Інформаційне право

УДК / UDC: 34:004:005.334
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364213

Володимир Арсентійович Ященко
Державна наукова установа "Інститут інформації, безпеки і права Національна академія правових наук України"
Київ, Україна
ORCID: https://orcid.org/0000-0002-2257-318X

РИЗИК ОРІЄНТОВАНИЙ МЕТОД ПРАВОВОГО РЕГУЛЮВАННЯ ЦИФРОВИХ ПРОЦЕСІВ

Анотація. *Прогрес цифрових технологій в Україні зумовив потребу удосконалення змісту та розширення сфери регламентації правових норм як відповіді на технологічні інновації. В ході регулювання цифрового контенту та цифрових послуг пропонується підхід, оснований на ризик-орієнтованій методології, яка останнім часом стала одним із ключових факторів впорядкування цифрових технологій у тому числі й штучного інтелекту.*

У статті аналізується зміст Законів України "Про інформацію", "Про електронні документи та електронний документообіг", "Про цифровий контент та цифрові послуги", "Про захист персональних даних" на предмет їх відповідності Національним стандартам України (ДСТУ IEC/ISO 3110: 2013, ISO 9001:2015, ДСТУ ISO 31000:2018), щодо методів оцінювання ризиків, їх рівнів, ідентифікації, стандартизації методів нормування ризиків та мінімізації їх можливої шкоди.

Проведений аналіз засвідчив, що це законодавство, побудоване за технологічно процесуальним типом, поетапно відтворює логіку цифрового процесу, виявляє ймовірні ризики, що супроводжують цей процес, і пропонує норми його регулювання. Водночас екстраполяція в профільних законах стандартних вимог оцінки ризиків, їх тяжкості та ймовірності, виявлення небезпечних значень тощо, не повною мірою реалізовується, що у свою чергу створює проблеми диференціації регуляторних практик. Звідси робиться висновок, що кількісно-якісний аналіз ризиків, розробка новітніх методологічних теорій до їх виявлення та мінімізації ще не задіяні належним чином в цифровій правотворчості. Пропонується нормативні концепції у цій сфері реалізувати через більш чітке визначення рівнів ризиків, їх кількісно-якісної оцінки, врахування переваг технологій та встановлення прийнятних рівнів ризиків.

В якості інструменту удосконалення ризик-орієнтованого методу запропоновано актуалізувати питання розвитку ризик-орієнтованого мислення, яке дає можливість узагальнення відображення цифрової дійсності і вироблення заходів, що запобігають або мінімізують порушення технологічних процесів.

Ключові слова: *ризик-орієнтований метод, цифрові технології, цифровий процес, цифровий контент, штучний інтелект, національний стандарт України, регулювання ризиків.*

Volodymyr A. Yashchenko
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2257-318X

RISK-ORIENTED METHOD OF LEGAL REGULATION OF DIGITAL PROCESSES

Summary: *The progress of digital technologies in Ukraine has necessitated the improvement of the content and expansion of the scope of legal norms as a response to technological innovation. In the course of regulating digital content and digital services, an approach based on risk-oriented methodology is proposed, which has recently become one of the key factors in organizing digital technologies, including artificial intelligence. The article analyzes the content of the Laws of Ukraine "On Information", "On Electronic Documents and Electronic Document Management", "On Digital Content and Digital Services", and "On Personal Data Protection" regarding their compliance with the National Standards of Ukraine (DSTU IEC/ISO 31010:2013, ISO 9001:2015, DSTU ISO 31000:2018) concerning risk assessment methods, their levels, identification, standardization of risk regulation methods, and minimization of their potential harm.*

The analysis demonstrated that this legislation, built on a technological-procedural type, step-by-step reproduces the logic of the digital process, identifies probable risks accompanying this process, and proposes norms for its regulation. At the same time, the extrapolation of standard requirements for risk assessment, their severity and probability, and the identification of dangerous values is not fully implemented in specialized laws, which in turn creates problems in the differentiation of regulatory practices. Hence, it is concluded that quantitative and qualitative risk analysis, as well as the development of modern methodological theories for their detection and minimization, are not yet properly utilized in digital lawmaking.

It is proposed to implement normative concepts in this area through a clearer definition of risk levels, their quantitative and qualitative assessment, consideration of technology benefits, and the establishment of acceptable risk levels. As a tool for improving the risk-oriented method, it is suggested to actualize the development of risk-oriented thinking, which allows for a generalized reflection of digital reality and the development of measures that prevent or minimize disruptions in technological processes.

Keyword: *risk-oriented method, digital technologies, digital process, digital content, artificial intelligence, national standard of Ukraine, risk regulation.*

Постановка проблеми. На вирішення проблеми постійного оновлення правових норм у зв'язку з потребою мінімізації ризиків швидкої еволюції цифрових технологій та штучного інтелекту, застосовується ризик-орієнтований метод. Цей метод нині став домінуючим фактором регулятивного втручання в регламентацію технологічних процесів, який створює можливість встановлення джерел ризиків, їх оцінки, класифікацію тощо, що дозволяє адаптувати правові норми до потреб унормування цих технологій, а відтак цей метод набуває регулятивного статусу. Аналіз профільного законодавства України через призму ризик-орієнтованого методу дозволяє з'ясувати досягнення та недопрацювання у забезпеченні подальшого безпечного для суспільства інноваційного розвитку технологій, сформувати диференційовані моделі їх впорядкування відповідно до різних рівнів ризику, а відтак впровадити заходи підвищення їх безпекової ефективності.

Результати аналізу наукових досліджень. Підґрунтям аналізу профільних законодавчих актів обрані Національні стандарти України щодо методів оцінювання ризиків (ДСТУ IES/ISO 3110:22013), формування ризик-орієнтованого мислення (ISO

9001:2015), ідентифікації ризиків (ДСТУ ISO 31000:2018). Основним методом став аналіз рівня екстраполяції вимог стандартів у змісті законодавчих актів, які регулюють цифрові процеси в України шляхом їх профілювання, відповідно до умов конкретної галузі чи сфери регулювання.

З метою уточнення формулювання поняття "ризику" використано відповідний зміст Національних стандартів України, окремі положення Регламенту (ЄС) 2024/1689 Європейського парламенту та Ради від 13 червня 2024 року, матеріали статті Мартіна Еберса щодо ризик орієнтованій відповідності цього Закону, в якій він висвітлює концептуальні засади впровадження даного методу для регулювання цифрових технологій.

Взято до уваги також точку зору Джулії Блек щодо інституалізації ризик-орієнтованого підходу, яка визнає ризики не просто технічним інструментом, а цілісною стратегією управління. Регулятор визначає цілі, ідентифікує ризики для цих цілей, розподіляє ресурси пропорційно до рівня цих ризиків (чим вищий ризик, тим жорсткіше регулювання).

В ході аналізу використано публікації з питань захисту прав споживачів в цифровому середовищі Гудими-Підвербецької М.М., яка акцентує увагу на ризиках порушення конфіденційності, невиконання договору, неналежної якості цифрових послуг, ризики маніпуляцій споживчою поведінкою через алгоритми, цілеспрямовану рекламу, Капітаненко Н.П. щодо правового забезпечення електронного документообігу, Юзько Т.М., Тунік Ю.М., Слугоцької В.М., відносно особливостей впровадження електронного діловодства в юридичній практиці.

Мета. На основі аналізу законодавства, що регулює функціонування цифрового середовища, висвітлення аспектів, які заслуговують схвалення та проблемних ситуацій, запропонувати шляхи та напрямки удосконалення законодавства та поліпшення використання ризик-орієнтованого методу регулювання цифрового середовища.

Виклад основного матеріалу. Стрімкий розвиток інформаційної складової сучасного суспільства закономірно активує потребу удосконалення інформаційних відносин, а відтак процесу їх правового регулювання, як відправного моменту їх практичної реалізації. Зауважимо, особливість формування інформаційних відносин дещо відрізняється від звичного уявлення своєю багатогранністю, поєднанням в їх змісті національного та міжнародного законодавства, інформаційно – технологічних аспектів, цифрових технологій, штучного інтелекту тощо, що зумовлює потребу пошуку нових підходів та методів до формування норм інформаційного права. Однією з ключових проблем стало питання належного правового регулювання цифрових процесів, тобто, правового забезпечення перетворення аналогової інформації в цифрову, юридичних способів об'єднання її фізичних та обчислювальних компонентів в освіті, виробництві, державному (публічному) управлінні тощо.

Традиційні імперативний та диспозитивний методи побудови правових норм, як засадні, висхідні для права в цілому та інформаційного права зокрема, були і залишаються одними з провідних методів, які, під впливом інформаційно-технологічних процесів теж трансформуються, набувають більш широкого, комплексного наповнення.

У наукових публікаціях щодо методів інформаційного права, як правило, стверджується, що на відміну від цивільного, адміністративного права, особливістю цих методів є їх комплексне застосування, тобто, поєднання імперативних та диспозитивних підходів. Насправді ця комплексність не є особливістю інформаційного права, вона

притаманна також іншим галузям права: цивільному, адміністративному, військовому тощо.

Так, у цивільному праві, крім диспозитивних, мають місце імперативні норми, наприклад, строки позовної давності та порядок їх обчислення; в адміністративному, поряд з імперативними нормами, також міститься ряд важливих диспозитивних норм, скажімо, право на оскарження, адміністративні договори; у військовому праві, де закономірно переважають імперативні норми, диспозитивні за змістом право військовослужбовців та ветеранів на медичну допомогу, контрактний спосіб формування кадрів ЗСУ, прийняття військової присяги – одні з найважливіших норм, без яких реалізація функцій оборони держави неможлива. Характерним є те, що в даних галузях права має місце фактор переважання одних методів над іншими.

Особливість же інформаційного права в тому, що через "всюдисущість" інформації, потреби регулювання її вироблення, зберігання, передачі, використання в різних сферах державної, суспільної діяльності, породжують різноспрямованість методів формування правових норм, тому ні імперативний, ні диспозитивний методи в інформаційному праві не мають переваги, а є однопорядковими. Тим більш важливо з'ясувати особливості модернізації цих методів у цифрових технологіях, як сукупності юридичних способів впливу держави на суспільні відносини в інформаційній сфері, що дасть змогу більш ефективно розбудовувати інформаційно- правові норми.

Зважаючи на зростаючий рівень небезпечності техногенних чинників, а також те, що в природі інформаційного права поєднуються як соціально – правові, так і технологічні, технічні норми та стандарти, цифрові процеси, які регулюють доступність інформації та її безпекову складову, представляють в єдності техніко-правові форми, практика формування інформаційно-правових норм, регулювання цифрових процесів зумовила виникнення та впровадження ризик-орієнтованого підходу їх формування, який за останні роки став, за висновком дослідника цього підходу у законодавстві ЄС, Мартіна Еберса: "домінуючою стратегією для політиків щодо ШІ – не лише в ЄС, а й у всьому світі – як на міжнародному, так і на національному рівнях, а також у роботі (міжнародних) органів зі стандартизації"[2].

М. Еберс досить ґрунтовно розкриває внутрішній зміст ризик-орієнтованого підходу, як засадного у регулюванні ШІ: "…основною метою є досягнення оптимального (або пропорційного) балансу між інноваціями та перевагами систем штучного інтелекту, з одного боку, та захистом фундаментальних цінностей, таких як безпека, здоров'я та основні права, з іншого" [2]. Таким чином, реалізація цієї мети можлива за умови ідентифікації та оцінки. Згідно пункту 26 Регламенту (ЄС) 2024/1689 Європейського парламенту та Ради від 13 червня 2024 року (далі Регламент ЄС): "Цей підхід має адаптувати тип та зміст таких правил до інтенсивності та масштабів ризиків, які можуть створювати системи штучного інтелекту. Тому необхідно заборонити певні неприйнятні практики використання штучного інтелекту, встановити вимоги до систем штучного інтелекту з високим рівнем ризику та зобов'язання для відповідних операторів, а також встановити зобов'язання щодо прозорості для певних систем штучного інтелекту" [1]. Вважаємо, що ця глобальна мета ризик-орієнтованого підходу та умови її реалізації за своєю змістовною наповненістю спрямовані не лише на регулювання ШІ, а практично на всі сфери інформаційного права та цифрових технологій.

Суть ризик-орієнтованого підходу полягає в тому, що ризики в даному випадку розглядаються в якості інструменту формування правових норм, дають можливість застосування принципу пропорційності до правового регулювання юридичного об'єкту

з метою здійснення диференціації рівня дозволено - недозволено в залежності від того, яка суспільна користь від використання цього об'єкту та одночасно враховується ймовірність створення ним небезпеки (шкоди). У статті 1 Регламенту ЄС із врахуванням ризиків встановлені комплексні "гармонізовані правила" використання систем ШІ, заборони певних практик, правила прозорості, моніторингу тощо [1]. Отже, ризики виступають в якості способу регулювання ШІ та цифрового середовища в цілому, в такому разі вони виконують функцію правового методу, тому ризик орієнтовний підхід слід кваліфікувати методом регламентації інформаційного права та цифрового середовища.

Таке тлумачення підтверджується Джулією Блек, ідеї якої використовуються в багатьох нормативних актах, що регулюють цифрове середовище, дає глибоке філософське й практичне обґрунтування того, як ризик став "центральним сонцем", навколо якого обертається сучасне регулювання. Вона стверджує, що "регулювання змістилося від контролю за діяльністю до управління ризиками, тобто, ймовірністю настання негативних наслідків". Д.Блек фокусується на "колонізації" поняття ризику, аналізуючи те, як об'єктивоване поняття ризику (ймовірність × наслідки) "колонізує" правову та адміністративну сфери, перетворюючи політичні та соціальні питання на управлінські задачі [3,с.304,310].

Слід зазначити, що цей метод є природним для права, він може виступати в якості дозвільного інструменту, рекомендаційного чи заборонного регулятора, враховує пропорційність заохочення та покарання в залежності від рівня завданої шкоди, а його актуалізація в кінці XX на початку XX1 століття зумовлена нагальною потребою встановлення таких правил суспільного прогресу, які б мінімізували можливості техногенних катастроф, нових технологічних ризиків для безпеки, здоров'я людини та існування суспільства. Ці обставини фактично надають ризик-орієнтованому методу статусу методологічного арсеналу сучасної юридичної науки.

Оскільки ключовим терміном даного дослідження виступає поняття "ризику", є потреба уточнити це поняття. Як відомо, поняття ризику пов'язується з ймовірністю виникнення негативних наслідків для людини та суспільства, усвідомленням небезпеки. Тобто, має місце ситуація невідомості щодо того, відбудеться певна подія чи ні, що створює невизначеність. Таким чином природа ризику безпосередньо пов'язана як з небезпекою, так і невизначеністю. П.2 статті 3 Регламенту (ЄС) визначає ризик як "поєднання ймовірності виникнення шкоди та тяжкості цієї шкоди"[1].

Мартін Еберс зазначає, що регулювання ШІ "… дотримується підходу, що ґрунтується на оцінці ризиків, – такого, що адаптує вибір та розробку регуляторних інструментів до рівня ризику, згідно з правилом: "чим вищий ризик, тим суворіші правила". З цією метою Регламент ЄС розрізняє чотири категорії ризику (неприйнятний, високий, обмежений та мінімальний), визначаючи регуляторні вимоги на основі ризиків, що створюються системами ШІ" [2].

Поняття ризику зафіксовано також в українському правовому полі. Згідно п.03.3 Національного стандарту України ДСТУ ISO 9001:2015 "ризик — це вплив невизначеності, а будь-яка невизначеність може мати позитивний чи негативний впливи. Позитивний відхил, зумовлений ризиком, може забезпечувати певну можливість, але не всі позитивні впливи ризику ведуть до можливостей"[4. Отже, ризик – це можливість настання негативних наслідків, виникнення небезпеки в умовах невизначеності.

За розпорядженням КМ України "Про затвердження Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру" засадними основами для формування "нормативної бази ризиків є два

основних рівні: мінімальний і гранично допустимий. Під час визначення рівнів прийнятних ризиків застосовуватимуться значення ризиків, що використовуються в економічно розвинутих державах, а саме: мінімальний ризик - менший або який дорівнює $1 \cdot 10^{-8}$; гранично допустимий ризик - який дорівнює $1 \cdot 10^{-5}$. Ризик, значення якого нижче або дорівнює мінімальному, вважається абсолютно прийнятним. Ризик, значення якого більше гранично допустимого, вважається абсолютно неприйнятним" [5].

В принципі чотири категорії ризику в Регламенті (ЄС) і два рівні ризику розпорядження КМ України не суперечать один одному і в узагальненому вигляді є однотипними. Поряд з цим вживаний в Концепції термін "рівні ризиків", на нашу думку, більшою мірою відповідає оцінці ризику, ніж категорії, про які пише Мартін Еберс.

Зважаючи на важливе значення ризик-орієнтованого методу у регулюванні інформаційно – технологічних процесів розглянемо окремі нормативні акти України, які тим чи іншим чином регулюють процеси цифрової трансформації, через призму врахування в їх змісті різних аспектів ризиків.

До критеріїв аналізу пропонується віднести сформульовані в національних стандартах ДСТУ IEC /ISO3110: 2013 [7] та ДСТУ ISO 31000:2018 [6] вимоги: ідентифікації ризиків; визначення їх рівнів; нормування цих рівнів; менеджменту ризику, методи оцінювання ризиків, стандартизація цих методів, які також мають місце і в Регламенті ЄС.

В першу чергу, доцільно з'ясувати, наскільки відповідає вимогам даного підходу один з основних нормативних актів у цій сфері - Закон України "Про інформацію". На момент прийняття цього Закону ризик орієнтовний метод ще не набув поширення в правотворчості, тому терміни ризики, небезпеки тощо в ньому відсутні. Поряд з цим за характером змісту статей Закону можна зробити висновок про те, що на той час основними інформаційними ризиками були обмеження доступності інформації, що створювало викривлене уявлення про життєдіяльність суспільства та недостатня розробленість системи захисту конфіденційної інформації про особу. У зв'язку з цим значна частина норм Закону регулює питання права на інформацію та захист інформації (ст.3 – державна інформаційна політика – розглядаються проблеми доступності інформації, ст.5 - право на інформацію, ст.6 – гарантії права на інформацію, ст.7 – охорона права на інформацію, ст.11 – забезпечення вільного доступу до інформації, ст.24 – заборона цензури тощо) [8].

Слід визнати, що така логіка цього Закону, розвинута у Законі України "Про доступ до публічної інформації", рівень ризику обмеження доступності до інформації знизила до прийнятного. При цьому законодавець не обмежився лише констатацією досягнутого, а юридично закріпив розуміння інформації як товару, що створило умови для подальшої розбудови інформаційного суспільства. Водночас ймовірні ризики маніпуляції інформацією, їх класифікація, проведення цілеспрямованих психологічних операцій, дезінформаційні виклики тощо фактично не визначаються, що може призвести до порушення системи інформаційної комунікації.

Щодо ризик-орієнтованого змісту Закону України "Про цифровий контент та цифрові послуги", то він побудований на апріорних засадах того, що виробничі відносини з приводу створення та використання цифрового контенту та цифрових послуг стрімко розвиваються, трансформуються і їх упорядкування потребує належного правового регулювання. Звідси зміст Закону розкриває саму технологію формування та розвитку відносин між виконавцем цифрового контенту, суб'єктом надання цифрових

послуг та їх споживачем. Тому ймовірність ризиків завдання шкоди цим відносинам концентрується навколо проблем якості цифрового контенту, його відповідності угоді зі споживачем, надійності та довготривалості дії контенту тощо.

У зв'язку з цим ст.2 Закону передбачає інтеграційність цифрового контенту з елементами цифрового середовища споживача, його модифікацію, функціональність, тобто, придатність до виконання передбачених функцій. Статтями 4, 5, 6 Закону передбачено суб'єктивні та об'єктивні критерії відповідності цифрового контенту та цифрових послуг вказаним вимогам, у разі порушення яких створюються ризики припинення відносин між виконавцем та споживачем [10]. Водночас рівні цих ризиків, їх нормування, методологія визначення прихованих небезпек, що можуть нести цифрові технології (прозорість інтернет реклами, онлайн ризики та ін.) не визначені.

У Законі України "Про цифровий контент та цифрові послуги" глобальні проблеми можливого створення цифровим контентом та цифровими послугами безпекових ризиків для людини та суспільства не розглядаються, застосовуються бланкетні норми [10]. В даному випадку законодавець посилається на Закон України "Про захист прав споживачів", стаття 1 якого передбачає безпеку продукції – "відсутність будь-якого ризику для життя, здоров'я, майна споживача і навколишнього природного середовища при звичайних умовах використання, зберігання, транспортування, виготовлення і утилізації продукції" [11].

Водночас, навряд чи можливо в загальному вигляді забезпечити належні права споживачів цифрового контенту та цифрових послуг в специфічних умовах цифрового середовища, яке формує власні виклики та можливі негативні наслідки використання послуг, не розкриває потенційно шкідливі характеристики впливу технологій штучного інтелекту на розвиток цифрового контенту, не здійснює диференціацію ризиків щодо дотримання права інтелектуальної власності, захисту конфіденційних даних, застосування технології смарт – контракту, яка змінює саму організацію бізнесу тощо. В цьому контексті Закон України "Про цифровий контент та цифрові послуги" потребує, вважаємо, суттєвого доопрацювання.

Як справедливо вказує Гудима - Підвербецька М.М.: "В час цифрового десятиріччя гостро постає питання захисту прав споживачів… Істотними серед яких можуть виявитися порушення конфіденційності, невиконання договору, укладеного на просторах Інтернету, неналежна якість цифрових послуг, ризики маніпуляцій споживчою поведінкою через алгоритми, цілеспрямовану рекламу та обмежену прозорість у роботі платформ" [12,с.87].

Закон України "Про електронні документи та електронний документообіг" технологічно процесуально регулює різні аспекти створення, обробки та зберігання електронних документів, тому безпекові складові його контенту концентруються навколо проблем цілісності, автентичності електронного документу, можливості його візуального відтворення, довго тривалості зберігання та ін. питання. Важливим безпековим аспектом є "обов'язковий реквізит електронного документа - обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили" [13, ст.1]. Це є прикладом ризик орієнтованого регулювання, де порушення технічних вимог анулює правову дію.

Можливі ризики недостовірності електронного документу нівелюються передбаченим ст.6 Закону електронним підписом та електронною печаткою. Один з важливих ризиків – створення умов для довготривалого зберігання електронного документа у тій формі, яка дозволяє перевірити її ідентичність. Зважаючи на потреби

зберігання електронного документа в цілісності та можливі ризики його втрати, ст.13 Закону встановлює обов'язкові вимоги до умов його зберігання:

"1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання" [10].

Такий підхід стимулює бізнес запроваджувати технології, які забезпечують довгострокове архівування електронних документів та зберігання важливих даних. Зокрема, застосування технології **LTA (Long Term Archive)** — технології, що періодично "перепідписують" документи новими ключами (архівні штампи часу). Інтерфейс LTA містить усі функції, необхідні для запиту збережених даних, запиту інформації про продуктивність для цілей моніторингу та отримання вибраних даних. Інтерфейс LTA забезпечує точні можливості запитів для стандартних метаданих, з детальним визначенням індексованих полів для кожного типу даних [14].

Позитивним з точки зору ризик орієнтованого підходу є норма (ст.15), згідно якої суб'єкти документообігу мають самостійно встановлювати рівень захисту документів, враховуючи ступінь їх конфіденційності. Це покладає відповідальність за оцінку ризиків на суб'єктів документообігу, а також дозволяє бізнесу диференційовано витрачати кошти на забезпечення конфіденційності.

На думку Капітаненко Н.П., яка не підтримана статистичними даними та соціологією, чинна практика електронного документообігу заслуговує схвалення: "Електронна форма документів забезпечує необхідний рівень інформаційної безпеки учасників правовідносин, бо обмін документами відбувається у зашифрованому вигляді з використанням кваліфікованого електронного підпису. Має місце економія людських та матеріальних ресурсів, які раніше використовувалися для друку, відправки та зберігання документів. Дистанційні переваги забезпечують мобільність та зручність пересилання документів через платформи електронного документообігу або електронну пошту" [15,с.136].

Водночас Юзько Т.М., Тунік Ю.М., Слугоцька В.М., на основі аналізу юридичної практики виокремлюють ряд суттєвих проблем, пов'язаних з впровадженням електронного діловодства. Зокрема, вони вказують на "відсутність взаємної сумісності між різними електронними системами. Наприклад, у юридичній практиці одночасно використовуються кілька окремих цифрових платформ (ЄСІТС, портал "Дія", електронний кабінет платника податків тощо), які не завжди інтегруються між собою. Це призводить до дублювання даних, затримок у роботі та ускладнення міжвідомчої комунікації." [16, с.256]. Автори відзначають недостатній рівень довіри до цифрових технологій у сфері судочинства, обмеження лише загальними положеннями законодавчого регулювання електронних доказів, потребу створення надійних резервних каналів зв'язку та технічної підтримки, а також удосконалення процесуальних строків і фіксації моменту подання електронного документа. [16, с.258].

Таким чином, в цьому Законі викладені регулятивні механізми технології впорядкування цифрового контенту та надання цифрових послуг, водночас загальні вимоги національних стандартів не отримали в Законі своєї профільної наповненості, у зв'язку з чим потребують подальшого регулювання питання ідентифікації ризиків, пов'язаних з зі створенням електронних документів та їх обігом, інтеграцією цифрових

платформ, збоїв у роботі систем, визначення ймовірних рівнів цих ризиків, їх мінімізація, стан надійності процедури ідентифікації електронного підпису, збереження цілісності інформації та її автентичності. У разі залишення Закону без змін виникає питання доцільності його існування, оскільки технологічний процес може бути успішно відтворений в цивільному кодексі України.

Закон України "Про захист персональних даних" чи не найбільш повно відображає у своєму змісті принципи ризик-орієнтованого методу і створює юридичні умови для збереження персональних даних та мінімізації ризику їх несанкціонованого витоку [17]. Водночас, він також побудований технологічно-процесуально і ризик як регулятивний фактор не профілюється відповідно до стандарту, що ускладнює процес оцінки впливу ризиків на чинний захист даних. У зв'язку з цим Закон потребує якісного оновлення, в першу чергу відповідно до вимог Загального регламенту ЄС про захист даних (GDPR) "Цей регламент діє в межах законодавства Європейського Союзу (ЄС) та Європейської економічної зони (ЄЕЗ) щодо захисту персональних даних усіх осіб у межах Європейського Союзу а також експорту персональних даних за межі ЄС і громадяни України, які здійснюють бізнес на європейському ринку також підпадають під дію регламенту" [18].

Таким чином проведений аналіз чинного законодавства, що регулює цифрове середовище, засвідчує, що наявний в них ризик орієнтовний зміст не формується на основі кількісно – якісного аналізу можливих небезпек та шкоди, а має умоглядний характер, базується на спогляданні, абстрактному уявленні про ризики. Наприклад, має місце така закономірність - якщо існують конфіденційні дані, значить є ризик їх витоку, який слід мінімізувати. З одного боку це правомірно, оскільки є відповіддю на потребу дня. В даному випадку має місце застосування "реактивного" мислення – безпосередньої реакції на проблему.

З іншого, формування індикаторів ризиків, що можуть призвести до розголошення даних, оцінка впливу організаційно-технічних заходів на нейтралізацію чи зменшення небезпечності ризиків, моделювання захисту цих даних здійснюється на повсякденному рівні, що не дає можливості прогнозувати швидкоплинні зміни технологічних умов та характеристик цифрового процесу, тобто, потрібен перехід від реактивного до проактивного прогнозування виникнення ризиків, конкретного, дослідного вивчення закономірностей, об'єктивних та суб'єктивних причин їх формування та прояву.

Усвідомлюючи складність математичного, індуктивного визначення рівнів ризиків, їх нормування для виявлення небезпечних значень, стандартизації методів визначення рівнів, все ж ці процеси потребують задіяння наукового підходу до узагальнення, універсалізації ризикових ознак, розробки новітніх методологічних підходів до їх виявлення, які ще не задіяні належним чином в цифровій правотворчості. В іншому разі наступний етап регулювання – управління ризиками, навряд чи буде успішним.

У конкретних галузях цифрового контенту чинні Національні стандарти, зміст Розпорядження КМ України "Про затвердження Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру" [5], в частині вимог застосовувати у нормативних актах та практичних безпекових заходах значення ризиків, статистичні дані потенційно небезпечних оцінок різних галузей, що піддаються регламентації, залишається не реалізованим повною мірою через те, що загальні вимоги не адаптуються до потреб конкретної галузі регулювання. Ці обставини, у свою чергу, знижують ефективність законодавства і можуть створити ризики уповільнення впровадження цифрових процесів.

Висновки. Ефективне застосування ризик-орієнтованого методу в цифровому середовищі є не локальним, а суспільно значущим аспектом удосконалення процесу правового регулювання цифровізації суспільства, і потребує внесення змін до нормативних актів шляхом профілювання вимог та підходів, сформульованих у відповідних стандартах. Однак у глобальному вимірі вирішити цю проблему можливо через формування ризик-орієнтованого мислення серед ІТ фахівців та спеціалістів з інформаційного права, що передбачено Національним стандартом України ISO 9001:2015.

Саме ризик-орієнтоване мислення, яке ґрунтується на уявленнях та образах можливих загроз та небезпек, які супроводжують впровадження цифрового контенту, дає можливість виявити істотні характеристики цифрової технології, встановити суттєві ознаки чинників, які можуть негативно вплинути на досягнення її позитивного результату, згрупувати ризики за цими ознаками та виробити заходи, що запобігають або мінімізують порушення технологічних процесів. Ефективним цей процес може бути лише в тому випадку, коли прийняття будь-якого технологічного, правового, організаційного тощо рішення в цифрових технологіях буде проходити через призму аналізу ризиків.

Більш того, ризик-орієнтоване мислення створює можливість розвитку ризик-менеджменту як цілісної функції безперервного процесу аналізу, узагальнення ризиків по мірі їх виникнення, прогнозування наслідків їх дії і вироблення конкретних кроків з вирішення проблемної ситуації. Пропонується тематику ризик-менеджменту включити до програм підготовки фахівців з інформаційного права.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література.

1. Регламент (ЄС) 2024/1689 Європейського парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту та вносить зміни до Регламентів (ЄС) № 300/2008, (ЄС) № 167/2013, (ЄС) № 168/2013, (ЄС) 2018/858, (ЄС) 2018/1139 та (ЄС) 2019/2144 та Директив 2014/90/ЄС, (ЄС) 2016/797 та (ЄС) 2020/1828 (Закон про штучний інтелект) URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#document1- дата звернення: 03.04.26 р.

2. Мартін Еберс. Дійсно ризик орієнтоване регулювання штучного інтелекту. Як впровадити Закон ЄС про штучний інтелект. URL: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/truly-riskbased-regulation-of-artificial-intelligence-how-to-implement-the-eus-ai-ct/E526C1D0D7368F9691082220609D60F4?utm_source=chatgpt.com – дата звернення: 03.04.26 р.

3. Julia Black: "The Role of Risk in Regulatory Processes" *(The Oxford Handbook of Regulation, 2010, pp. 302-348).*

4. Національний стандарт України: ДСТУ ISO 9001:2015. Системи управління якістю: Наказ від 21.12.2015 № 203 Про прийняття нормативних документів України, гармонізованих з міжнародними та європейськими нормативними документами, та скасування нормативних документів України // Державне підприємство «український науково – дослідний і навчальний центр проблем стандартизації, сертифікації та якості».

5. Про затвердження Концепції управління ризиками, виникнення надзвичайних ситуацій техногенного та природного характеру: Розпорядження КМ України від 22.01.2014 № 37-р.

6. Національний стандарт України: ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови: Наказ від 29.11.2018 № 446 Про прийняття та скасування

національних стандартів, прийняття поправки до національного стандарту //Державне підприємство «Український науково – дослідний і навчальний центр проблем стандартизації, сертифікації та якості»

7. Національний стандарт України ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT): Наказ Мінекономрозвитку України від 11 грудня 2013 р. N 1469

8. Про інформацію: Закон України від 02.10.1992. № 2657-XII. Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650

9. Про доступ до публічної інформації: Закон України від 13.01.2011. № 2939-VI. Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314

10.Про цифровий контент та цифрові послуги: Закон України від від 10.08.2023. № 3321-IX. Відомості Верховної Ради (ВВР), 2023, № 90, ст.345

11. Про захист прав споживачів: Закон України від 12.05.1991 № 1023-XII. Відомості Верховної Ради УРСР (ВВР), 1991, № 30, ст.379

12. Гудима-Підвербецька М.М. Захист прав споживачів у цифровому середовищі: виклики та перспективи //Науковий вісник Ужгородського Національного Університету, 2024. Серія ПРАВО. Випуск 86: частина 2. с.87-94. URL:https://doi.org/10.24144/2307-3322.2024.86.2.14) - дата звернення: 25.04.26р.

13.Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275

14. Збереження даних та довгостроковий архів) - https://sentinels.copernicus.eu/copernicus-operations/data-preservation-and-long-term-archi.

15. Капітаненко Н.П Правове забезпечення електронного документообігу //Науковий вісник Ужгородського університету Серія ПРАВО. Випуск 84: частина 3. 2024. С.130-138)

16. Юзько Т.М., Тунік Ю.М., Слугоцька В.М. Особливості впровадження електронного діловодства в юридичній практиці: організаційні та процесуальні аспекти Науковий вісник Ужгородського Національного Університету, 2025 Серія ПРАВО. Випуск 90: частина 2. - с.253-258

17. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481

18. Загальний регламент ЄС про захист даних (GDPR) (GDPR) URL:kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf. – дата звернення: 21.03.26р.

Володимир Арсентійович Ященко
доктор юридичних наук, професор
головний науковий співробітник Державної наукової установи “Інститут інформації, безпеки і права Національної академії правових наук України”
04053, Україна, м. Київ, пров. Несторівський, 4
email: vay_@ukr.net

Volodymyr A.Yashchenko
Doctor of Law, Professor
Chief Research Fellow
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
4 Nestorivskyi Lane, Kyiv, 04053, Ukraine
email: vay_@ukr.net

Рекомендоване цитування: Ященко В.А. Ризик орієнтовний метод правового регулювання цифрових процесів. *Інформація і право*. № 2(57)/2026. 2026. С. 10-21. https://doi.org/10.37750/2616-6798.2026.2(57).364213

Suggested Citation: Yashchenko V. (2026) Risk-Oriented Method of Legal Regulation of Digital Processes. *Information and Law*. 2(57)/2026. 10-21. https://doi.org/10.37750/2616-6798.2026.2(57).364213

Дата надходження статті до редакції: 12.05.2026 р.
Дата прийняття статті до друку після рецензування: 19.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~