний із цим стан правового регулювання; виявити прогалини та інші вади, що заважають оптимально впливати на ризики; запропонувати шляхи їх вирішення з використанням досвіду ЄС.

## 1. МАТЕРІАЛИ ТА МЕТОДИ

Методологічну основу цього дослідження склали методи та прийоми наукового пізнання, комплексне застосування яких дозволило здійснити ґрунтовний аналіз фактичного стану та правового забезпечення відносин із елементами ризиків, виявити їх різновиди залежно від ступеня користі та/або небезпеки для суспільного розвитку.

У процесі здійснення цього дослідження використовувалася низка філософсько-світоглядних, загальнонаукових і спеціально-наукових методів.

Використання *діалектичного методу* дало можливість розкрити сутність ризиків у суспільних відносинах (особливо, пов'язаних із цифровізацією та використанням економіко-правового механізму публічно-приватного партнерства), а *формально-логічний* метод дозволив виділити ті характеристики відносин, що свідчать про наявність у них певного ступеня ризику, щоб їх класифікувати за цією ознакою. Метод *аналізу* використано при вивченні наукових напрацювань у сфері дослідження ризиків як вітчизняних, так і зарубіжних учених і практиків, стану правового регулювання відповідних суспільних відносин в Україні та ЄС. За допомогою методу *синтезу* було зроблено висновки щодо ефективності наявних у вітчизняному законодавстві правових механізмів для подолання або зменшення негативних наслідків ризиків у вищезазначених відносинах.

У дослідженні використаний *порівняльний* метод, що серед іншого дав змогу порівняти ступінь ефективності правового регулювання відносин, пов'язаних із ризиками цифровізації та інвестування у формі публічно-правового партнерства, в праві України та ЄС. *Синергетичний* метод використано для встановлення впливу ступеня ризику на вимоги щодо застосування цифрових технологій (зокрема штучного інтелекту) та корупційно-інвестиційних ризиків при реалізації проєктів ППП, а метод *системного аналізу* – при визначенні взаємозв'язку процесів посилення боротьби з корупцією та іншими зловживаннями в процесі інвестування у формі публічно-приватного партнерства з вимогами до ППП, включно з його формою (суто договірна чи інституційна, для якої характерним є поєднання корпоративних і договірних відносин).

*Прогностичний* метод став у нагоді при прогнозуванні можливих ефектів запровадження інституційної форми ППП та класифікації, пов'язаних із цифровізацією ризиків. Це дозволило встановити критерії можливості, обмеження чи заборони застосування відповідної форми ППП із урахуванням ступеня можливих негативних наслідків для суспільства, його членів. Використання *формально-юридичного* методу як одного зі спеціально-наукових методів дало змогу з'ясувати зміст правових норм, що регулюють відносини у відповідній сфері, їх місце в системі права України, а також виробити рекомендації щодо вдосконалення чинного законодавства України з питань встановлення критеріїв поділу ризиків за ознакою їх ймовірних наслідків (насамперед негативних) для суспільства та його членів (приватних партнерів у відносинах ППП, юридичних і фізичних осіб, на яких впливають ризики цифровізації).

Застосування *порівняльно-правового* методу пов'язане з необхідністю врахування євроінтеграційного напрямку вдосконалення законодавства України і, відповідно, порівняння ступеня ефективності правового регулювання зазначених відносин в ЄС та Україні, а в підсумку – напрацювання рекомендацій щодо врахування досвіду Євросоюзу в процесі вдосконалення відповідного законодавства України.

## 2. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Стрімкі темпи запровадження цифрових технологій у всі основні сфери суспільного й значною мірою приватного життя забезпечили низку незаперечних переваг, що стали в пригоді в період коронавірусної пандемії й повномасштабної війни, розв'язаної російською державою проти України. Подібні технології створюються/вдосконалюються зазвичай із використанням штучного інтелекту, який, крім незаперечних переваг (насамперед – можливість надшвидкої обробки інформації, прийняття на підставі результатів її аналізу оптимальних рішень), може становити значну небезпеку для суспільства й приватного життя громадян у разі його використання з недобросовісною метою та/або без належного контролю з боку людини. Означена проблема стає вельми актуальною з огляду на недалеку пер-

спективу втрати такого контролю, про що не лише попереджають провідні вчені, а й закликають до вжиття кардинальних заходів на кшталт заборони його використання в певних випадках [16].

Євросоюз одним із перших відреагував на проблеми з використання ШІ, прийнявши відповідний Регламент 2024/1689 (Artificial Intelligence Act, далі – AI Act [8]). Україна, попри констатацію необхідності врегулювання використання ШІ у відповідному підзаконному акті [21], підписання Рамкової конвенції про штучний інтелект та права людини [22], що визначає принципи, яких держава має дотримуватися у формуванні законодавства та застосуванні ШІ-продуктів у публічному секторі, аналітичних матеріалів Міністерства цифрової трансформації щодо оптимального підходу до регулювання технологій штучного інтелекту в Україні [23], досі не прийняла ґрунтовний Закон про ШІ на зразок AI Act [8], хоча про проект такого акту є згадки в мережі Інтернет [17]. AI Act є одним із перших в світі правових актів, який покликаний регулювати використання штучного інтелекту, визначаючи кілька категорій ШІ залежно від ступеня їх ризику (системи ШІ *неприйняттого ризику*, що забороняються; системи ШІ з *високим рівнем ризику*, які підлягають суворим вимогам, перш ніж їх можна буде вивести на ринок; ШІ *обмеженого ризику*, що пов'язаний із необхідністю прозорості щодо його використання; ШІ *мінімального або відсутнього ризику*, для застосування якого не запроваджуються обмеження).

І. І. Забокрицький [24], аналізуючи AI Act, підкреслює важливість його для євроінтеграційного курсу України, оскільки положення AI Act можуть (і мають) лягти в основу українського законодавства, предметом регулювання якого будуть пов'язані з використанням штучного інтелекту відносини. Визначення досить широкого кола суб'єктів у цьому акті, як зазначає дослідник, дає змогу гнучко підходити до правового регулювання штучного інтелекту – запобігати ризикам не обмежуючи ті випадки, коли використання таких систем є доцільним і корисним для суспільства. Разом із тим розробники українського варіанту проекту подібного акта підкреслюють урахування в ньому української специфіки [17], особливості якої поки що не можна визначити через відсутність широкого оприлюднення цього документа для обговорення. Проте маємо Рекомендації з відповідальної розробки систем із використанням технологій штучного інтелекту, розроблені фахівцями Мінцифри за участі низки зарубіжних і міжнародних організацій [18].

Стрімке поширення використання ШІ в Україні, його важливість для цифрового розвитку інноваційної діяльності, а також складність ШІ з точки зору наслідків його використання для суспільства і необхідності попередження зумовлених ним ризиків – яскраве свідчення необхідності прийняття подібного закону, оскільки наша держава прагне до членства в ЄС, а, отже, положення AI Act для неї вкрай важливі з точки зору адаптації вітчизняного законодавства до права ЄС.

Загалом використання цифрових технологій гостро потребує правового забезпечення, що враховує ризики, які виникають при застосуванні таких технологій.

Насамперед це стосується встановлення меж (обмежень) щодо їх використання залежно від ступеня ризику, що віддзеркалено в AI Act. Крім прийняття спеціального закону на кшталт AI Act, необхідно розвинути положення про «цифрові права» особи як різновиду особистих немайнових прав, що створюють можливість реалізації інтересів у сфері діджиталізації; чіткіше врегулювати особливості здійснення та захисту особистих немайнових прав, якими наділені особи, котрі мають спеціальні правові статуси (правові модуси), зокрема, цифрова (електронна) особа; доповнити чинний ЦК України серед іншого положеннями щодо (1) відшкодування шкоди, завданої шкідливим програмним забезпеченням; (2) відшкодування шкоди, завданої робототехнікою та штучним інтелектом. На цьому було наголошено робочою групою з рекодифікації цивільного законодавства України [25, с. 18, 51]. Такий підхід, на нашу думку, допоможе запобігти прикрим випадкам нехтування небезпекою при застосуванні цифрових та інших сучасних технологій (зокрема, біотехнологій), які надають величезні можливості вирішення складних проблем, хоча часом застосовуються безвідповідально та/або непрофесійно, нехтуючи ймовірністю настання негативних наслідків.

Видається доцільним підтримати висловлену позицію, що розв'язання проблем правового регулювання використання цифрових технологій, забезпечення захисту прав і законних інтересів фізичних та юридичних осіб від порушень із застосуванням цифрових технологій та притягнення до відповідальності за шкоду, завдану застосуванням цифрових технологій лежить у площині модернізації чинного законодавства в таких напрямках: 1) вирішення питання відповідальності за шкоду, завдану штучним інтелектом, виходячи з того наскільки такий штучний інтелект був автономним; 2) застосування правил відшкодування шкоди, завданої джерелом підвищеної небезпеки, до відносин із використанням цифрових технологій, виходячи з того, чи була шкода, завдана дією чи бездіяльністю штучного інтелекту, передбачуваною [14, с. 158].

Наступна порушена в цій статті проблема – ризику публічно-приватного партнерства, що забезпечує інвестування складних і високовартісних інвестиційно-інноваційних проєктів. Нещодавно прийнятий Закон «Про публічно-приватне партнерство» [20] (як нова версія Закону «Про державно-приватне партнерство» [26]) містить чимало нових положень, спрямованих на вдосконалення відносин такого партнерства. Проте у цьому законі належним чином не враховано положення Регламенту 2021/2085, особливості якого полягають (серед іншого) у двох основних питаннях: участі на стороні публічного партнера кількох дружніх держав та інституційній формі такого партнерства, яка забезпечує постійний контроль за перебігом внесення інвестицій та реалізацією проєкту/проєктів ППП. Ці особливості вельми важливі з огляду на таке.

По-перше, це стосується обсягу інвестицій. Участь кількох дружніх держав разом із Україною як публічних партнерів дозволить забезпечити величезний обсяг інвестицій, необхідних для України в умовах війни та повоєнної відбудови, а іноземні держави-партнери матимуть змогу долучитися до отриманого Україною

під час війни важливого досвіду подолання її наслідків, відсічі агресії й, відповідно, взяти участь у реалізації важливих проєктів, щодо яких вони мають спільну з Україною заінтересованість (наприклад, спрямованих на зміцнення колективної безпеки в умовах зростаючих загроз від агресивних держав).

По-друге, важливе значення має інституційна форма партнерства, що передбачає створення партнерами спільного підприємства (участь у такому підприємстві), за допомогою органів якого відбуватиметься постійний контроль за внесенням інвестицій представниками партнерів в органах такого підприємства. Зазначене вельми актуальне з огляду на вище згадану проблему корупції та зловживань у процесі інвестування й отримання донорської допомоги в Україні й, відповідно, загрозу нецільового використання коштів партнерів внесених за договірним партнерством, де, у тому числі, і коштів донорів (така можливість передбачена Законом про ППП [20]).

Економіко-правовий механізм ППП, попри понад 15-річну тривалість правового регулювання на рівні закону<sup>1</sup>, не досить широко використовується на практиці (за винятком концесійних проєктів) з огляду на низку причин, одна з яких – відсутність у ньому положень про інституційну форму партнерств. Можливість же участі на боці державного партнера не лише Української держави в особі уповноважених органів та органів місцевого самоврядування, а й інших, дружніх щодо України, держав цим та новим законами не передбачена. Йдеться про міжнародне партнерство для реалізації інвестиційно-інноваційних проєктів міжнародного значення, оскільки в сучасному світі чимало проблем (економічних, національної та регіональної безпеки, включно з кібербезпекою) має транснаціональний характер. Про це, зокрема, свідчить і агресія російської держави проти України та погрози російських політиків щодо застосування ядерної зброї. З огляду на ці обставини після початку повномасштабної війни проти України з боку її російського сусіда значна частина країн світу прийняла нові стратегії національної безпеки, в яких наголошується на важливості використання в цій справі партнерських відносин як за участі національних суб'єктів, так і дружніх держав [27; 28; 29; 30].

Необхідність міжнародного інвестиційного партнерства для України викликана потребами часу й наявними обставинами: захист країни від агресора, численні руйнування, необхідність підтримання життєдіяльності країни, включно з її критичною інфраструктурою, що страждає від постійних ворожих нападів, відновлення зруйнованого – все це потребує колосальних коштів [31], яких критично бракує. Донорська допомога дружніх держав, якій Україна щиро вдячна, не безмежна. Відтак необхідно знаходити власні джерела та використовувати зарубіжний досвід, у тому числі подібне до європейського інституційне публічно-приватне партнерство за участі кількох дружніх держав та бізнесу, використання якого в справі зміцнення національної безпеки та повоєнної відбудови є вкрай

<sup>1</sup> Перший Закон, що регулював відносини державно-приватного партнерства було прийнято ще в 2010 р. [26].

важливим. Йдеться не лише про Регламент 2021/2085 від 19.11.2021, а й про зміни до нього у зв'язку з прийняттям Акту про мікросхеми [31], причини прийняття якого полягають у необхідності забезпечення незалежності ЄС і Європи в цілому від виробництва мікросхем в Азії з проблемами безпеки її країн з огляду на зростаючі воєнні загрози.

Переваги такого партнерства незаперечні, оскільки воно забезпечує:

– можливість акумулювання великих ресурсів (кількох держав та бізнесу) у справі реалізації виключно важливих інвестиційно-інноваційних проєктів міжнародного значення;

– застосування інституційної форми партнерства, що опосередковується через спільне підприємство за участі партнерів, дозволяючи використати можливості корпоративних відносин, а саме: забезпечити управління партнерством та контроль використання інвестицій за допомогою системи органів СП, сформованих із представників публічних і приватних партнерів, а також міжнародних експертів; зменшити загрозу корупційних зловживань шляхом відкритості інформації про перебіг інвестування та, відповідно, вкладення коштів партнерів у проєкти ППП;

– вирішення проблем транснаціонального значення в сфері оборони, цифровізації (кібербезпеки, зокрема), охорони здоров'я, захисту та відновлення об'єктів критичної інфраструктури тощо.

Разом із тим використанню потенціалу такого партнерства не сприяє чинне нормативно-правове забезпечення, оскільки Закон України «Про публічно-приватне партнерство» [20], як і його попередник – Закон «Про державно-приватне партнерство» [26] не передбачає інституційної форми ППП та можливості участі на боці публічних партнерів не лише України та її органів місцевого самоврядування, а й інших, дружніх щодо України, держав, які мають заінтересованість у реалізації спільних інвестиційно-інноваційних проєктів і бажають надати допомогу Україні в формі інвестування, а не обтяжливої для них безкоштовної допомоги, цільове використання якої вони нерідко не спроможні навіть контролювати на додаток до загрози корупційних та інших зловживань.

Набутий Україною колосальний досвід щодо застосування новітніх технологій у військовій техніці, відновлення поранених, щодо засобів і методів відновлення критичної інфраструктури після ворожих атак, забезпечення населення всім необхідним у критичних умовах війни, у справі кібербезпеки та використання цифрових технологій на фронті та в тилу [32; 33; 34; 35] є корисним у справі колективної безпеки дружніх для України держав, що може їх спонукати до встановлення подібного до вже традиційного в ЄС інституційного публічно-приватного партнерства за умови відповідного корегування українського законодавства, зокрема Закону «Про публічно-приватне партнерство».

Запровадження в Україні партнерства на зразок закріпленого в Регламенті (ЄС) 2021/694 і встановлення договірних відносин із дружніми державами як потенційними партнерами, дасть змогу вирішити низку важливих для нашої країни проблем, у тому числі:

– залучити в Україну значно більші за обсягом інвестиції, ніж за партнерства, передбаченого чинним Законом України про ППП, та за інших (у тому числі вищезазначених) форм/моделей інвестування;

– забезпечити ефективність управління інвестиціями в проекти ППП та контролю за їх реалізацією шляхом використання потенціалу корпоративних відносин;

– сприяти адаптації українського законодавства до права ЄС;

– зменшити корупційні й інвестиційні ризики у відносинах ППП, завдяки використанню потенціалу корпоративних відносин між партнерами з відповідним створенням постійно діючих органів управління та контролю за перебігом інвестування в межах партнерства. Це сприятиме його ефективності й авторитету України як правової держави, що забезпечує врахування інтересів інвесторів-партнерів, наділяючи їх відповідним обсягом прав щодо вкладених інвестицій протягом усього циклу інвестування;

– забезпечити баланс інтересів: дружніх держав-партнерів – щодо отримання статусу інвестора за надану Україні підтримку, можливість долучення до багато досвіду України, отриманого під час війни та об'єднання зусиль для вирішення спільних проблем, включно з колективною безпекою (всіх її складових); українського суспільства – у значних міжнародних інвестиціях, необхідних в умовах війни та повоєнної відбудови; приватного бізнесу – щодо надання сприяння з боку України за участь у такому партнерстві. У підсумку це забезпечить реалізацію інвестиційних проектів міжнародного значення в посиленні національної безпеки країн-партнерів, що відповідає конституційним засадам кожної з них як одного з основних завдань сучасних держав в умовах посилення загроз суспільному благополуччю.

Пошук дієвих засобів забезпечення національної безпеки та повоєнної відбудови країни – ключові завдання Української держави в справі гарантування конституційних засад як суверенної, незалежної, демократичної, соціальної та правової держави, що дбає про дотримання прав і свобод людини та гідних умов її життя [36, преамбула, ст. 1], а залучення до цього дружніх держав на засадах інвестування – сприятиме взаємовигідному співробітництву з членами міжнародного співтовариства [36, ст. 18]. Укладена ж минулого року Угода між Урядом України та Урядом Сполучених Штатів Америки про створення Американсько-українського інвестиційного фонду відбудови у формі обмеженого партнерства [37] свідчить не лише про актуальність партнерства для України та його адаптування до стандартів ЄС, а й про необхідність закріплення цього поняття в ЦК України [4] з відповідним визначенням його змісту, а також форм і видів.

## ВИСНОВКИ

Ризик – невід'ємний елемент суспільного й приватного життя. Проте правила їх розподілу, що закріплені в праві, є недостатньо досконалими в умовах зростаючих загроз суспільному благополуччю, від якого залежить і благо приватних осіб. Розпочата російською державою повномасштабна війна проти нашої країни,

її наслідки, зокрема масштабні руйнування, колосальні втрати (територій, людського потенціалу через загибель і виїзд у більш безпечні країни значної частини громадян), – усе це актуалізувало необхідність перегляду підходів до мінімізації ризиків. Тотальна цифровізація попри незаперечні переваги – забезпечення зв'язку, модернізація озброєння, дистанційне спілкування, вирішення надскладних проблем за допомогою штучного інтелекту тощо – створює й додаткові ризики. Зменшення таких ризиків пов'язане з урахуванням рівня їх небезпеки. Одним із кроків у цьому напрямі стало прийняття в ЄС Регламенту 2024/1689, спрямованого на зменшення небезпеки від використання такого важливого надбання цифровізації, як штучний інтелект, особливо з неприйнятним та високим ступенями ризику. Україна, обравши європейський вектор розвитку, має вдосконалювати національне законодавство не лише через інтеграцію положень європейських документів, а й урахувати українську специфіку.

Наявна потреба в колосальних ресурсах, від отримання яких залежить доля України та її громадян, може бути вирішена через залучення інвестицій. Альтернативою донорській допомозі дружніх держав, яка для них стає обтяжливою через відсутність компенсації, за винятком суто моральної, може стати спільне (за участі України, дружніх держав та приватного бізнесу) інвестування з використанням механізму інституційного публічно-приватного партнерства, подібного до передбаченого Регламентом ЄС 2021/2085. Це дасть змогу не лише забезпечити надходження необхідних для України коштів, а й зменшити корупційні й інвестиційні ризики завдяки перевагам корпоративних відносин через створене партнерами для цієї мети спільне підприємство і, відповідно, можливості постійного контролю за процесами внесення інвестицій та реалізації проєктів такого партнерства. Такий підхід потребує розробки й обговорення законопроекту, подібного до Регламенту ЄС, щоб уникнути проблеми, подібної з публічно-приватним партнерством (оновлений у минулому році закон про партнерство мало чим нагадує його європейський варіант через відсутність інституційної форми публічно-приватного партнерства, яка зменшує ризики при інвестуванні в проєкти ППП) та забезпечити можливість участі в ролі публічних партнерів кількох дружніх держав нарівні з Україною.

Відтак проблема правового забезпечення мінімізації ризиків залишається не лише актуальною, а її вирішення конче необхідним для виживання України в умовах війни, подолання її наслідків і повоєнного відновлення. Це особливо яскраво проявляється у відносинах партнерського інвестування та використання надбань новітніх технологій, зокрема штучного інтелекту, що зумовлює потребу врахування європейського досвіду при внесенні відповідних змін до чинної або розробки нової редакції Закону України про публічно-приватне партнерство, який значною мірою має бути подібним до Регламенту 2024/1689, а також удосконалення механізмів розподілу ризиків у Цивільному кодексі України, враховуючи, що вони (ризики) притаманні не лише відносинам цифровізації.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Цопа В. Ідентифікація і класифікація ризиків. URL: <https://qualityexpert.com.ua/articles/657215-identyfikatsiya-i-klasifikatsiya-ryzykiv> (дата звернення: 10.12.2025).
- [2] Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15> (дата звернення: 25.09.2025).
- [3] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV. URL: <https://zakon.rada.gov.ua/laws/show/1618-15#Text>
- [4] Цивільний кодекс України. Науково-практичний коментар (стаття 842). URL: [https://protocol.ua/ua/tsivilniy\\_kodeks\\_ukraini\\_stattya\\_842/](https://protocol.ua/ua/tsivilniy_kodeks_ukraini_stattya_842/) (дата звернення: 30.11.2025).
- [5] Корупція в енергетиці під час війни: викрито організовану групу (ФОТО+СХЕМА). Національне антикорупційне бюро України. URL: <https://nabu.gov.ua/news/koruptsiia-v-energetytsi-pid-chas-viiny-vykryto-organizovanu-grupu/> (дата звернення: 30.12.2025).
- [6] Більшість українців вважають, що з початку повномасштабного вторгнення рівень корупції зріс – КМІС. *Forbes Ukraine*. URL: <https://forbes.ua/news/bilshist-ukraintsv-vvazhayut-shcho-z-pochatku-povnomasshtabnogo-vtorgnennya-riven-koruptsii-zris-orituvannya-kmis-03102025-33099> (дата звернення: 30.12.2025).
- [7] Герасименко П. Корупція під час війни. *Організація українських націоналістів*. URL: <https://ukrnationalism.com/publications/5750-koruptsiia-pid-chas-viiny.html> (дата звернення: 30.12.2025).
- [8] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (дата звернення: 12.11.2025).
- [9] Великанова М. М. Ризики в цивільному праві : монографія. Київ : Алерта, 2019. 378 с.
- [10] Андреева О. В. Ризик у договірних зобов'язаннях : дис. ... канд. юрид. наук : 12.00.03. Київ, 2015. 193 с. URL: [https://scc.knu.ua/upload/iblock/e8d/dis\\_%D0%90%D0%BD%D0%B4%D1%80%D0%B5%D1%94%D0%B2%D0%B0%D0%9E.%D0%92..pdf](https://scc.knu.ua/upload/iblock/e8d/dis_%D0%90%D0%BD%D0%B4%D1%80%D0%B5%D1%94%D0%B2%D0%B0%D0%9E.%D0%92..pdf).
- [11] Іванов А. М., Іванюк А. О., Шимбарьов В. О. Сутність та правова природа ризику в договорах підряду. *Юридичний науковий електронний журнал*. 2021. № 11. С. 170–172. URL: <https://doi.org/10.32782/2524-0374/2021-11/40>.
- [12] Дубицька Н. Т. Ризик та відповідальність у приватному праві. *Часопис Київського університету права*. 2021. № 2. С. 197–201. URL: <https://doi.org/10.36695/2219-5521.2.2021.39>.
- [13] Скриньковський Р., Тиркало Ю. Підприємницькі ризики: сутність, види, методи оцінки та шляхи їх зниження. *Trajectoriâ Nauki = Path of Science*. 2021. Vol. 7, no. 12. P. 2015–2023. URL: <https://doi.org/10.22178/pos.77-11>.
- [14] Великанова М. М. Штучний інтелект: правові проблеми та ризики. *Вісник Національної академії правових наук України*. 2020. № 4. С. 185–198. URL: [https://doi.org/10.37635/jnalsu.27\(4\).2020.185-198](https://doi.org/10.37635/jnalsu.27(4).2020.185-198).
- [15] Вінник О. Відносини щодо сучасних технологій, ризиків при їх використанні та стратегічного партнерства в ракурсі вдосконалення правового регулювання відповідно до євроінтеграційного курсу України. *Адаптація законодавства України до положень права Європейського Союзу* : зб. матер. Всеукр. наук.-практ. конф. (м. Київ, 10 жовтня 2025 р.). Одеса : Юридика, 2025. С. 42–46.
- [16] Вчені прогнозують, що людство втратить контроль над штучним інтелектом вже у 2026 році. URL: <https://noworries.news/vcheni-prognozuyut-shho-lyudstvo-vtratyt-kontrol-nad-shtuchnym-intelektom-vzhe-u-2026-roczii/> (дата звернення: 15.10.2025).

- [17] Семенюта І. Лабораторія цифрової безпеки представила план дій щодо впровадження Акту про ШІ в Україні. URL: <https://ms.detector.media/withoutsection/post/38746/2025-12-17-laboratoriya-tsyfrovoi-bezpeky-predstavyla-plan-diy-shchodovprovdzhennya-aktu-pro-shi-v-ukraini/> (дата звернення: 17.12.2025).
- [18] Рекомендації з відповідальної розробки систем із використанням технологій штучного інтелекту. URL: <https://storage.thedigital.gov.ua/files/8/e8/da2197e1f813b2c5d29294e1ba580e8b.pdf> (дата звернення: 01.01.2026).
- [19] Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe. URL: <https://eur-lex.europa.eu/legal-content/EN/TX/T/?uri=CELEX%3A02021R2085-20230921> (дата звернення: 01.11.2025).
- [20] Про публічно-приватне партнерство : Закон України від 19.06.2025 №4510–20. URL: <https://zakon.rada.gov.ua/laws/show/4510-20> (дата звернення: 01.11.2025).
- [21] Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року : Розпорядження Кабінету Міністрів України від 31.12.2024 № 1351-р. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-p> (дата звернення: 14.02.2025).
- [22] Безпечний ШІ для мільйонів українців: Україна підписала Рамкову конвенцію про штучний інтелект та права людини. URL: <https://www.kmu.gov.ua/news/bezpechnyi-shi-dlia-milioniv-ukraintsiv-ukraina-pidpysala-ramkovu-konventsiiu-pro-shtuchnyi-intelekt-ta-prava-liudyny> (дата звернення: 08.09.2025).
- [23] Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Липень 2024. 30 с. URL: <https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf> (дата звернення: 08.09.2025).
- [24] Забоклицький І. І. Акт про штучний інтелект (Artificial Intelligence Act, AI Act) як основа правового регулювання штучного інтелекту в ЄС: огляд основних положень. *Аналітично-порівняльне правознавство*. 2025. Т. 3. С. 282–286. URL: <https://doi.org/10.24144/2788-6018.2025.03.3.44>.
- [25] Концепція оновлення Цивільного кодексу України. Київ : Видавничий дім «Ар-Тек», 2020. 128 с.
- [26] Про державно-приватне партнерство : Закон України від 01.07.2010 №2404-VI. URL: <https://zakon.rada.gov.ua/laws/show/2404-17> (дата звернення: 26.09.2025).
- [27] National Security Strategy. October 2022. URL: <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf> (дата звернення: 23.09.2024).
- [28] National Security Strategy of Japan. December 2022. URL: <https://www.cas.go.jp/jp/siryou/22121banzenhoshou/nss-e.pdf> (дата звернення: 23.09.2024).
- [29] National Cyber Strategy 2022. URL: <https://www.gov.uk/government/publications/national-cyber-strategy-2022> (дата звернення: 23.09.2024).
- [30] Security Strategy of the Czech Republic 2023. URL: [https://mzv.gov.cz/file/5119429/MZV\\_BS\\_A4\\_brochure\\_WEB\\_ENG.pdf](https://mzv.gov.cz/file/5119429/MZV_BS_A4_brochure_WEB_ENG.pdf) (дата звернення: 23.09.2024).
- [31] European Chips Act. URL: <https://digital-strategy.ec.europa.eu/en/policies/european-chips-act> (дата звернення: 22.06.2024).
- [32] ЗСУ щомісяця виявляють тисячі цілей за допомогою штучного інтелекту – Міноборони. URL: <https://flot2017.com/zsu-shchomisiatsia-vyavliaiut-tysiachi-tsilej-zadomohoiu-shtuchnoho-intelektu-minoborony/> (дата звернення: 23.09.2024).
- [33] Країни НАТО дослухаються до досвіду наших бойових медиків і тому оновлюють свої стандарти – Тетяна Остащенко. URL : <https://armyinform.com.ua/2023/08/02/krayiny-nato-dosluyayutsya-do-dosvidu-nashyh-bojovyh-medykiv-i-tomu-onovlyuyut>

svoiy-standarty-tetyana-ostashhenko/ (дата звернення: 05.01.2026).

- [34] Як війна в Україні стала «лабораторією» для інновацій і випробувань західної зброї. *Голос Америки*. URL: <https://www.holosameryky.com/a/ukrainia-zakhidna-zbroia-vyprobuvannia/6919181.html> (дата звернення: 24.09.2024).
- [35] Наше завдання в технологічній війні – постійно генерувати інновації, – Михайло Федоров. URL: <https://www.kmu.gov.ua/news/nashe-zavdannia-v-tekhnohichnii-viini-postiino-heneruvaty-innovatsii-mykhailo-fedorov> (дата звернення: 24.09.2024).
- [36] Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://constitution.in.ua/> (дата звернення: 03.01.2026).
- [37] Угода між Урядом України та Урядом Сполучених Штатів Америки про створення Американсько-Українського інвестиційного фонду відбудови. URL: [https://zakon.rada.gov.ua/laws/show/840\\_001-25#Text](https://zakon.rada.gov.ua/laws/show/840_001-25#Text) (дата звернення: 05.01.2026).

## REFERENCES

- [1] Tsopa, V. (2023). *Identification and classification of risks*. Quality Expert. Retrieved from <https://qualityexpert.com.ua/articles/657215-identyfikatsiya-i-klassyfikatsiya-ryzykiv>
- [2] Civil Code of Ukraine: Law of Ukraine. (2003, January). Retrieved from <https://zakon.rada.gov.ua/laws/show/435-15>
- [3] Civil Procedure Code of Ukraine: Law of Ukraine. (2004, March). Retrieved from <https://zakon.rada.gov.ua/laws/show/1618-15#Text>
- [4] Scientific and Practical Commentary to the Civil Code of Ukraine (Article 842). Protocol. Retrieved from [https://protocol.ua/ua/tsivilniy\\_kodeks\\_ukraini\\_stattya\\_842/](https://protocol.ua/ua/tsivilniy_kodeks_ukraini_stattya_842/)
- [5] National Anti-Corruption Bureau of Ukraine. (2025). *Corruption in the energy sector during the war: Organized group exposed*. Retrieved from <https://nabu.gov.ua/news/koruptciia-v-energetytsi-pid-chas-viyiny-vykryto-organizovanu-grupu/>
- [6] Forbes Ukraine. (2025). *Most Ukrainians believe corruption has increased since the start of the full-scale invasion – KIIS*. Retrieved from <https://forbes.ua/news/bilshist-ukraintsiv-vvazhayut-shcho-z-pochatku-povnomasshtabnogo-vtorgnennya-riven-koruptsii-zrisopituvannya-kmis-03102025-33099>
- [7] Herasymenko, P. (2025). *Corruption during the war*. Organization of Ukrainian Nationalists. Retrieved from <https://ukrnationalism.com/publications/5750-koruptsiia-pid-chas-viiny.html>
- [8] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
- [9] Velykanova, M. M. (2019). *Risks in Civil Law*: Monograph. Alerta.
- [10] Andreyeva, O. V. (2015). *Risk in contractual obligations* (Candidate dissertation). Retrieved from [https://scc.knu.ua/upload/iblock/e8d/dis\\_%D0%90%D0%BD%D0%B4%D1%80%D0%B5%D1%94%D0%B2%D0%B0%D0%9E.%D0%92..pdf](https://scc.knu.ua/upload/iblock/e8d/dis_%D0%90%D0%BD%D0%B4%D1%80%D0%B5%D1%94%D0%B2%D0%B0%D0%9E.%D0%92..pdf)
- [11] Ivanov, A. M., Ivanyuk, A. O., & Shymbaryov, V. O. (2021). Essence and legal nature of risk in construction contracts. *Juridical Scientific Electronic Journal*, (11), 170–172. Retrieved from <https://doi.org/10.32782/2524-0374/2021-11/40>
- [12] Dubytska, N. T. (2021). Risk and liability in private law. *Kyiv University of Law Journal*, (2), 197–201. Retrieved from <https://doi.org/10.36695/2219-5521.2.2021.39>
- [13] Skrynkovskyy, R., & Tyrkalo, Y. (2021). Entrepreneurial risks: Essence, types, assessment

- methods and ways to reduce them. *Traektoriâ Nauki = Path of Science*, 7(12), 2015–2023. Retrieved from <https://doi.org/10.22178/pos.77-11>
- [14] Velykanova, M. M. (2020). Artificial intelligence: Legal problems and risks. *Journal of the National Academy of Legal Sciences of Ukraine*, (4), 185–198. Retrieved from [https://doi.org/10.37635/jnalsu.27\(4\).2020.185-198](https://doi.org/10.37635/jnalsu.27(4).2020.185-198)
- [15] Vinnyk, O. (2025). Relations regarding modern technologies, risks in their use and strategic partnership in the perspective of improving legal regulation in accordance with the European integration course of Ukraine. In *Adaptation of Ukrainian legislation to the provisions of European Union law* (pp. 42–46). Yurydyka.
- [16] Noworries News. (2025). *Scientists predict that humanity will lose control over artificial intelligence as early as 2026*. Retrieved from <https://noworries.news/vcheni-prognozuuyut-shho-lyudstvo-vtratyt-kontrol-nad-shtuchnym-intelektom-vzhe-u-2026-roczii/>
- [17] Semenyuta, I. (2025). *Digital Security Lab presented an action plan for the implementation of the AI Act in Ukraine*. Detector Media. Retrieved from <https://ms.detector.media/withoutsection/post/38746/2025-12-17-laboratoriya-tsyfrovoi-bezpeky-predstavyla-plan-diy-shchodo-vprovadzhenya-aktu-pro-shi-v-ukraini/>
- [18] Ministry of Digital Transformation of Ukraine. (2026). *Recommendations for the responsible development of systems using artificial intelligence technologies*. <https://storage.thedigital.gov.ua/files/8/e8/da2197e1f813b2c5d29294e1ba580e8b.pdf>
- [19] Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02021R2085-20230921>
- [20] On Public-Private Partnership: Law of Ukraine. (2025, June). Retrieved from <https://zakon.rada.gov.ua/laws/show/4510-20>
- [21] On approval of the Strategy for digital development of innovative activity of Ukraine for the period until 2030: Order Cabinet of Ministers of Ukraine (2024, December, No. 1351-r). Retrieved from <https://zakon.rada.gov.ua/laws/show/1351-2024-p>
- [22] Government Portal. (2025). *Safe AI for millions of Ukrainians: Ukraine signed the Framework Convention on Artificial Intelligence and Human Rights*. Retrieved from <https://www.kmu.gov.ua/news/bezpechnyi-shi-dlia-milioniv-ukraintiv-ukraina-pidpysalaramkovu-konventsiiu-pro-shtuchnyi-intelekt-ta-prava-liudyny>
- [23] Ministry of Digital Transformation of Ukraine. (2024). *White Paper on AI Regulation in Ukraine*. Retrieved from <https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf>
- [24] Zabokrytsky, I. I. (2025). Artificial Intelligence Act (AI Act) as the basis for legal regulation of artificial intelligence in the EU: Overview of the main provisions. *Analytical and Comparative Jurisprudence*, (3), 282–286. Retrieved from <https://doi.org/10.24144/2788-6018.2025.03.3.44>
- [25] *The Concept of updating the Civil Code of Ukraine*. (2020). ArtEk.
- [26] On State-Private Partnership: Law of Ukraine. (2010, July). Retrieved from <https://zakon.rada.gov.ua/laws/show/2404-17>
- [27] The White House. (2022). *National Security Strategy*. Retrieved from <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>
- [28] Government of Japan. (2022). *National Security Strategy of Japan*. Retrieved from <https://www.cas.go.jp/jp/siryu/221216anzenhoshou/nss-e.pdf>
- [29] Government of the United Kingdom. (2022). *National Cyber Strategy 2022*. Retrieved

- from <https://www.gov.uk/government/publications/national-cyber-strategy-2022>
- [30] Ministry of Foreign Affairs of the Czech Republic. (2023). *Security Strategy of the Czech Republic 2023*. Retrieved from [https://mzv.gov.cz/file/5119429/MZV\\_BS\\_A4\\_brochure\\_WEB\\_ENG.pdf](https://mzv.gov.cz/file/5119429/MZV_BS_A4_brochure_WEB_ENG.pdf)
- [31] European Commission. (2024). *European Chips Act*. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/european-chips-act>
- [32] Ministry of Defence of Ukraine. (2024). *AFU identify thousands of targets every month with the help of artificial intelligence*. Retrieved from <https://flot2017.com/zsu-shchomisiatsia-vyiavliaiut-tysiachi-tsilej-za-dopomohoiu-shtuchnoho-intelektu-minoborony/>
- [33] Ostashchenko, T. (2023, August 2). *NATO countries listen to the experience of our combat medics and therefore update their standards*. ArmyInform. Retrieved from <https://armyinform.com.ua/2023/08/02/krayiny-nato-dosluhayutsya-do-dosvidu-nashyh-bojovyh-medykiv-i-tomu-onovlyuyut-svoyi-standarty-tetyana-ostashhenko/>
- [34] Voice of America. (2024). *How the war in Ukraine became a «laboratory» for innovation and testing of Western weapons*. Retrieved from <https://www.holosameryky.com/a/ukraina-zakhidna-zbroia-vyprobuvannia/6919181.html>
- [35] Fedorov, M. (2024). *Our task in the technological war is to constantly generate innovations*. Government Portal. Retrieved from <https://www.kmu.gov.ua/news/nashe-zavdannia-v-tekhnologichnii-viini-postiino-heneruvaty-innovatsii-mykhailo-fedorov>
- [36] Constitution of Ukraine: Law of Ukraine. (1996, June). Retrieved from <https://constitution.in.ua/>
- [37] Agreement between the Government of Ukraine and the Government of the United States of America on the establishment of the American-Ukrainian Investment Fund for Reconstruction (2024). Retrieved from [https://zakon.rada.gov.ua/laws/show/840\\_001-25#Text](https://zakon.rada.gov.ua/laws/show/840_001-25#Text)

### **Оксана Мар'янівна Вінник**

Доктор юридичних наук, професор

Член-кореспондент НАПрН України

Національна академія правових наук України

61024, вул. Григорія Сковороди, 70, Харків, Україна

Головний науковий співробітник відділу приватноправових досліджень

Інститут правотворчості та науково-правових експертиз

Національної академії наук України

01024, вул. Пилипа Орлика, 3, Київ, Україна

*email: vinnoks@gmail.com*

### **Oksana M. Vinnyk**

Doctor of Law, Professor

Corresponding Member of the NALS of Ukraine

National Academy of Legal Sciences of Ukraine  
61024, 70 Hryhoriia Skovorody Str., Kharkiv, Ukraine

Chief researcher of the Department of Private Law Research  
Institute of Lawmaking and Scientific and Legal Expertise  
National Academy of Sciences of Ukraine  
01024, 3 Pylyp Orlyk Str., Kyiv, Ukraine  
*email: vinnoks@gmail.com*

**Марина Миколаївна Великанова**

Доктор юридичних наук, професор  
Завідувач відділу приватноправових досліджень  
Інститут правотворчості та науково-правових експертиз  
Національної академії наук України  
01024, вул. Пилипа Орлика, 3, Київ, Україна,

Професор кафедри цивільного права  
Київського національного університету імені Тараса Шевченка  
01601, вул. Володимирська, 64/13, Київ, Україна  
*email: velikanova2008@gmail.com*

**Maryna M. Velykanova**

Doctor of Law, Professor  
Head of the Department of Private Law Research  
Institute of Lawmaking and Scientific and Legal Expertise  
National Academy of Sciences of Ukraine  
01024, 3 Pylyp Orlyk Str., Kyiv, Ukraine

Professor of the Department of of Civil Law  
Taras Shevchenko National University of Kyiv  
01601, 64/13 Volodymyrska Str., Kyiv, Ukraine  
*email: velikanova2008@gmail.com*

**Рекомендоване цитування:** Вінник О. М., Великанова М. М. Ризики цифровізації та партнерства: правовий аспект. *Вісник Національної академії правових наук України*. 2026. Т. 33. № 1. С. 220–238. <https://doi.org/10.31359/10.31359/1993-0909-2026-33-1-220>

**Suggested Citation:** Vinnyk, O. M. & Velykanova, M. M. (2026). Risks of digitalization and partnership: legal aspects. *Journal of the National Academy of Legal Sciences of Ukraine*, 33 (1), 220–238. <https://doi.org/10.31359/1993-0909-2026-33-1-220>

Дата першого надходження статті до видання: 16.01.2026

Дата прийняття статті до друку після рецензування: 16.02.2026

Дата публікації (оприлюднення): 31.03.2026