

УДК 346.1

DOI <https://doi.org/10.32849/2663-5313/2020.3.10>**Оксана Вінник,***докт. юрид. наук, професор,**член-кореспондент Національної академії правових наук України,**головний науковий співробітник відділу правового забезпечення ринкової економіки**Науково-дослідного інституту приватного права і підприємництва**імені академіка Ф. Г. Бурчака Національної академії правових наук України*

ПЕРЕВАГИ ТА РИЗИКИ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ: ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

Стаття присвячена правовим проблемам забезпечення соціального спрямування цифровізації з метою мінімізації пов'язаних із цим ризиків та стимулювання переваг цифрових технологій.

Аналізуються властивості цифровізованих явищ (зокрема, штучного інтелекту, віртуальних підприємств, бізнес-сайтів тощо) з точки зору переваг, що вони надають, та ризиків, які виникають у процесі їх недобросовісного чи неконтрольованого їх використання. Серед переваг – швидкість (обміну інформацією, пошуку необхідних рішень, оцінки ситуації, оплати тощо), зручність (без обов'язкових за традиційних зв'язків присутності заінтересованих осіб в певному місці, в певний час), висока ефективність (наукових та маркетингових досліджень, бізнес-операцій), доступність (можливість використання незалежно від місця перебування замовника/покупця та виконавця/продавця, надавача послуг), економічність (зменшення витрат), транснаціональність (широкі можливості замовлення товарів / пошуку контрагентів за кордоном), необмеженість в часі (без перерв, режиму роботи і вихідних) тощо. Проте, крім згаданих переваг, цифровізованим явищам (штучному інтелекту, віртуальним підприємствам, бізнес-сайтам тощо) притаманні значні ризики, пов'язані з недобросовісним та/або неконтрольованим їх використанням. Внаслідок цього можуть виникнути значні матеріальні втрати, загроза безпеці людей, а в найгіршому випадку – диктат з боку осіб, що контролюють штучний інтелект, або вибуття останнього з-під контролю людей. За цих умов зростає необхідність правового забезпечення цивілізованого (з урахуванням загальносуспільних інтересів) спрямування цифровізації та використання цифровізованих явищ. Таку роль має забезпечувати держава з огляду на наявність у неї відповідних засобів та заінтересованості. Насамперед ідеться про нормативно-правове регулювання, вдосконалення якого має включати правові механізми контролю за використанням електронних ресурсів, в тому числі запровадження державної реєстрації відповідальних за їх використання в публічних сферах осіб, основних засад відповідальності таких осіб за недобросовісне та/або неконтрольоване використання електронних ресурсів у публічних сферах, включаючи бізнес. Закріпити такі механізми пропонується в кодифікованому акті, яким може бути чинний Господарський кодекс України чи новий – Кодекс цифрової економіки чи Цифровий кодекс.

Ключові слова: цифровізація, цифрова економіка, штучний інтелект, віртуальне підприємство, бізнес-сайт, відповідальність.

Постановка проблеми. Про специфіку сучасного суспільного (включно з економічним) життя свідчить хоча б той факт, що словом 2019 року, за версією словника сучасної української мови (UA.NEWS), визнано слово «діджиталізація», яке є спрощеною формою вітчизняного терміна «цифрова трансформація» [1] і означає насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично створює кіберфізичний простір, уможливаючи інтегральну взаємодію віртуального та фізичного [2]. У результаті цифровізації економічної сфери

формується цифрова економіка (далі – ЦЕ), яка базується на інформаційно-комунікаційних, і насамперед цифрових, технологіях, стрімкий розвиток та поширення яких вже сьогодні впливають на традиційну (фізично-аналогову) економіку, трансформуючи її з такої, що споживає ресурси, в економіку, що створює ресурси [2]. Ключовим ресурсом ЦЕ є дані, що, завдяки функціонуванню електронно-цифрових пристроїв, засобів та систем, генеруються та забезпечують електронно-комунікаційну взаємодію складників такої економіки. Разом із тим рівень цифрової грамотності в Україні, за оцінками Міністерства цифрової трансформації України

(далі – Мінцифри), нижче від середнього [3], що свідчить не лише про цифрову нерівність (поділ суспільства на багатих і бідних за критерієм наявності у них цифрових ресурсів, знань та навичок), а й про відсутність реальних цифрових можливостей у більшості споживачів, які і без того є слабкішими учасниками відносин у сфері господарювання, проте забезпечують прибутковість бізнесу як основну мету такої діяльності. Брак або навіть відсутність необхідних цифрових навичок у більшості громадян, а також відповідних пристроїв, можливості оплати послуг Інтернету тощо – один із тих бар'єрів, що необхідно подолати на шляху до цивілізованої цифровізації. Крім того, наявність істотних ризиків застосування цифрових технологій, відставання та вади державного (в тому числі нормативно-правового) регулювання зумовлюють актуальність цієї проблеми, що не знайшла ще комплексного висвітлення на теоретичному рівні, хоча чимало дослідників присвячують свої праці окремим аспектам цифровізації, зокрема: О. А. Беяневич – договірним відносинам з використанням електронних ресурсів, В. В. Кочин і К. Єфремова – складникам відносин ЦЕ, в тому числі віртуальним підприємствам, В. М. Гончаренко – саморегулюванню у сфері ЦЕ, Є. О. Харитонов, О. І. Харитонova – ролі IT-права в регулюванні суспільних відносин, Ю. І. Остапенко і С. Я. Сенюта – правовому забезпеченню телекомунікаційної галузі, Н. Б. Пацурія – електронним страховим послугам, О. В. Шаповалова – електронним публічним реєстрам, П. О. Бітюк – конкуренції в умовах ЦЕ та ін.

Метою статті є спроба висвітлення проблеми необхідності комплексного регулювання відносин цифровізації у сфері економіки для того, аби її незаперечні переваги не були спотворені зловживаннями, і, відповідно, ролі правового регулювання в забезпеченні соціального спрямування цифровізації.

Виклад основного матеріалу. Отже, цифровізовані явища (такі як смарт-контракти, зберігання інформації в «хмарі», електронні платежі, віртуальні підприємства, віртуальні офіси, електронні кабінети, бізнес-сайти, включно з Інтернет-магазинами та торговельними Інтернет-платформами, використання відповідного програмного забезпечення, що мінімізує ризики, в тому числі технологія блокчейну, боти, штучний інтелект, криптовалюти тощо) потребують відповідних знань та навичок, набути та підтримувати які непросто. А їх відсутність у цифрову епоху загрожує не лише ймовірністю матері-

альних втрат у відносинах зі спритними шахраями, які зазвичай краще знаються на можливостях цифрових технологій, ніж сумлінні громадяни, а й навіть фактичним безправ'ям, зумовленим відсутністю необхідних для цього можливостей (не говорячи про вади нормативного регулювання, в тому числі відсутність закріпленого на рівні закону поняття цифрових прав).

Цифрові технології, що забезпечують цифровізацію не лише економіки, а й інших сфер суспільного та приватного життя, зазвичай пропагуються як надзвичайно прогресивні, такі, що забезпечать прорив в усіх напрямках суспільного буття, зробивши його більш ефективним, приємним та легким, звільнивши людей від рутинних дій (зокрема, пошуку інформації про товари, роботу, навчання, потенційних контрагентів/партнерів тощо). Проте кожне суспільне явище має дві сторони: сприятливу (умовно позитивну) і ризикову (умовно негативну). Це справедливо й щодо цифрових технологій та згаданих цифровізованих явищ. Ситуація з поширенням коронавірусу та пов'язаним із цим шоком зумовили поширення використання цифрових технологій в усіх сферах життя, і бізнес не став винятком: для роботи в режим он-лайн переходять бізнесмени, їх працівники та клієнти/споживачі, інвестори [4].

Кожен із цифрових ресурсів (включаючи вищезгадані) має як сприятливі для цивілізованого суспільства риси, так і вельми проблематичні. Одна з головних рис згаданих технологій – можливість діяти в Інтернет-просторі анонімно, забезпечуючи максимальну не лише швидкість операцій, пов'язаних із поширенням/пошуком/використанням інформації, а й їх приватність, а отже, і залучення до відповідних процесів максимальної кількості заінтересованих осіб. З іншого боку, використання такої анонімно приватності недобросовісними особами суспільно небезпечно, оскільки ускладнює, а нерідко й унеможлиблює визначення відповідальної особи, що своїми недобросовісними діями у віртуальному просторі (зазвичай в мережі Інтернет та/або з використанням мобільних телефонів/смартфонів) завдає шкоди іншим особами, та притягнення її до відповідальності. Крім того, Інтернет-простір – транснаціональний, а отже, діяти в ньому можна незалежно від місця фактичного перебування, яке до того ж нерідко важко визначити, якщо заінтересована в цьому особа не називає себе або надає викривлену інформацію, бажаючи уникнути відповідальності за зловживання приватністю на шкоду іншим учасникам відносин. Виявлення таких осіб потребує участі компетентних органів різних

держав, що зумовлює необхідність і встановлення відповідних правил їх взаємодії на транснаціональному рівні.

Досить популярний нині і вельми перспективний штучний інтелект має значні переваги, серед яких – краді за людські можливості в різних сферах: бізнесу (заробляння великих грошей на біржі [5], швидкість отримання необхідних дозволів та реєстраційних процедур, включно зі сферою будівництва [6], науки (отримання результатів наукових досліджень, зокрема медичних, що в умовах стрімкого поширення в усьому світі коронавірусу надзвичайно важливо [7]), державної служби (відповідне скорочення кількості держслужбовців [8]), у побуті (шопінг [9], спілкування [10]) тощо.

Разом із тим подібні інновації широко використовуються недобросовісними учасниками суспільних відносин, включно з криміналом, який, за оцінкою скандально відомого підприємця Джона Макафи, історично завжди був першим у застосуванні новітніх технологій на тлі відставання влади щодо запобігання недобросовісному їх використанню [11]. Це стосується не лише вдосконалення вірусів, що вражають комп'ютери/смартфони і завдають їх власникам значної шкоди через витік конфіденційної інформації чи грошові втрати [12], а насамперед – *штучного інтелекту*, який Ілон Маск вважає чи не найбільшою загрозою людству, оскільки надмірний і неконтрольований з боку уряду розвиток цієї сфери може загрожувати людям безробіттям, нестабільністю в соціальній сфері або почати поширювати фейкову інформацію і маніпулювати нею, а найгірше – може стати безсмертним диктатором, «від якого ніхто не зможе втекти» [13; 14].

Широке використання криптовалют становить загрозу для сфери кредитування [15], а нещодавнє блокування відео про криптовалюту на YouTube, як зазначає технічний директор EOS-стартапа Block.one Ден Ларімер, свідчить про те, що могутні е-корпорації можуть запроваджувати тотальну цензуру [16]. Більш того, він пропонує повернутися до паперових носіїв інформації, оскільки електронні легко знищити; відповідно, треба усвідомити, що ми нічого не контролюємо «на своєму телефоні», більш того, «ми все більше на шляху до того, що програмне забезпечення буде лише за інклюзивним доступом» [16]. У зв'язку з цим пригадуються сумні картини кіберизованого суспільства, описані фантастами, які, як виявилось, мало в чому помиляються.

¹ Як це поширено в інтернет-оголошеннях про розпродаж товарів за привабливими цінами [25].

Негативні сторони використання штучного інтелекту та інших досягнень цифровізації вже давно даються взнаки, хоча повідомляється про це значно рідше, ніж про революційні їхні переваги. Напади на людей [17] (поки що поодинокі випадки на тлі незначного використання роботів можуть мати катастрофічні наслідки у разі масового їх застосування), заволодіння фінансовою інформацією громадян та комерційних структур з метою отримання доступу до їхніх грошових активів [18; 19], у тому числі криптовалютних [20], численні кібератаки на сайти державних установ, бізнес-організації тощо, що завдають значної шкоди, паралізуючи на певний час їхню діяльність, у зв'язку з чим низка країн вимагає поширення на них (кібератаки) спеціального режиму санкцій, передбачених за застосування хімічної зброї [21].

Хоча ризики тотальної автоматизації/цифровізації очевидні, проте в численних працях *акцентується* увага в основному на перевагах цифрових явищ, що змінюють світ [22; 23 та ін.]. На спалах б'ють лише окремі знавці цих технологій, і серед них – Ілон Маск, якого важко звинуватити в їх незнанні або фінансовій заінтересованості критики щодо браку адекватної реакції урядів провідних країн світу на цифрові ризики [13; 14], включаючи адекватне їм нормативно-правове регулювання.

Відсутність цивілізованого режиму таких електронних ресурсів, як сайти, в кращому разі може загрожувати непорозумінням або конфузом [24], в гіршому – завданням шкоди численним споживачам, що не можуть визначити особу інтернет-продавця, який їх ошукав завдяки недостовірній інформації (або її відсутності) про товари та про особу продавця¹, що мала б розкриватися відповідно до законодавства (зокрема, законів «Про електронну комерцію» [26] та «Про захист прав споживачів» [27]). Крім того, досить поширеним є використання таких сайтів групою осіб, яких нерідко іменують себе «віртуальним підприємством», використовуючи традиційні поняття – підприємство чи магазин. Тому більшість пересічних громадян-споживачів сприймають цифровізовані явища як реальні, що існують в аналоговій економіці. Серед них:

– віртуальне підприємство: сприймається багатьма як належним чином легалізоване підприємство зі статусом юридичної особи; натомість це група осіб (фізичних та/або юридичних), заінтересованих у використанні одного електронного (зазвичай Інтернет) ресурсу (бізнес-сайту, зокрема), проте без оформлення їх організаційної єдності як юридичної особи або партнерів на підставі угоди про спільну діяльність;

– Інтернет-магазин: нерідко сприймається як електронна версія звичайного магазину з його власником, хоча насправді це сайт, на якому його користувачі (а їх може бути кілька або навіть багато) розміщують інформацію про пропоновані до продажу товари; вітчизняне законодавство, ґрунтовним знанням якого можуть похвалитися навіть не всі професійні юристи, визначає **веб-сайт** як сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу [28];

– боти (англ. **bot**, від *robot* — «робот»): сприймається як реально існуючий суб'єкт (підприємець, організація чи її працівники), хоча є програмою, що забезпечує виконання автоматично та/або за заданим розкладом (алгоритмом) комплексу послідовних дій, і має в цьому якусь схожість із людиною [29; 30]; боти нерідко відносять до штучного інтелекту/ШІ (англ. *Artificial intelligence*, AI), що критикується прибічниками альтернативної точки зору (дискусію з цього приводу залишаємо знавцям цифрових технологій); система *штучного інтелекту* є однією з найперспективніших напрямів комп'ютерних наук, що вивчає методи розв'язання задач, для яких не існує способів вирішення, дозволяючи оперувати даними та самонавчатися; має необмежену сферу застосування (від створення роботів, які самостійно приймають рішення, до машин з автопілотом чи онлайн-перекладачів у реальному часі) [29; 30]. Проте постає проблема щодо етичності використання штучного інтелекту/ШІ та відповідності встановленим правилам, чим опікується ЄС, визначивши 7 принципів застосування ШІ: 1) він має заслуговувати на довіру, відповідати законам та правилам; 2) повинен контролюватися людиною, розроблятися з урахуванням інтересів суспільства та прав людини, не зменшувати та не обмежувати право людини на прийняття рішень; 3) надійність та безпека: системи ШІ мають бути досить стабільними на випадок помилок або дисфункції систем на весь період їхнього функціонування; 4) повага до приватних прав людини та до безпеки баз даних, коли такі дані не будуть використовуватися проти людини; 5) прозорість: людина має отримати можливість відстежувати результати діяльності штучного інтелекту або відповідних систем; 6) системи ШІ мають застосовуватися на

недискримінаційній основі: враховувати всі людські особливості, включаючи фізичну спроможність, навички та потреби, і бути доступними для всіх людей; 7) системи ШІ мають сприяти розвитку суспільства та вирішенню проблем охорони довкілля, що передбачає принцип відповідальності людини за використання систем штучного інтелекту та за результати такої діяльності [31].

Подібні до вищезгаданих правил можна поширити й на інші цифровізовані явища (з урахуванням їхніх особливостей), проте однією з основних проблем у застосуванні таких правил є їх нормативно-правове закріплення, що стосується і принципу визначення відповідальної за використання ШІ особи. Враховуючи, що використання ШІ, як і інших електронних ресурсів, може мати непередбачуваний ефект, в тому числі негативний, слід встановити на законодавчому рівні необхідність легалізації особи, яка його використовує у бізнес-діяльності та інших сферах суспільного життя, шляхом реєстрації у відповідному реєстрі. Для цього мають бути запроваджені електронні реєстри: а) власників та фактичних користувачів бізнес-сайтів (для здійснення бізнес-діяльності), в тому числі Інтернет-магазинів, торговельних Інтернет-платформ; у разі використання такого ресурсу учасниками віртуального підприємства – відповідальний за використання подібного сайту учасник віртуального підприємства; б) власників та осіб, що фактично використовують ШІ в бізнес-діяльності, в наданні відповідних електронних послуг (в тому числі адміністративних); в) головних учасників віртуальних підприємств, які використовують один електронний ресурс, а також власників та відповідальних користувачів бізнес-сайтів спільного (групою осіб) використання на підставі угоди про спільну діяльність (така угода, якщо її укласти в письмовій формі, включно з електронною її модифікацією, забезпечить можливість визначення особи, відповідальної за недобросовісне використання бізнес-сайту, в тому числі розміщення недостовірної, неправильної чи неповної інформації про пропоновані до продажу товари, про продавця тощо). Крім того, мають бути встановлені **основні засади відповідальності**, пов'язані з використанням ШІ та інших електронних ресурсів: а) за використання ШІ – за аналогією з відповідальністю за використання джерела підвищеної небезпеки, оскільки всі наслідки використання ШІ важко передбачити, як і забезпечення 100-відсоткового контролю над ним; б) за *недобросовісне* (з порушенням вимог законодавства, прав та законних інтересів користувачів/споживачів) використання

сайту для бізнес-діяльності відповідальність має покладатися: за загальним правилом – на власника або особу, що використовує сайт для бізнес-діяльності (якщо її можна визначити); у разі використання учасниками віртуального підприємства одного електронного ресурсу/сайту принцип відповідальності має визначитися в укладеній між ними угоді про спільну діяльність та, відповідно, про спільне використання сайту (відповідає фактичний користувач, визначений в угоді з власником сайту), а за відсутності такої угоди – відповідальність має покладатися на власника сайту або фактичного його користувача, зареєстрованого у відповідному реєстрі.

Зазначені правові механізми повинні закріплюватися на рівні акта, що має силу закону, зокрема Кодексу. Пропозиції щодо кодифікації відносин у сфері цифрової економіки різні (прийняття Кодексу цифрової економіки [32] чи Цифрового кодексу [33] або включення до чинного Господарського кодексу України відповідних ключових положень щодо цифровізованих явищ у сфері економіки із забезпеченням ґрунтового регулювання складних відносин на певних ринках, щодо певних ресурсів тощо в спеціальних законах [34]. Проте, який би шлях не було обрано, законодавець має врахувати необхідність забезпечення державою соціального спрямування такого регулювання (як і економіки в цілому, що передбачено ст. 13 Конституції України), в тому числі закріпити в такому акті механізми подолання цифрової нерівності шляхом покладення на відповідальний у сфері цифровізації орган своєчасного вжиття відповідних заходів (крім навчання вразливих верств населення цифровій грамотності, видання відповідних, своєчасно оновлюваних посібників та словників у паперовій і електронній формі, які б дозволили пересічним громадянам орієнтуватися в цифровому світі з його перевагами та загрозами, кількість та види яких постійно зростають; надання на безоплатній основі консультацій з питань цифровізації та цифровізованих явищ; просування платформи з розгляду в режимі он-лайн споживачьких спорів у сфері електронної комерції як альтернативи судовим процедурам, з використанням напрацьованого в ЄС щодо цього досвіду [35; 36]).

Висновки

Отже, цифровізація всіх сфер суспільного, в тому числі економічного, життя – ознака сьогодення. Проте аналіз практики використання цифровізованих явищ (штучного інтелекту, віртуальних підприємств, бізнес-сайтів тощо) свідчить про їх не-

однозначність: крім незаперечних переваг (швидкість відповідних процесів, зручність, доступність, економічність), їм притаманні і ризики, пов'язані з недобросовісним та/або неконтрольованим їх використанням, що може спричинити матеріальні втрати та/або загрозувати безпеці людей, а в найгіршому випадку – диктатурі з боку осіб, що контролюють штучний інтелект, або вибуття останнього з-під контролю людей. За цих умов зростає необхідність правового забезпечення цивілізованого (з урахуванням загальносуспільних інтересів) спрямування цифровізації та використання цифровізованих явищ. Таку роль має забезпечувати держава з огляду на наявність у неї відповідних засобів та заінтересованості як захисника суспільних інтересів.

У зв'язку з відставанням державного, в тому числі нормативно-правового, регулювання цифровізації в згаданому ракурсі пропонується низка заходів, спрямованих на забезпечення контролю за використанням електронних ресурсів (а саме: державна реєстрація відповідальних за їх використання у сфері бізнесу та інших публічних сферах осіб; визначення основних засад відповідальності за недобросовісне та/або неконтрольоване чи ризиковане їх використання у сфері економіки; покладення низки додаткових обов'язків на відповідальний за цифровізацію уповноважений орган) та закріплення таких механізмів у кодифікованому акті, присвяченому правовому регулюванню відносин у сфері ЦЕ.

Список використаних джерел:

1. Названо слово року за версією словника сучасної української мови (UA.NEWS). URL: <https://ua.news/ua/nazvano-slovo-goda-po-versiyu-slovaryu-sovremenogo-ukraynskogo-yazyka/> (дата звернення: 27.12.2019).
2. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки : схвалено розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р. *Урядовий кур'єр*. 2018. № 88.
3. Більше половини українців погано розбираються в інтернеті: результати дослідження. URL: <https://aspi.com.ua/news/suspilstvo/bilshopolovini-ukrainciv-pogano-rozbirayutsya-v-interneti-rezultati-doslidzhennya> (дата звернення: 27.12.2019).
4. Коронавірус змінює бізнес: банкіри світу відмовляються від традиційних правил. URL: <https://ua.news/ua/koronavyrus-menyayet-byznes-bankyr-myra-otkazyvayutsya-ot-tradytsyonnyh-pravyl/> (дата звернення: 27.02.2020).
5. Штучний інтелект здатен заробити на біржі 30 % річних. URL: https://ipress.ua/news/shtuchnyu_intelekt_zdaten_zarobyty_na_

birzhi_30_richnyh_203749.html (дата звернення: 22.02.2020).

6. Федоров: Через е-кабінет застройщика начато уже более тысячи строк. URL: <https://journalist.today/fedorov-cherез-je-kabinet-zastrojshhika-nachato-uzhe-bolee-tysjachi-stroek/> (дата звернення: 24.02.2020).

7. Искусственный интеллект нашел мощный антибиотик, убивающий самые опасные бактерии. URL: <https://www.facenews.ua/news/2020/473548/> (дата звернення: 23.02.2020).

8. 250 тис держслужбовців можна замінити роботами та зекономити на податках. URL: https://ipress.ua/news/250_tys_derzhsluzhbovtiv_mozhna_zaminity_robotamy_ta_zeconomytu_na_podatkah_198444.html (дата звернення: 23.02.2020).

9. Елена Филатова. Смарт-зеркала и магазины без касс: технологии, которые изменили шопинг за 10 лет. URL: <https://psm7.com/e-commerce/qr-kody-i-smart-zerkala-texnologii-kotorye-izmenili-shopping-za-10-let.html> (дата звернення: 12.01.2020).

10. Штучний інтелект Google читає по губах на 35 % краще, ніж людина. URL: https://ipress.ua/news/shtuchnyy_intelekt_google_chytaie_po_gubah_na_35_krashche_nizh_lyudyna_188843.html (дата звернення: 22.02.2020).

11. Джон Макафи: использование криминалом анонимных криптовалют предвещает их широкое принятие. URL: <https://forklog.com/dzhon-makafi-ispolzovanie-kriminalom-anonimnyh-kriptoalyut-predveshhaet-ih-shirokoe-prinyatie/> (дата звернення: 22.02.2020)

12. Обнаружен вирус, который научился обходить двухфакторную аутентификацию Google. URL: <https://bykvu.com/ru/bukvy/vijavleno-virus-jakij-navchivsja-obhoditidvuhfaktornu-autentifikaciju-google/> (дата звернення: 29.02.2020).

13. Илон Маск: штучний інтелект є «найбільшою загрозою» людству. URL: https://ipress.ua/news/ilon_mask_shtuchnyy_intelekt_ie_naubilshoyu_zagrozoju_lyudstvu_218751.html (дата звернення: 22.02.2020).

14. Илон Маск: Штучний інтелект може стати «безсмертним диктатором». URL: https://zik.ua/news/2018/04/10/ilon_mask_shtuchnyy_intelekt_mozhe_staty_bezsmertnym_dyktatorom_1301427 (дата звернення: 22.02.2020).

15. В Банке Англии считают стейблкоины возможной угрозой для кредитной системы. URL: <https://internetua.com/v-banke-anglii-scsitauat-steiblkoiny-vozmojnoi-ugrozoi-dlya-kreditnoisistemy> (дата звернення: 02.03.2020).

16. Дэн Лаример: технологические гиганты ведут мир в оруэлловскую антиутопию. URL: <https://forklog.com/den-larimer-tehnologicheskie-giganty-vedut-mir-v-oruellovskuyu-antiutopiyu/> (дата звернення: 28.12.2019).

17. У Китаї вперше робот напав на людину. URL: https://ipress.ua/news/u_kytai_upershe_robot_napav_na_lyudynu_188582.html дата (звернення: 22.02.2020).

18. Киберполиция разоблачила участника международной хакерской группировки. URL: <https://lenta.ua/kiberpolitsiya-razoblachila-uchastnika-mezhdunarodnoy-hakerskoj-gruppirovki-39159/> (дата звернення: 24.02.2020).

19. Киберполіція викрила киянина у спустошенні банківських карток іноземців. URL: <https://internetua.com/kiberpoliciya-vikrila-kiyanina-uspustoshenni-bankivskih-kartok-inozemciv> (дата звернення: 06.02.2020).

20. Илон Маск пожаловался на криптовалютных мошенников в Twitter. Макафи готов решить проблему за 24 часа. URL: <https://forklog.com/ilon-mask-pozhalovalsya-na-kriptoalyutnyh-moshennikov-v-twitter-makafigotov-reshit-problemu-za-24-chasa/> (дата звернення: 22.02.2020).

21. Евросоюз обговорить запровадження санкцій проти РФ і Китаю за кібератаки. URL: <https://ua.news.ua/evrosoyuz-obsudyt-vvedenyesanktsiy-protyv-rf-y-kytaya-za-kyberataky/> (дата звернення: 28.02.2020); ЕС готовит необычные киберсанкции против России – Bloomberg. URL: <https://ghall.com.ua/2020/02/27/es-gotovit-neobychnye-kibersanktsii-protiv-rossii-bloomberg/> (дата звернення: 28.02.2020).

22. Крістофер Стайнер. Тотальна автоматизація. Як комп'ютерні алгоритми змінюють життя / пер. з англ. О. Логоцький. Київ : Наш формат, 2018. 280 с.

23. Дон Текспотт, Алекс Тепскотт. Блокчейн революція. Як технологія, що лежить в основі біткоїна та інших крипто валют, змінює світ / пер. з англ. Ю. Григоренко та Г. Левів. Львів : Літопис, 2019. 492 с.

24. Конфуз Елизаветы II: сайт королевской семьи отсылал посетителей смотреть китайскую порнографию. URL: <http://u-news.com.ua/88197-konfuz-elizavety-ii-sajt-korolevskoj-semi-otsylal-posetitelej-smotret-kitajskuju-pornografiju.html> (дата звернення: 24.02.2020).

25. Воспользуйся лучшей ценой года на кожаную обувь. URL: <https://butiqmall.com/c28e7bc0a6?subid1=2859733&subid2=283579036&subid3=70017&subid4={SiteCategoryID}> (дата звернення: 12.01.2020).

26. Про електронну комерцію : Закон України від 3 вересня 2015 р. № 675-VIII. URL: <https://zakon.rada.gov.ua/laws/show/675-19> (дата звернення: 03.03.2020).

27. Про захист прав споживачів : Закон України від 12 травня 1991 р. № 1023-XII. URL: <https://zakon.rada.gov.ua/laws/show/1023-12> (дата звернення: 03.03.2020).

28. Про електронні довірчі послуги : Закон України від 5 жовтня 2017 р. № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення: 03.03.2020).

29. Штучний інтелект рекламують як вирішення усіх проблем, насправді ж він часто помиляється й не може замінити людину – інженер з Принстона пояснює чому. URL: <https://thetabel.com.ua/texts/38487-shtuchnyy-intelekt-reklamuyut-yak-virishennya-usih-problem-naspravdi-vin-chasto-pomilyaetsya-й-ne-mozhe-zaminity-lyudynu--inzhener-z-Prinstona-poyasnyuє-чому>

romilyayetsya-i-ne-mozhe-zaminiti-lyudinu-inzhener-z-prinstona-poyasnyu-chomu (дата звернення: 01.03.2020).

30. Що таке СШІ. URL: <http://ai.lviv.ua/ais/> (дата звернення: 01.03.2020).

31. В Євросоюзі розробили «етикет» для штучного інтелекту. URL: <https://www.ukrinform.ua/rubric-technology/2676698-v-evrosouzi-rozrobili-etiket-dla-stuchnogo-intelektu.html> (дата звернення: 01.03.2020).

32. Вінник О.М. Правове забезпечення цифрової економіки та електронного бізнесу : монографія. Київ, 2018. 212 с. URL: <https://drive.google.com/file/d/1vxqKHGxjYnZ30HgZUU6TNAZEXytW5nsK/view>. (дата звернення: 01.03.2020).

33. Стефанчук анонсував медичний і цифровий кодекси. URL: https://ukr.lb.ua/news/2020/02/25/450867_stefanchuk_anonsuvav_medichniy_i.html (дата звернення: 25.02.2020).

34. Вінник О.М. Потенціал Господарського кодексу України в ракурсі цифровізації економіки та соціального її спрямування. *Підприємництво, господарство і право*. 2020. № 2. С. 25.

35. Regulation (EU) № 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) № 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0524> (дата звернення: 22.08.2019).

36. Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR). URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0063:0079:EN:PDF> (дата звернення: 22.08.2019).

The article addresses the legal challenges of ensuring the digital focus of digitalisation in order to minimize the risks involved and to promote the benefits of digital technologies. The properties of digital phenomena (including artificial intelligence, virtual enterprises, business sites, etc.) are analyzed in terms of the benefits they provide and the risks arising from their unfair or uncontrolled use.

Among the advantages are speed (of sharing information, finding the right solutions, assessing the situation, paying, etc.), convenience (without the mandatory presence of interested persons in a particular place at a certain time), high efficiency (scientific and marketing research, business operations), accessibility (possibility to use regardless of the location of the customer / buyer and contractor / seller, service provider), economy (reduction of costs), trans nationality (wide possibilities of ordering goods / searching for a counterparty abroad), unlimited in time (without breaks, mode of operation and output) and others. However, in addition to the aforementioned advantages, the digitized phenomena (artificial intelligence, virtual enterprises, business sites, etc.) present significant risks associated with fraudulent and / or uncontrolled use. This can result in significant material loss, a threat to human security, and in the worst case, dictation by those who control artificial intelligence, or the latter out of control. Under these conditions, there is a growing need for legal support for the civilization (taking into account public interests) of digitalisation and the use of digitally addressed phenomena. The state should play a similar role in view of the availability of adequate resources. First and foremost, it concerns regulatory regulation, the improvement of which should include legal mechanisms for controlling the use of electronic resources, including the introduction of state registration of those responsible for their use in public spheres, the main principles of liability of such persons for fraudulent and / or uncontrolled electronic resources. use in public areas, including business. It is proposed to consolidate such mechanisms in a codified act, which may be the current Economic Code of Ukraine or a new one – the Digital Economy Code or the Digital Code.

Key words: digitalization, digital economy, Artificial Intelligence, virtual enterprise, business sites, responsibility.

