INTERNATIONAL SCIENCE SPACE

# ЦИФРОВІ ТЕХНОЛОГІЇ У ПРАВІ, МЕДИЦИНІ ТА ЕКОНОМІЦІ: РЕГУЛЯТОРНІ МОДЕЛІ ТА ПРАКТИЧНІ ВИКЛИКИ

**КОЛЕКТИВНА МОНОГРАФІЯ**

Луцьк
Вежа-Друк
2026

УДК 004:[34+61+33]](02)
Ц 72

*Рекомендовано до друку рішенням Вченої ради Державного вищого навчального закладу «Ужгородський національний університет» (Протокол № 12 від «25» вересня 2026 року).*

**Авторський колектив:**

О. В. Батанов, Л. Б. Васильчук, С. Б. Карвацька, І. С. Пирога, Ю. М. Бисага, С. С. Пирога, І. О. Щербатюк, А. М. Лисенко, А. З. Ланкевич, А. М. Галайко, О. Н. Романюк, С. В. Павлов, Л. П. Денищич, В. П. Майданюк.

**Рецензенти:**

**Дробуш І. В. –** доктор юридичних наук, професор;
**Щербанюк О. В. –** доктор юридичних наук, професор.

**Цифрові технології у праві, медицині та економіці: регуляторні моделі**
Ц 72 **та практичні виклики:** колективна монографія / за заг. ред. В. В. Берч, В. І. Продан. **–** Луцьк : Вежа-Друк, 2026. – 364 с.

ISBN 978-966-940-783-2

Колективна монографія присвячена комплексному міждисциплінарному дослідженню цифрової трансформації права, медицини та економіки, її регуляторних моделей, інституційних передумов і практичних наслідків. У виданні розкрито теоретико-методологічні та прикладні проблеми цифрового конституціоналізму, електронного правосуддя в Україні та Європейському Союзі, цифрової трансформації міжнародного права під впливом штучного інтелекту і цифрових доказів, модернізації правового регулювання податкової політики в умовах європейської інтеграції. Окрему увагу приділено цифровій трансформації обліково-аналітичних систем підприємств, проблематиці громадського здоров'я та захисту репродуктивних прав, а також клінічному застосуванню тривимірного моделювання, штучного інтелекту і цифрових двійників у медицині. Міждисциплінарний характер видання дав змогу поєднати правовий, економічний, медичний і технологічний виміри цифровізації та простежити взаємозв'язок між технологічними інноваціями, трансформацією регуляторних механізмів, ефективністю функціонування відповідних систем і необхідністю забезпечення прав та законних інтересів людини. Монографія адресована науковцям, викладачам, здобувачам вищої освіти, правникам, медичним працівникам, економістам, представникам органів публічної влади та бізнесу, а також усім, хто професійно працює з проблематикою цифрової трансформації.

**УДК 004:[34+61+33]](02)**

ISBN 978-966-940-783-2
© Берч В. В., Продан В. І. (ред), 2026

**ЗМІСТ**

**ПЕРЕДМОВА** ..... **6**

**РОЗДІЛ 1. ЦИФРОВИЙ КОНСТИТУЦІОНАЛІЗМ ЯК КОНЦЕПТ (О.В. Батанов)** ..... **11**

1.1. Теоретико-методологічні проблеми цифрового конституціоналізму ..... 11

1.2. Людський вимір цифрового конституціоналізму ..... 15

1.3. Цифровий конституціоналізм у фокусі організації та діяльності публічної влади ..... 28

**РОЗДІЛ 2. ЕЛЕКТРОННЕ ПРАВОСУДДЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: РЕГУЛЯТОРНІ МОДЕЛІ УКРАЇНИ ТА ЄВРОПЕЙСЬКОГО СОЮЗУ (Л.Б. Васильчук)** ..... **56**

2.1. Електронне правосуддя як регуляторна модель ..... 58

2.2. Українська модель електронного правосуддя: становлення та ключові виклики ..... 62

2.3. Європейська модель електронного правосуддя: наднаціональна інтероперабельність і національні практики ..... 68

2.4. Процесуальні гарантії цифрового правосуддя: доступ, ідентифікація, докази та безпека ..... 78

2.5. Напрями розвитку та критерії ефективності електронного правосуддя в Україні ..... 87

**РОЗДІЛ 3. ЦИФРОВА ТРАНСФОРМАЦІЯ МІЖНАРОДНОГО ПРАВА: ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЦИФРОВИХ ДОКАЗІВ НА СУЧАСНЕ МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ (С.Б. Карвацька)** ..... **103**

3.1. Цифровізація міжнародно-правового простору та трансформація традиційних моделей правового регулювання ..... 103

3.2. Міжнародно-правові засади регулювання штучного інтелекту ..... 112

3.3. Перспективи розвитку міжнародно-правового регулювання цифрового середовища та стратегічні орієнтири для України ..... 129

**РОЗДІЛ 4. ЦИФРОВА МОДЕРНІЗАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ ПОДАТКОВОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ (І.С. Пирога, Ю.М. Бисага, С.С. Пирога, І.О. Щербатюк)** ..... **147**

4.1. Пріоритети цифровізації податкової політики України в контексті адаптації до стандартів ЄС ..... 154

4.2. Цифрові інструменти податкової політики у забезпеченні функцій соціальної держави ..... 163

4.3. Зарубіжний досвід цифрового моніторингу та оподаткування вивозу капіталу і великих статків ..... 174

4.4. Правове регулювання рентних відносин в умовах упровадження цифрових технологій обліку природних ресурсів ..... 183

4.5. Використання цифрових платформ для узгодження законних інтересів суб'єктів податкових правовідносин ..... 193

**РОЗДІЛ 5. ЦИФРОВА ТРАНСФОРМАЦІЯ ОБЛІКОВО-АНАЛІТИЧНОЇ СИСТЕМИ ПІДПРИЄМСТВА: КОНЦЕПЦІЯ, ІНСТРУМЕНТИ ТА ОЦІНКА ЕФЕКТИВНОСТІ (А.М. Лисенко)** ..... **218**

5.1. Теоретичні засади формування обліково-аналітичної системи підприємства ..... 218

5.2. Цифрові технології та інструменти функціонування сучасної обліково-аналітичної системи ..... 223

5.3. Функціональна модель та інструментарій цифрової трансформації обліково-аналітичної системи ..... 241

5.4. Система індикаторів ефективності цифрової трансформації обліково-аналітичної системи підприємства ..... 257

**РОЗДІЛ 6. ЦИФРОВІЗАЦІЯ ДЕРЖАВНОГО УПРАВЛІННЯ ЯК МЕХАНІЗМ ЗАПОБІГАННЯ ВИДАННЮ ТА ВИКОНАННЮ ЗЛОЧИННИХ НАКАЗІВ (А.З. Ланкевич)** ..... **268**

6.1. Владний наказ у цифровому середовищі як форма публічно-владного волевиявлення ..... 268

6.2. Механізми фіксації походження, руху та зміни владного наказу .....273
6.3. Цифрові процедурні запобіжники під час формування владного наказу 277
6.4. Контрольований виняток, цифровий аудит та гарантії належного функціонування системи .....281
**РОЗДІЛ 7. ГРОМАДСЬКЕ ЗДОРОВ'Я НАЦІЇ ТА ПРОБЛЕМИ ЗАХИСТУ РЕПРОДУКТИВНИХ ПРАВ НАСЕЛЕННЯ В УКРАЇНІ (А.М. Галайко)** .....**292**
7.1. Громадське здоров'я як соціально-правова проблема сучасності.....292
7.2. Репродуктивне здоров'я української нації.....303
7.3. Питання рівного доступу у сфері репродуктивних прав людини .....306
7.4. Насильство та його вплив на репродуктивне здоров'я нації.....309
**РОЗДІЛ 8. КЛІНІЧНЕ ЗАСТОСУВАННЯ ТРИВИМІРНОГО МОДЕЛЮВАННЯ В МЕДИЦИНІ (О.Н. Романюк, С.В. Павлов, Л.П. Денищич, В.П. Майданюк)** ..... **326**
8.1. Використання тривимірного моделювання в кардіології.....327
8.2. Застосування у діагностиці онкологічних захворювань.....331
8.3. Тривимірне моделювання у травматології та ортопедії .....334
8.4. Застосування у нейрохірургії та неврології.....337
8.5. Стоматологія та щелепно-лицева хірургія.....340
8.6. Використання тривимірного моделювання для проведення віртуальних медичних операцій.....342
8.7. Перспективи використання штучного інтелекту і цифрових двійників...350
**ПІСЛЯМОВА** .....**356**

# ПЕРЕДМОВА

Цифрова трансформація упродовж останніх років набула ознак одного з визначальних чинників суспільного розвитку, позаяк істотно змінила усталені моделі правового регулювання, економічної діяльності, публічного управління, охорони здоров'я, наукової комунікації та професійної практики. Цифрові технології дедалі складніше розглядати виключно як технічний інструментарій, покликаний оптимізувати окремі процеси. Штучний інтелект, алгоритмічні системи, великі дані, хмарні технології, цифрові платформи, автоматизовані системи прийняття рішень, тривимірне моделювання, цифрові двійники, електронні інформаційні системи та інші технологічні рішення формують нове середовище суспільних відносин, у якому змінюються способи реалізації прав людини, функціонування державних і приватних інституцій, організації економічних процесів, надання медичної допомоги та прийняття професійно значущих рішень.

Саме на перетині технологічних можливостей і суспільної потреби в їх належному нормативному, етичному та інституційному впорядкуванні виникає комплекс проблем, дослідженню яких присвячена колективна монографія «Цифрові технології у праві, медицині та економіці: регуляторні моделі та практичні виклики». Її концептуальний задум ґрунтується на міждисциплінарному осмисленні цифровізації як складного процесу, наслідки якого неможливо повноцінно дослідити в межах лише однієї галузі знань. Технологічна модернізація права закономірно пов'язана з питаннями економічної ефективності, захисту даних, цифрової безпеки та людської автономії; цифровізація медицини породжує нові вимоги до правового режиму медичних даних, відповідальності, інформованої згоди та допустимих меж алгоритмічного втручання; трансформація економічних процесів потребує переосмислення інформаційної інфраструктури підприємств, управління ризиками, контролю, аудиту та механізмів прийняття рішень.

Особливе значення має нормативний вимір цифрової трансформації. Динаміка технологічного розвитку суттєво випереджає традиційні механізми

формування правових норм, що закономірно породжує регуляторні прогалини, конкуренцію юрисдикцій, проблеми визначення відповідального суб'єкта, допустимості автоматизованого прийняття рішень, використання персональних і чутливих даних, доказового значення цифрової інформації та встановлення меж втручання держави і приватних технологічних операторів у сферу особистої автономії. За цих обставин правове регулювання цифрового середовища дедалі більше тяжіє до багаторівневої моделі, в якій взаємодіють конституційні принципи, національне законодавство, міжнародні стандарти, право Європейського Союзу, акти рекомендаційного характеру, професійні стандарти, етичні норми та механізми саморегулювання.

Поряд із зазначеним, цифровізація ставить перед юридичною наукою значно складніші завдання, ніж просте нормативне супроводження технологічних інновацій, зокрема, необхідність переосмислення окремих фундаментальних категорій права в умовах, коли алгоритм здатний безпосередньо впливати на становище людини, цифрова платформа фактично виконує функції регулятора суспільної комунікації, персональні дані набувають значної економічної цінності, а технологічна інфраструктура стає необхідною умовою реалізації дедалі ширшого кола прав і свобод. У науковий дискурс входять категорії цифрових прав, цифрової ідентичності, алгоритмічної підзвітності, цифрового суверенітету, права на захист від автоматизованого рішення, цифрової інклюзії, інформаційної автономії особи, відповідального штучного інтелекту. Доктринальне опрацювання зазначених питань потребує поєднання правових аргументів із розумінням технологічної природи відповідних процесів.

Не менш глибокі зміни відбуваються у медицині. Сучасні цифрові рішення розширюють можливості діагностики, прогнозування, планування лікування та персоналізації медичної допомоги. Тривимірне моделювання, технології штучного інтелекту, автоматизована інтерпретація медичних зображень, телемедицина, цифрові двійники, роботизовані системи та персоналізована аналітика поступово інтегруються в клінічну практику.

Технологічний прогрес закономірно актуалізує питання безпеки пацієнта, клінічної валідності цифрових систем, розподілу професійної відповідальності, достовірності алгоритмічних висновків, конфіденційності медичної інформації та збереження за людиною реальної можливості контролювати рішення, що стосуються її здоров'я і фізичної недоторканності. Цифрова медицина тому потребує одночасного розвитку технологічних, клінічних, правових та етичних механізмів гарантування інтересів пацієнта.

Економічний вимір цифровізації охоплює серед іншого трансформацію управлінських моделей, обліково-аналітичних систем, механізмів контролю, фінансового планування, податкового адміністрування, аудиту та оцінювання ризиків. Сучасне підприємство дедалі більше функціонує як складна інформаційна система, де значна частина управлінських рішень залежить від якості даних, швидкості їх обробки, сумісності цифрових платформ та можливості застосування прогнозної аналітики. Запровадження ERP-систем, Business Intelligence, Big Data, хмарних технологій, автоматизованого контролю й алгоритмічних інструментів формує новий рівень інформаційного забезпечення економічної діяльності, але водночас створює ризики технологічної залежності, кібервразливості, помилкової інтерпретації даних та недостатньої прозорості автоматизованих рішень.

Важливе місце у проблематиці монографії посідає людина як центральний адресат і водночас активний учасник цифрової трансформації. Технологічний розвиток не може оцінюватися виключно крізь призму продуктивності, швидкості або економічної доцільності. Критеріями його суспільної прийнятності мають залишатися людська гідність, свобода, рівність, приватність, безпека, доступність технологій, недискримінація та можливість ефективного захисту порушених прав. Саме людиноцентричний вимір дозволяє встановити межу між інновацією, яка розширює людські можливості, та технологічним рішенням, здатним створювати нові форми залежності, нерівності або непрозорого контролю.

Структура колективної монографії відображає багатовимірність предмета дослідження. Представлені в ній наукові розвідки охоплюють доктринальні, нормативні, інституційні, економічні, медичні, технологічні та прикладні аспекти цифрової трансформації. Поряд із питаннями цифрового конституціоналізму, міжнародно-правового регулювання, цифрових доказів, застосування штучного інтелекту, громадського та репродуктивного здоров'я, тривимірного моделювання в медицині й цифровізації обліково-аналітичних процесів предметом уваги авторів є й інші напрями, об'єднані спільною проблематикою впливу сучасних технологій на людину, суспільство, державу та економіку. Розширення тематичного поля видання відповідає самій природі цифрової трансформації, яка не визнає традиційних дисциплінарних меж і постійно породжує нові об'єкти наукового осмислення.

Об'єднання у межах одного видання представників різних наукових спеціальностей дає можливість розглядати цифровізацію не фрагментарно, а через взаємозв'язок технологічних рішень, регуляторних моделей та їх практичних наслідків. Саме міждисциплінарність дозволяє виявити проблеми, які залишаються непомітними при суто галузевому аналізі: розходження між технологічною можливістю та юридичною допустимістю; між економічною ефективністю та необхідністю захисту прав людини; між клінічною користю цифрової технології та ризиком надмірної алгоритмізації медичного рішення; між прагненням до автоматизації та потребою зберегти персоніфіковану відповідальність за наслідки її використання.

Запропоновані авторами положення, узагальнення та практичні висновки не претендують на завершення наукової дискусії щодо цифрової трансформації. Навпаки, швидкість технологічних змін зумовлює відкритий характер більшості досліджуваних питань і потребу в їх постійному доктринальному переосмисленні. Значна частина сучасних регуляторних моделей перебуває у процесі становлення, а практика застосування штучного інтелекту, цифрових платформ, автоматизованих систем, медичних цифрових технологій та

інтелектуальної аналітики формує нові проблемні ситуації швидше, ніж наука і законодавець можуть запропонувати вичерпні відповіді.

Сподіваємося, що колективна монографія стане простором для подальшої фахової дискусії щодо оптимального співвідношення технологічного розвитку, нормативного регулювання та захисту людини в цифровому середовищі, а її результати становитимуть інтерес для науковців, викладачів, здобувачів освіти, правників, медичних працівників, економістів, представників органів публічної влади, бізнесу та всіх, хто професійно працює з проблематикою цифрової трансформації.

Цифрова епоха ставить перед наукою питання, які ще донедавна перебували переважно у площині технологічного прогнозування. Сьогодні вони безпосередньо визначають зміст прав людини, напрями державної політики, стандарти медичної допомоги, моделі економічного управління та межі допустимого використання технологій. Від якості наукового осмислення цих процесів значною мірою залежатиме, чи стане цифрова трансформація інструментом розширення людських можливостей і суспільного розвитку, чи джерелом нових ризиків, нерівностей та форм технологічної залежності.

*З повагою до авторів, читачів і науки, що формує майбутнє,*

*Вероніка Берч та Вікторія Продан,*

*співзасновниці International Science Space*

# РОЗДІЛ 1
# ЦИФРОВИЙ КОНСТИТУЦІОНАЛІЗМ ЯК КОНЦЕПТ

Автор: ***Батанов Олександр Васильович,*** *доктор юридичних наук, професор, заслужений діяч науки і техніки України, провідний науковий співробітник відділу конституційного та муніципального права Інституту держави і права імені В. М. Корецького НАН України*

## 1.1. Теоретико-методологічні проблеми цифрового конституціоналізму

Сучасне конституційне право зазнає суттєвих змін під впливом цифровізації, яка охоплює маже всі сфери суспільного життя. Впровадження цифрових технологій не лише трансформує зміст традиційних прав людини, а й зумовлює появу її нових – цифрових – прав, що потребують належного правового закріплення, реалізації та захисту. Водночас відсутність усталеного підходу до розуміння природи цифрових прав, наявність цифрової нерівності, складність визначення юрисдикції у цифровому просторі та зростаючі ризики порушення приватності вимагають переосмислення конституційно-правових підходів до регулювання прав людини в умовах цифрового середовища. Ці обставини актуалізують потребу в комплексному аналізі цифровізаційних процесів у сфері конституційного права та розробленні механізмів забезпечення цифрових прав в Україні.

Проблематиці цифровізації конституційного права та його інформаційного виміру в умовах глобалізації вже були присвячені деякі наші дослідження [2-4]. Також питанням цифрових прав людини, електронного урядування, інформаційної відкритості держави та трансформації механізмів реалізації і гарантування прав людини в умовах цифрової епохи, присвячено низку наукових

праць багатьох вітчизняних вчених-правознавців. Зокрема на рівні концептуального осмислення, сутність цифрового конституціоналізму, його парадигмальні засади та перспективи розвитку в Україні були розкриті у дослідженнях В. М. Бесчастного, Н. В. Бочарової, Т. А. Костецької, М. В. Костицького, та Н. В. Кушакової-Костицької та ін. [9; 26-28; 32].

Парадигмальне значення в умовах сучасних цифрових викликів має доктринальне обґрунтування Л. С. Городнюк, О. П. Дзьобань, О. Е. Радутним та іншими науковцями феномену цифрової людини [8; 15-17; 40-41; 43].

Теоретичну базу інформаційного виміру прав людини, інформаційних прав у цифрову добу, поняття цифрових прав, їх класифікації та ціннісного виміру, реалізації у глобалізаційному контексті, а також окремі аспекти цифрових прав людини, зокрема право на забуття, цифрову ідентичність тощо, викладено в працях О. О. Тихомирова, Н. В. Кушакової-Костицької, Д. М. Бєлова, Н. В. Верлос, О. В. Петришина, А. О. Сапарової, В. І. Чалчинського та ін. [6-7; 10-14; 31; 33; 38; 42; 46-47].

Також у фокусі уваги вітчизняних науковців також були загальні виклики й перспективи цифровізації публічного управління та нормативного супроводу цифрової трансформації держави [1]; електронної участі в управлінні державними справами [18], електронного урядування та демократії [19; 23; 29-30], факторів та перспектив запровадження інституту інформаційного омбудсмана [5; 21; 36; 39; 45] тощо.

Незважаючи на помітний доробок у цьому напрямі, актуальним залишається потреба комплексного теоретико-правового осмислення феномену цифрового конституціоналізму, цифровізації у площині конституційного права з урахуванням трансформації публічно-владних відносин, необхідності належного конституційного забезпечення цифрових прав людини та механізмів реалізації інформаційних функцій держави у цифрову епоху, конституціоналізації інформаційного права тощо.

Метою цього розділу монографії є аналіз концептуальних проблем формування феномену цифрового конституціоналізму, а також інших цифровізаційних аспектів сучасного конституційного права та основних викликів, що постають перед конституційно-правовим регулюванням у цифрову епоху. Адже сучасне конституційне право переживає період фундаментальних змін, зумовлених цифровою революцією та процесами глобалізації, під впливом яких розширюється конституційно-правова матерія, а об'єкти конституційно-правового регулювання ускладнюються або набувають нового змісту. Це відображає багатовекторний характер сучасних трансформацій конституційного права, серед яких цифровізація займає особливе місце. Створення різноманітних цифрових інфраструктур стало основним чинником розширення доступу громадян до глобального інформаційного середовища та знань.

Так, як констатує О. О. Тихомиров, «цифровізація людського життя набирає обертів і веде до еволюції соціуму не тільки в технологічній, а й у багатьох інших площинах – інтелектуальній, соціальній, правовій, економічній, культурній тощо. Істотність цифрової трансформації суспільства сягнула меж, коли відбувається вплив на засади правового регулювання, його пріоритети, ідеали, ключові ідеї, до яких насамперед належать права людини», система яких «певною мірою змінюється під впливом цифровізації – виникають нові права, ефективні механізми здійснення вже відомих прав, обмеження й вимоги, принципи побудови відносин. Проте ці зміни варто сприймати як органічні, як такі, що мають знайти своє невід'ємне місце в загальному дискурсі про права людини, зокрема в межах розвитку інформаційних прав – як їх сучасний прояв» [46, с. 131].

Більш того, тотальна цифровізація відкрила перед сучасною людиною безліч можливостей, створила нову систему відносин «людина-світ»: тепер будь-який аспект загальнолюдського буття неможливо уявити без залученості у цифровий вимір. Як зазначає К. С. Гончаренко «в умовах сьогодення ми повинні дивитися на людину крізь призму техногенності, урбанізації, де-ієрархізації

соціальних та культурних меж. Адже саме завдяки цим процесам відбувається формування нового уявлення про людину. Зі жвавим розвитком технологічних процесів відбулися кардинальні зміни у розумінні людини» [15, с. 137-138].

«З огляду на це, – доводить Л. С. Городнюк, – наприкінці XX ст. – на початку XXI ст. з'явилася, а в кінці першої чверті сторіччя сформувалася цифрова (дигітальна) людина, або Homo Digitalis, – принципово новий тип Homo Sapiens, який співіснує з цифровими пристроями і цифровими системами, має цифрову ідентифікацію, чия життєва творчість відбувається в декількох вимірах, в тому числі і значною мірою, у віртуальному, чиє буття суттєво або цілковито залежить від цифрового світу». На її думку, «феноменологія цифрової людини полягає, зокрема, в тому, що вона розвивається та трансформується темпорально і експоненційно, здивовуючи сама себе і ледве встигаючи фіксувати і теоретизувати власну трансформацію у всьому її розмаїтті. Практика (повсякденна цифрова діяльність мільйонів людей) випереджає теоретичні дослідження щоденними винаходами, постійними цифровими оновленнями та налаштуваннями, які відкривають нові просторові та комунікативні обрії, породжують нові форми та грані комунікації, соціальних інтересів та відносин, формуючи сучасну людину з новим світоглядом, новою епістемологічною позицією і онтологічними імперативами». Більш того, «цифрова людина значно відрізняється від попередніх поколінь Homo Sapiens – способом мислити, способом приймати рішення, способом діяти, задовільняти власні і колективні потреби, навіть способом писати, читати та рахувати тощо, і саме вона, з власними світоглядними і ціннісними орієнтирами і екзистенційним баченням майбутнього – архітектор та оператор цивілізаційних трансформацій» [16, с. 30-31].

Розглядаючи словосполучення «цифрова людина» як синонім понять «інформаційна людина» (homo informaticus) та «мережева людина», О. П. Дзьобань доводить, що «цифрова людина створює нові штучні взаємозв'язки в межах, які вона інформаційно може попередньо встановити, в

результаті чого виникають відповідні інформаційні структури». На його переконання, «формування цифрової людини – це одна з базисних характеристик інформаційного суспільства, коли кожне з діалектично взаємопов'язаних начал людини: фізичне, психічне й соціальне, вимагає спеціального урахування, оскільки лише у цьому випадку нові можливості інформаційного суспільства можуть бути повною мірою використані для розвитку цифрової людини» [17, с. 13].

«На сучасному етапі тотального упровадження цифрових технологій, – продовжує свої роздуми О. П. Дзьобань, – змінюється не тільки те що робить людина, але й те, ким вона є і в кого перевтілюється. Цифрові трансформації у соціумі здійснюють багатоплановий вплив на людину і позначаються на всіх сферах її життєдіяльності: на недоторканності особистого життя і формах власності, на зміні характеру поведінки споживачів, на кількості часу, присвячуваного роботі, відпочинку й сім'ї, на принципах розвитку кар'єри та методах удосконалення навичок. Цифрова людина може змінювати свої корпоративні зв'язки, не будучи до них жорстко прив'язаною; вона може і здатна дуже гнучко вибудовувати стосунки з іншими людьми, долучатися до різних соціальних спільнот і різних культурних традицій. Цифрова людина менше обтяжена сформованими та історично обумовленими стереотипами, вона володіє більш мобільними реакціями і здатністю маніпулювати будь-якими пластами інформації, вона набуває нової абстрактної форми свого існування. … Отже, сучасні інформаційно-технологічні процеси призводять до зміни реальності, у якій перебуває людина, здебільшого переводять їх у цифрову площину. Врешті, ця реальність стає віртуальною: образно-особистісною та метафоричною, веде людину іншим витком спіралі розвитку, одночасно повертаючи її в царину архетипів і символів (цифри)» [17, с. 13-14].

## 1.2. Людський вимір цифрового конституціоналізму

З огляду на зазначені та інші тенденції, цифровізація конституційного права проявляється в декількох ключових напрямах. Насамперед ідеться про трансформацію традиційних конституційних прав людини під впливом цифрових технологій. Сучасні цифрові інструменти змінюють не лише форми реалізації більшості суб'єктивних прав людини, а й саму природу її взаємодії з державою та публічною владою в цифровому вимірі, що потребує парадигмального оновлення усієї доктрини конституційного права відповідно до нових суспільних викликів.

Прикладом тому є, зокрема, право на участь в управлінні державними справами, яке реалізується через механізми електронної демократії, як-от електронні петиції, онлайн-голосування та платформи для громадських консультацій, що охоплюють нові форми безпосередньої демократії в цифровому форматі [18].

Без перебільшення, практична реалізація більшості громадянських, політичних, економічних і соціальних прав без доступу до сучасних інформаційно-комунікаційних технологій та їх безпосереднього використання є ускладненою, якщо взагалі можливою. Так, право на доступ до інформації тепер нерозривно пов'язане з цифровою інфраструктурою та рівнем цифрової грамотності. Право на свободу зібрань та об'єднань дедалі частіше реалізується в онлайн-просторі, який є вразливим до цензури, блокування та алгоритмічного контролю. Право на свободу вираження поглядів трансформується під впливом цифрових платформ, де модерація контенту здійснюється алгоритмами, що можуть обмежувати плюралізм думок. Право на працю та справедливі умови праці тепер значною мірою залежать від цифрової грамотності через автоматизацію та створення гіг-економіки. Право на приватність і захист персональних даних стикається з новими викликами, зокрема масовим збором даних, профілюванням, таргетуванням та автоматизованим ухваленням рішень на основі штучного інтелекту. Такі системи можуть посилювати нерівність у суспільстві та інколи навіть породжувати дискримінацію та підривати засади

«процедурної» справедливості, особливо у сфері соціального забезпечення. Запровадження автоматизованих систем ухвалення рішень щодо соціальних виплат суттєво впливає на реалізацію права на соціальне забезпечення [11, с. 19].

Право на свободу слова набуває нових форм реалізації в цифровому середовищі через соціальні мережі, блогінг та інші онлайн-платформи, які водночас породжують нові ризики – поширення дезінформації, кібербулінг тощо. Право на приватність вимагає посиленого захисту персональних даних в умовах масового збору, обробки та використання інформації технологічними компаніями. Це знаходить підтвердження, зокрема, у положеннях Загального регламенту ЄС про захист даних (GDPR) [60], а також в українському законодавстві, яке нині перебуває у процесі адаптації до європейських стандартів.

Більш того, цифровізація суспільного життя суттєво трансформує форми реалізації такого фундаментального права, як свобода думки, совісті та релігії. Як зазначає Р. В. Терлецький, «інтернет та цифрові комунікаційні технології створили новий простір для реалізації релігійних переконань, що проявляється у проведенні онлайн-богослужінь, дистанційній релігійній освіті, діяльності віртуальних релігійних спільнот та поширенні релігійної інформації через соціальні мережі. У цьому контексті цифровий простір стає важливим середовищем функціонування релігійних організацій, водночас породжуючи нові правові та філософські питання щодо: меж реалізації релігійної свободи; можливості людини отримати повноцінний релігійний досвід онлайн; впливу штучного інтелекту (ШІ) на віросповідання людини; взаємодії людини як суб’єкта правовідносин, що пройшла онлайн-релігійну трансформацію, з реальним суспільством. Філософсько-правовий аналіз цієї проблеми пов’язаний також із ширшим питанням сучасності: антропологією цифрової епохи. Адже людина дедалі більше взаємодіє зі світом через інформаційні технології, що змінює спосіб сприйняття нею реальності, комунікативний та духовний досвід. У цьому контексті цифрові інструменти мають не лише технічний характер, але

й виступають новим середовищем формування світогляду, зокрема й релігійного. Віртуальний простір стає доповненням і розширенням релігійної комунікації, створюючи нові форми духовної взаємодії у глобалізованому цифровому суспільстві» [44, с. 202].

Під впливом сучасних цифрових трансформацій виникають принципово нові права людини – цифрові права, які відображають специфіку життєдіяльності в інформаційному суспільстві. Як справедливо зазначають О. Б. Братасюк та Н. Ф. Ментух, «цифрові права людини слід розглядати як окрему групу прав людини, які пов'язані з використанням та/або реалізовуються в мережі «Інтернет» за допомогою спеціальних пристроїв» [10, с. 59]. Д. М. Бєлов, І. Є. Переш та І. Покорба, у свою чергу, підкреслюють, що «цифрові права повинні охоплювати всі права людини в умовах цифровізації та розвитку сучасних інформаційно-комунікаційних технологій» [7, с. 111].

Цю позицію поділяють також А. О. Гачкевич та В. А. Хомин, які наголошують, що «дилема щодо природи цифрових прав полягає у тому, чи вони являють собою нову категорію прав, чи є сучасною інтерпретацією добре відомих фундаментальних прав людини». Ця дилема, на їх погляд, «наштовхує на думку, що сам по собі термін «цифрові права» може вживатись в різних розуміннях, зокрема щодо усіх прав, здійснення та захист яких тісно пов'язаний сьогодні з використанням цифрових інструментів або має суттєву онлайн-складову», а також лише тих, які претендують «на статус фундаментальних в цифрову епоху». З огляду на це, на їх думку, «концептуальне наповнення поняття цифрових прав лежить в площині використання цифрових технологій в мережі Інтернеті. Їхнє призначення полягає в тому, щоб надати правову форму численним можливостям для людини, які з'явились з цифровими трансформаціями. Цифрові права одночасно є й інструментами охорони персональних даних та іншої інформації, контроль над якою прагнуть здійснювати користувачі Інтернету. Зрештою, цифрові права – це також про

доступ до цифрових технологій та підключення до Інтернету, як й видалення з нього» [14, с. 100-101].

На думку, О. О. Тихомирова, «здійснюючи наукове осмислення цифрових прав загалом як своєрідної новітньої групи прав, необхідно враховувати їх наступність щодо категорії «інформаційні права людини», тобто у незавершеному логічному ряду: права людини, інформаційні права людини, цифрові права людини. З огляду на те, що цифрові технології є віхою інформаційних технологій, цифрові права варто розглядати як компонент інформаційних прав людини». Таким чином, – вважає він, – «сьогодні до «цифрових прав людини» доцільно застосовувати широку трактовку і сприймати їх як складну еволюційно сформовану категорію в системі прав людини. Ідея «цифрових прав» охоплює особливості (умови) реалізації визнаних прав людини в цифровому середовищі (не тільки online) та за допомогою цифрових інструментів в реальному житті, нові суб'єктивні права як юридичну конкретизацію правових можливостей людини в цифровому середовищі, систему принципів і своєрідних гарантій захисту прав людини в процесі використання цифрових технологій» [46, с. 138].

Таким чином, концепція цифрових прав людини ґрунтується на усвідомленні того, що в умовах цифрової трансформації суспільства доступ до цифрової інфраструктури, інформаційно-комунікаційних технологій та мережі Інтернет перетворюється з технічної можливості на необхідну передумову ефективної реалізації конституційних прав і свобод людини. Цифровий простір стає самостійним середовищем здійснення прав людини, у межах якого традиційні права набувають нових форм реалізації, а також виникають специфічні правомочності, зумовлені особливостями цифрової взаємодії.

Свідченням тому є конституційне регулювання інформаційно-комунікативних відносин у багатьох державах у сучасному світі. Так, наприклад, ще у 2001 році Конституцію Греції [61] було доповнено окремою статтею 5А, яка не лише гарантує кожному право на інформацію, як це передбачено

законодавством, а й право на участь у житті інформаційного суспільства. Встановлюється, що сприяння доступу до інформації, що передається в електронному вигляді, а також її створенню, обміну та поширенню є обов'язком держави, за умови дотримання гарантій, передбачених цією Конституцією. По суті Греція стала однією з перших держав, яка на рівні конституції закріпила право людини бути учасником інформаційного суспільства.

Стаття 35 Конституції Португалії [51], яка називається «Використання інформаційних технологій», охоплює різні групи інформаційних та цифрових прав, закріплюючи право громадян на використання інформаційних технологій. Гарантується, що кожен громадянин має право на доступ до всіх комп'ютеризованих даних, що стосуються його особи, вимагати їх виправлення та оновлення, а також право бути поінформованим про мету, для якої вони призначені, як це передбачено законом. Передбачено, що закон визначає поняття персональних даних, а також умови, що застосовуються до їх автоматизованої обробки, об'єднання, передачі та використання, і гарантує їх захист, зокрема за допомогою незалежного адміністративного органу. Також гарантується, що інформаційні технології не можуть використовуватися для обробки даних, що стосуються ідеологічних або політичних переконань, партійної чи профспілкової приналежності, релігійних переконань, приватного життя або етнічного походження, за винятком випадків, коли на це надано явну згоду суб'єкта даних або отримано дозвіл, передбачений законом, із гарантіями відсутності дискримінації, або з метою обробки статистичних даних, які не дозволяють ідентифікувати окремих осіб.

Установлюється, що кожному гарантується вільний доступ до інформаційних мереж загального користування. Закон визначає режим, що регулює транскордонні потоки даних, та відповідні засоби захисту як персональних даних, так і інших даних, захист яких виправданий національними інтересами.

Також цією статтею Конституції Португалії встановлено низку заборон інформаційній сфері. Зокрема, заборонено доступ третіх осіб до персональних даних, за винятком виняткових випадків, передбачених законом, а також присвоєння єдиного національного номера будь-якому громадянину.

У редакції 2013 року в Конституції Мексики [49] також з'явилося закріплення права на доступ до інформаційно-комунікаційних технологій в цілому та мережі інтернет зокрема (стаття 6). При цьому інформаційні права розглядаються як через призму захисту персональних даних, подібно підходу Португалії, так і через призму гарантування доступу індивідів до публічної інформації, а також універсальної цифрової інклюзії. Зокрема встановлюється, що кожний має право на вільний доступ до різноманітної та актуальної інформації, а також на пошук, отримання та поширення інформації та ідей будь-якого характеру за допомогою будь-яких засобів вираження. Держава гарантує право на доступ до інформаційно-комунікаційних технологій, а також до послуг радіомовлення та телекомунікацій, включаючи широкосмуговий доступ та Інтернет. З цією метою держава створить умови для ефективної конкуренції у сфері надання зазначених послуг.

У цій ж статті Конституції Мексики гарантуються права у сфері радіомовлення та телекомунікацій. Установлюється, що держава гарантує населенню інтеграцію в суспільство інформації та знань шляхом реалізації політики загальної цифрової інклюзії з річними та шестирічними цілями. З огляду на те, що телекомунікації є послугами загального інтересу, держава гарантує, що вони надаватимуться в умовах конкуренції, якості, плюралізму, універсального покриття, взаємоз'єднання, конвергенції, безперервності, вільного доступу та без свавільного втручання.

Ця ж стаття Конституції Мексики містить безпосередню вказівку на створення автономного органу гарантування та моніторингу додержання відповідного права, який зобов'язаний діяти відповідно до закону про прозорість та доступ до публічної інформації, а також про захист персональних даних, що

перебувають у володінні суб'єктів, на які поширюються відповідні зобов'язання, на умовах, встановлених загальним законом, прийнятим Конгресом Союзу з метою визначення основ, загальних принципів та процедур реалізації цього права. У своїй діяльності цей орган повинен керуватися принципами визначеності, законності, незалежності, неупередженості, ефективності, об'єктивності, професіоналізму, прозорості та максимальної відкритості.

Конституція Еквадору [52] містить окремий структурний підрозділ «Інформація та комунікація» (ст. ст. 16-20). Передбачається, що усі особи, як індивідуально, так і колективно, мають право на: 1) вільну, міжкультурну, інклюзивну, різноманітну та партисипативну комунікацію в усіх сферах соціального взаємодії, будь-якими засобами та у будь-якій формі, власною мовою та з використанням власних символів; 2) універсальний доступ до інформаційно-комунікаційних технологій; 3) створення засобів масової інформації та доступ, на рівних умовах, до використання частот радіоспектру для управління державними, приватними та громадськими радіо- та телевізійними станціями, а також до вільних діапазонів для використання бездротових мереж; 4) доступ та використання всіх форм візуальної, аудіальної, сенсорної та іншої комунікації, що забезпечують інклюзію осіб з інвалідністю; 5) брати участь у передбачених Конституцією формах громадської участі у сфері комунікації

У 2023 році Конституція Перу [50] були доповнена статтею 14-А, якою було закріплено державне гарантування права на доступ до безкоштовного інтернету на всій території країни, забезпечене державними або приватними інвестиціями. З огляду на це, Республіка Перу, виокремлюючи право на доступ до інтернету на рівні Основного Закону, просунулася далі за інших в питанні реального забезпечення доступу до мережі як невід'ємного і безумовного права її громадян.

Попри те, що безпосереднє конституційне закріплення цифрових прав, їх видів та гарантій лише нещодавно почало з'являтися у сучасному конституційному праві, свідченням чому є наведений досвід відповідних держав, де конституційні норми безпосередньо стосуються захисту персональних даних,

доступу до Інтернету, участі в інформаційному суспільстві та використання цифрових технологій тощо. Водночас у більшості демократичних держав цифрові права формуються шляхом еволюційного тлумачення класичних конституційних прав і свобод судами або деталізуються у спеціальному законодавстві, а не через внесення змін до тексту конституції. З огляду на це, доцільно говорити не лише про «цифрові права», а й про ширший процес цифрової конституціоналізації, який охоплює як конституційні тексти, конституційну юриспруденцію та профільне законодавство, так і міжнародно-правове регулювання.

У цьому контексті визнання Організацією Об'єднаних Націй значущості вільного, відкритого та недискримінаційного доступу до мережі Інтернет як фундаментальної умови здійснення прав людини відображає формування сучасної парадигми цифрових прав, загальноєвропейський рівень визнання та гарантування яких, зокрема, посилився та вийшов на новий рівень свого існування у вигляді цілісної тенденції цифровізації права в цілому та конституційного права, зокрема, у зв'язку з прийняттям Португальської хартії прав людини в цифрову епоху [48] від 17 травня 2021 року та Лісабонської декларації – цифрова демократія з метою [59] від 1 червня 2021 року, якою по суті визначалась нова парадигма цифрового переходу в ЄС та проголошувалось застосування «європейського способу ведення бізнесу» як всесвітньо визнаної ціннісної пропозиції та унікальної конкурентної переваги, яка підвищує стандарти завдяки «збалансуванню технологічного розвитку з повагою до етичних принципів і заохоченням прав людини» тощо.

Такий підхід ґрунтується на розумінні Інтернету не лише як технологічної платформи комунікації, а як універсального середовища реалізації свободи вираження поглядів, доступу до інформації, освіти, участі в демократичних процесах, здійснення економічної діяльності та інших конституційно гарантованих прав. Відтак право на доступ до Інтернету набуває інтегративного характеру, оскільки забезпечує практичну можливість реалізації широкого

спектра інших прав і свобод людини в умовах цифрового суспільства. Наведені аспекти важливі та збігаються з первинними орієнтирами

Отож до основних цифрових прав людини можемо віднести наступні: право на доступ до Інтернету, яке забезпечує можливість користування глобальною мережею; право на цифрову грамотність, що включає можливість отримання навичок роботи з цифровими технологіями; право на захист персональних даних у цифровому середовищі; право на цифрову приватність; право бути забутим, тобто право вимагати видалення інформації про себе з мережі «Інтернет»; право на цифрову безпеку; право на рівний доступ до цифрових технологій тощо.

Особливої уваги заслуговує право на доступ до Інтернету, яке в умовах пандемії COVID-19 набуло критичного значення. Дослідники констатують, що «пандемія COVID-19 загострила проблему права на доступ до Інтернету, оскільки він залишився фактично єдиним каналом для отримання інформації зі всього світу, а також обмеження чи неможливість реалізації даного права великою мірою впливає на реалізацію інших конституційних прав, таких як право на освіту, право на участь в управлінні державними справами тощо» [10, с. 58].

«Право на доступ до Інтернету, – вважають Н. Лесько та М. Антонов, – не має на меті лише фізичну можливість доступу до мережі Інтернет. Воно базується на комунікаційній цінності Інтернету, що передбачає зв’язок цього права з іншими правами і свободами людини та необхідність доступу до Інтернету для їх реалізації, зокрема, свободи думки, вираження поглядів та переконань, права на розвиток, політичних прав, екологічних та інших основних прав людини» [33, с. 160].

«Цифрова ідентичність, – зазначає Н. В. Гавриленко, – нині здійснює неабиякий вплив на життя людини», яка, набуваючи особливого значення у контексті взаємодії особи з електронними системами державного управління та цифровими сервісами, порушує серйозні проблеми у «сфері права, державного управління, фінансів, економіки, освіти, технологій» та постає «доволі

масштабним поняттям, яке включає і конфіденційну, і особисту інформацію, і персональні дані та дані про нашу взаємодію з онлайн-середовищем». На думку цього автора, «формування цифрової ідентичності – це питання особистої, суспільної і національної безпеки. Як раніше ми вчилися читати і писати, так само зараз ми повинні вчитися формувати свою цифрову ідентичність» [13, с. 162, 163, 165].

Окремо в науковій літературі звертається увага на право бути забутим, поняття якого «виникло в контексті зростаючого цифрового сліду, який кожен залишає в інтернеті. З появою соціальних мереж та пошукових систем, особиста інформація стала легко доступною для широкої аудиторії. Розвиток цієї концепції пов'язаний із захистом приватності та підвищенням контролю громадян над своєю особистою інформацією». Розвиток «права на забуття», зазначають вітчизняні вчені-конституціоналісти, що «тісно пов'язаний із зростанням технологій та розширенням цифрового простору. Визначення меж цього права вимагає не тільки юридичної уваги, але і практичних та етичних рішень у цифровому віці», стаючи «ключовим елементом захисту особистої приватності в цифровій епосі» [6, с. 58, 61].

Це право набуває особливої актуальності у зв'язку з розширенням обсягів обробки персональних даних у цифровому середовищі, що часто призводить до порушення приватності особи та тривалого збереження інформації, яка може завдати шкоди репутації або порушити право на недоторканність особистого життя. Визнання цього права, зокрема в практиці Суду Європейського Союзу (справа Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, де рішення Суду Європейського Союзу чітко фіксує, що пошукові системи, такі як Google, відповідають за обробку персональних даних і повинні враховувати запити на видалення посилань, якщо вони є «недоречними, неактуальними або надмірними» [53]), слугує підтвердженням його правового значення як інструменту забезпечення контролю особи над своїм цифровим образом.

Таким чином систему цифрових прав людини можна класифікувати за декількома критеріями. За сферою реалізації – права, що реалізуються винятково в цифровому середовищі (право на цифрову ідентичність, право на забуття), та права, що мають як традиційну, так і цифрову форму реалізації (свобода слова, право на приватність). За характером захисту – індивідуальні та колективні цифрові права. За ступенем новизни – традиційні права в цифровій формі та принципово нові цифрові права тощо.

Слід відзначити, що конституційне закріплення цифрових прав людини може здійснюватися двома основними способами: через «конституалізацію цифрових прав» (пряме закріплення в конституції нових цифрових прав) та «цифровізацію конституційних прав» (адаптація традиційних конституційних прав до цифрового середовища). Досвід окремих європейських держав показує, що існування цифрових прав людини є вже фактом, який підтверджується на законодавчому рівні. Так, наприклад, Органічний закон Іспанії 3/2018 про захист персональних даних і гарантії цифрових прав від 5 грудня 2018 р. [58] закріпив цілий комплекс цифрових прав.

В Україні процес конституціоналізації цифрових прав перебуває на початковій стадії. І хоча ст. 34 Конституції України закріплює право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань, а також право вільно збирати, зберігати, використовувати і поширювати інформацію, а ці положення створюють конституційну основу для реалізації цифрових прав, вони потребують подальшого розвитку через спеціальне законодавство та можливі конституційні зміни.

Як зазначає О. О. Тихомиров, «ідея цифрових прав тільки наповнюється юридичним змістом. Вона має гнучко реагувати на проблеми у сфері прав людини, що виникають у зв’язку з інтеграцією інформаційних технологій в соціальне життя». З огляду на це, каталог цих прав є «відкритим і дискусійним, його наперед не можна сприймати категорично. Перспективи подальшого визнання та юридичної конкретизації цифрових прав на тлі тих впливів, які

створюють цифрові технології, видаються очевидними, і сьогодні як предмет дискусії вже висуваються нові варіанти суб'єктивних «цифрових прав», наприклад: право бути offline, право не знати, право почати з чистого (цифрового) аркуша, право на термін дії даних, право знати цінність своїх даних тощо. Проте й не варто забувати, що цифрова трансформація лише еволюційний етап, його часові рамки не безмежні і в перспективі відбуватимуться соціальні зміни, зокрема зумовлені технологічним розвитком, що імовірно створять потреби в інших новітніх підходів до прав людини» [46, с. 141-142].

Зокрема, важливим аспектом розвитку цифрових прав в Україні є їх захист та забезпечення. У цьому контексті актуалізується питання запровадження інституту спеціалізованого інформаційного омбудсмана [5; 21; 36; 39; 45]. Зарубіжний досвід, зокрема країн Балтії, демонструє ефективність таких інституцій у сфері цифрового захисту. Так, естонський Data Protection Inspectorate (AKI) виконує функції контролю за дотриманням прав громадян у цифровому просторі, включно з можливістю винесення обов'язкових приписів, накладення штрафів та ініціювання кримінальних справ у випадку порушень. Завдяки цій моделі в 2013 році оброблено понад 1 300 звернень і близько 550 скарг щодо порушення приватності або неправомірного використання інформації, що підтверджує дієвість інституту як механізму контролю цифрових прав [57].

Схожі тенденції спостерігаються у Великобританії, де Information Commissioner's Office (ICO) активно залучається до захисту цифрових прав: у 2018 р. ICO надало понад 470 000 консультацій і опрацювало близько 41 600 скарг щодо порушень GDPR – що ілюструє роль омбудсмана як ключового носія захисту цифрових прав [56]. Тобто саме наявність незалежного цифрового омбудсмана сприяє ефективному захисту цифрових прав громадян, забезпечуючи оперативне реагування та моніторинг інформаційної політики держави в цифровому просторі.

В умовах наявних в Україні системних викликів, насамперед, таких як недостатня прозорість обробки персональних даних та ризики цифрової дискримінації, ідея створення інституту інформаційного омбудсмана виявляється дуже перспективною. Вона могла б забезпечити незалежний моніторинг, оперативне реагування на порушення та підвищення цифрової відповідальності як серед державних органів, так і серед приватного сектору.

### 1.3. Цифровий конституціоналізм у фокусі організації та діяльності публічної влади

Важливим аспектом осмислення феномену цифрового конституціоналізму є його зв'язок із проблемами організації публічної влади (безпосередньої демократії, державної влади та місцевого самоврядування) та в цілому взаємодії суспільства та держави. Електронне урядування стає новою формою здійснення публічної влади, що забезпечує більшу ефективність, прозорість та підзвітність органів влади. За визначенням Концепції розвитку електронного урядування в Україні, електронне урядування є формою організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій [24].

З огляду на це, О. Ю. Кудрявцев зазначає, що «інформаційно-телекомунікаційні технології стали невід'ємним елементом сучасності, від яких залежить не тільки розвиток науки і техніки, але й громадянського суспільства. Але однією з необхідних передумов сталого розвитку суспільства є можливість конструктивного діалогу між владою та громадянами, з залученням останніх до процесів вироблення та прийняття загальнозначущих рішень». На його переконання, «такий діалог та конструктивна співпраця є запорукою здійснення ефективної політики, яка спроможна забезпечити реальний громадянський контроль, гарантувати права індивіда, зміцнюючи довіру громадян до інститутів політичної влади». Також він вказує, що «поставленої мети, зокрема, можна досягти завдяки впровадженню системи електронного урядування, яка здатна

забезпечити новий рівень комунікації між громадянами та владою, безперешкодний доступ до публічної інформації. Означені процеси потенційно сприятимуть участі індивідів у виробленні та впровадженні державної політики, що виведе державні послуги на якісно новий рівень» [29, с. 5-6].

Визначаючи цифровізацію як «ефективну сучасну динамічну форму взаємодії політичних суб'єктів – суспільства і держави для досягнення цілей і утвердження цінностей демократії та прав людини», О. В. Марко доводить, що «вона проявляється у впровадженні сучасних комунікаційних технологій для обміну, збору та аналізу інформації, уможливлює інтегральну взаємодію між громадянами та органами публічної влади, дієву політичну участь, прозорість діяльності суб'єктів і доступність до послуг і сервісів». На його думку, «цифровізація взаємовідносин між суспільством і державою є результатом технологічного детермінізму та логіки еволюції демократії. Технологічні інновації сприяли зменшенню відстаней, насамперед у просторовому вимірі, та посиленню контролю над громадянами. … Попри кризу, в якій опинилися демократичні режими на початку XXI ст., цифровізація сприяє появі цифрової демократії, позбавленої низки недоліків традиційних форм і з перспективами ефективнішої взаємодії між суспільством і державою. Пропонована нею децентралізована і безпосередня система взаємодії може радикально трансформувати національну та глобальну політику» [35, с. 2].

О. В. Марком виділено та проаналізовано такі види цифрової демократії (технологічно зумовлені форми демократії) як: деліберативна демократія, плинна демократія та концепція п'ятої влади. Так, на його думку, «деліберативна демократія передбачає трансформацію парламенту в деліберативну асамблею, широке залучення громадян та організацій громадянського суспільства до формування державної політики, розвиток неформалізованих форм суспільних дискусій. Плинна демократія передбачає, що громадянин може як особисто брати участь у процесах прийняття рішень, так і делеґувати свій голос іншому представникові, якого вважає більш компетентним у певних питаннях або

спроможним відстояти свої погляди. Концепція п'ятої влади наголошує на зростанні підзвітності органів публічної влади, приватних підприємств завдяки координації зусиль громадян через комунікаційні можливості, які надає Інтернет» [35, с. 4-5].

Таким чином, з огляду на сучасні трансформації суспільного розвитку, доцільно говорити про формування цифрово-інформаційної парадигми конституційного права, основні детермінанти якої слід розглядати як багаторівневу систему взаємопов'язаних чинників, що визначають не лише адаптацію держави до цифрової реальності, а й переосмислюють природу конституційного права як механізму організації інформаційного простору, регулювання цифрових відносин, захисту інформаційної автономії особи та забезпечення легітимності цифрового публічного управління.

У цьому контексті сучасний конституціоналізм постає як цифрово-інформаційна модель організації публічної влади, у межах якої держава виступає не лише носієм суверенної влади, а й ключовим суб'єктом формування цифрового середовища, гарантом інформаційних, та їх нового покоління – цифрових, прав людини, регулятором обігу даних та інституційним координатором цифрової взаємодії суспільства, бізнесу і публічної адміністрації.

На наш погляд, можна виділити такі ключові детермінанти цифрово-інформаційної парадигми конституціоналізму та інформаційної функції сучасної держави.

Філософсько-аксіологічні детермінанти (цифровий гуманізм та інформаційна автономія людини) визначають ціннісну основу інформаційної функції конституційної держави. У межах сучасного конституціоналізму відбувається перехід від традиційної моделі «держави як адміністратора інформації» до моделі «цифрової держави для людини», у якій інформаційні ресурси, цифрові технології та дані розглядаються передусім як інструменти реалізації людської гідності, свободи, приватності та самореалізації. Центральним стає принцип людиноцентричності цифрової трансформації,

відповідно до якого технологічний розвиток має бути підпорядкований правам людини.

Нормативно-правові детермінанти (конституціоналізація цифрового простору) забезпечують правове оформлення інформаційної функції держави через закріплення цифрових прав людини, принципів доступу до інформації, захисту персональних даних, інформаційної безпеки, відкритості державних даних та меж використання цифрових технологій органами влади. У межах цифрового конституціоналізму право постає як система «правил цифрового порядку», яка одночасно обмежує державне втручання в інформаційну сферу та легітимує використання цифрових інструментів для реалізації публічних функцій.

Історичні детермінанти (еволюція інформаційної ролі держави) відображають перехід від паперово-бюрократичної моделі публічної адміністрації до цифрової держави, від централізованого володіння інформацією до мережевих моделей її створення, обробки та використання. Ця трансформація формує нове розуміння держави як оператора цифрових інфраструктур, гаранта інформаційної сумісності та координатора цифрової взаємодії.

Політичні детермінанти (демократизація інформаційної влади) передбачають вплив цифрових технологій на механізми здійснення безпосередньої демократії, політичної участі та публічного контролю. Електронна демократія, цифрові форми участі громадян, відкриті дані та прозорість алгоритмічного управління формують модель цифрової демократії, у якій інформація стає ключовим ресурсом легітимації публічної влади.

Інформаційно-технологічні детермінанти (цифрова інфраструктура та управління даними) є базовими для розкриття змісту інформаційної функції держави. Вони охоплюють розвиток цифрової інфраструктури, електронного урядування, державних інформаційних систем, технологій штучного інтелекту, механізмів управління великими даними та забезпечення технологічної

сумісності публічних сервісів. У цьому контексті держава виступає не лише регулятором інформаційних процесів, а й архітектором цифрового середовища.

Культурно-ціннісні детермінанти (інформаційна культура суспільства) визначають рівень цифрової грамотності, довіри до цифрових сервісів, здатність громадян відповідально використовувати інформацію та брати участь у цифрових процесах. Формується культура інформаційної та цифрової відповідальності, що включає критичне сприйняття інформації, повагу до приватності, етичне використання цифрових технологій та усвідомлення значення даних як суспільного ресурсу.

Екологічні та технологічні детермінанти (сталий цифровий розвиток) передбачають врахування довгострокових наслідків цифровізації, зокрема енергетичної ефективності цифрової інфраструктури, скорочення цифрової нерівності, доступності технологій та екологічної відповідальності цифрового сектору. У цьому контексті формується концепція сталого цифрового конституціоналізму.

Європейсько-інтеграційні та глобалізаційні детермінанти зумовлюють включення держави у глобальний інформаційний простір, імплементацію міжнародних стандартів цифрових прав, захисту персональних даних, кібербезпеки та відповідального використання штучного інтелекту. Це трансформує інформаційну функцію держави у напрямі відкритості, сумісності та глобальної цифрової взаємодії.

Безпекові та посткризові детермінанти (інформаційна та кібербезпека) визначають нову роль держави в умовах цифрових загроз, інформаційних атак, кіберконфліктів та кризових ситуацій. Держава постає як гарант інформаційного суверенітету, захисник критичної цифрової інфраструктури та суб’єкт забезпечення стійкості інформаційного простору. Як зазначає Ю. В. Завгородня, «сутність управлінської діяльності держави у сфері кібернетичної безпеки полягає у формуванні якісної політики щодо використання досягнень інформаційно-технологічного характеру населенням, органами управління чи

промисловим сектором; визначає необхідність передбачати негативні наслідки використання окремих кібернетичних можливостей суспільством та мінімізувати ризики їх настання. Вказані цілі державної діяльності повинні досягатися прийняттям і впровадженням комплексу нормативно-правових актів міжнародного, державного та локального характеру, спрямованих на врегулювання відносин у кібернетичному просторі, а також контролем та оцінкою виконання таких актів. Даний аспект має бути невід'ємною частиною інформаційної політики, політики інформаційної безпеки держав» [20, с. 26].

Також Ю. В. Завгородня зазначає, що «цифровізація суспільної діяльності стала необхідністю в умовах глобальних катаклізмів, які переживає людство, наприклад, у формі пандемій – небезпечних захворювань, що потребують адаптивного процесу та дій превентивного характеру, як це відбувалося, наприклад, щодо вирішення проблем, пов'язаних із Covid-19. Кіберпростір став як полем оперативного позитивного реагування та інформування щодо вирішення складних проблем, так і можливістю дискредитації політики у сфері охорони здоров'я. А нині українське суспільство в умовах повномасштабної війни стикається з використанням комплексу заходів військових, економічних, політичних тощо, що включають і кіберборотьбу, яка вийшла за межі територіального протиборства сторін і має характер когнітивної війни із залученням кібермеханізмів» [20, с. 27].

У сукупності зазначені детермінанти формують цифрово-інформаційну парадигму конституційного права, у межах якої, по-перше, інформаційні процеси підпорядковуються цілям забезпечення прав людини, демократичного контролю та суспільної довіри; по-друге, право виступає інструментом організації цифрового простору, а цифрові технології – фактором трансформації правової системи; по-третє, інформаційна функція держави стає одним із центральних елементів сучасного конституційного порядку.

Ключовою категорією цієї парадигми виступає публічний інформаційний інтерес, який відображає суспільну потребу у доступності, достовірності, безпеці

та належному використанні інформації. Реалізація інформаційної функції сучасної держави відбувається через балансування інтересів: індивідуальних (право на приватність, інформацію, цифрову автономію), колективних (потреба суспільства у відкритому інформаційному середовищі) та публічних (інтерес держави у забезпеченні інформаційного порядку і цифрової безпеки).

Саме така модель перетворює інформаційну функцію держави на системоутворюючий механізм узгодження цифрової свободи, інформаційної безпеки, технологічного розвитку та демократичної легітимності влади.

Особливо важливим аспектом цифровізації конституційного права є формування інформаційної функції держави, адже сучасне суспільство, де основним предметом праці більшої частини людей є інформація та знання, а знаряддям праці – інформаційні технології, з повною впевненістю можна називати інформаційним.

Так, аналіз існуючих загальнотеоретичних підходів дає підстави Т. А. Костецькій підґрунтя для виділення основних ознак інформаційної функції держави, притаманних державним функціям: набуття рис стійкого, постійного напряму та виду діяльності держави, що має власну періодизацію існування; прояв через відповідну функцію сутності і соціального призначення держави, обумовлених завданнями, які виникають перед нею на відповідному етапі розвитку; серед основних завдань, які є першоосновою інформаційної функції: створення правових, організаційних, науково-технічних, економічних, фінансових та інших умов для реалізації інформаційних прав людини і громадянина, інформаційних потреб суспільства; формування системи національних інформаційних ресурсів; забезпечення національної інформаційної безпеки і в перспективі побудова інформаційного суспільства; реальність функції, оскільки завдання, напрями діяльності держави базуються на конституційно-правових засадах; комплексний характер функції, здійснення в певних формах і конкретними методами тощо [25, с. 119].

О. П. Климентьєв, обґрунтовуючи «необхідність законодавчого визначення інформаційної функції як основної конституційно визначеної функції держави», визначає її як «самостійний і пріоритетний напрям державної інформаційної політики, котрий здійснюється за допомогою інформаційних засобів для досягнення інформаційного суверенітету, вільного та безпечного інформаційного розвитку інформаційного суспільства в рамках конкретної держави, в тому числі для захисту інформаційних прав, свобод і законних інтересів людини і громадянина, і водночас виступає інформаційною формою досягнення цілей суспільства і держави, в інших найбільш важливих сферах життєдіяльності суспільства» [22, с. 4].

Ж. О. Павленко зазначає, що інформаційна функція держави «має всі істотні ознаки основних функцій держави, що виділяються в науці» та «являє собою сформований на сучасному етапі розвитку основний напрямок діяльності держави в інформаційній сфері, важливість правового регулювання якої зумовлена об'єктивними процесами глобальної інформатизації. Вона безпосередньо виражає і предметно конкретизує сутність сучасної держави – досягнення демократичного громадянського суспільства у глобальному інформаційному просторі» [37, с. 210].

Інший вітчизняний вчений-правознавець О. М. Лощихін вказує, що «курс на формування так званої сервісної держави, що має швидко та якісно надавати громадянам і організаціям публічні послуги, вимагає налагодження взаємодії публічно-владних структур із громадянами та організаціями, тобто комунікації, взаємного обміну інформацією, що сьогодні має нерівноправний, далеко не партнерський і зовсім нерівний характер, як того вимагають принципи розвитку демократичної, соціально-правової держави та громадянського суспільства». При цьому він виділяє комунікативну функцію держави, яка, на його думку, «має свій зміст, способи і структури, своє забезпечення. Специфіка цієї функції полягає у способах її впливу на суспільство: цілеспрямована інформованість населення, а часом маніпулювання суспільною свідомістю, інші способи

передачі інформації створюють необхідні умови для існування та функціонування інших галузей влади, усієї держави» [34, с. 266].

З огляду на це, він робить висновок, що «комунікативна функція держави – це один з кардинальних напрямків і видів діяльності держави щодо інформаційного забезпечення її діяльності в цілому, її органів, установ, посадових осіб та інформаційного обслуговування громадян. Оскільки специфіка інформації як ресурсу впливає на розосереджуваність елементів комунікативної функції й поєднання з іншими напрямками і видами державної діяльності, то ця функція є похідною від функції держави щодо захисту прав і свобод людини, а також політичної, економічної, соціальної та інших об'єктних функцій держави, тому що здійснення будь-якої з них не можливе без інформаційного компонента» [34, с. 267].

На наш погляд, попри певну відмінність теоретичних підходів, застосування функціонального підходу до дослідження діяльності держави в умовах формування та розвитку цифрового конституціоналізму дає змогу розкрити інформаційну функцію держави як самостійний напрям і вид державної діяльності, пов'язаний із формуванням, збиранням, обробленням, поширенням, захистом та використанням інформації у процесі здійснення публічної влади. Його застосування у поєднанні з концепціями цифрового конституціоналізму та цифрового права дозволяє відійти від традиційного розуміння інформаційної діяльності держави як сукупності адміністративно-технічних процедур і розглядати її як фундаментальний механізм організації сучасного конституційного порядку.

На парадигмальному рівні сучасне осмислення інформаційної функції держави пов'язане із трансформацією класичної державоцентричної моделі управління інформаційними потоками. Якщо в умовах індустріального суспільства держава переважно виступала монополістичним виробником, регулятором та розпорядником суспільно значущої інформації, то у цифрову епоху вона функціонує у складному середовищі взаємодії з громадянами,

цифровими платформами, приватними технологічними суб'єктами, інститутами громадянського суспільства та мережевими спільнотами. Це зумовлює перехід від моделі одностороннього інформаційного контролю до моделі відкритого, децентралізованого та сервісно орієнтованого управління інформаційними ресурсами.

У цьому контексті інформаційна функція держави набуває комплексного характеру. З одного боку, вона пов'язана із забезпеченням інформаційної безпеки, формуванням правових режимів обігу інформації, гарантуванням достовірності суспільно значущих даних, захистом персональної інформації та забезпеченням стійкості цифрової інфраструктури. З іншого боку, вона реалізується через створення умов для вільного доступу до інформації, розвитку цифрової демократії, електронної участі громадян, інноваційної діяльності та використання цифрових технологій як інструментів реалізації прав людини.

Важливим методологічним орієнтиром у дослідженні інформаційної функції держави є феномен цифрової свободи. У сучасному конституціоналізмі вона розглядається не лише як свобода від необґрунтованого втручання держави у сферу інформаційних відносин, а як гарантований конституцією простір доступу, створення, поширення та використання інформації за допомогою цифрових технологій. У цьому сенсі інформаційна функція держави має оцінюватися через її здатність забезпечувати та розширювати цифрові можливості особи, а не через надмірний контроль інформаційних процесів або концентрацію цифрових ресурсів у руках публічної влади.

З огляду на це, інформаційна функція держави постає як інструмент реалізації цифрових прав людини, що перебуває у функціональному зв'язку з принципами верховенства права, прозорості, відкритості влади, пропорційності, інформаційної безпеки, захисту приватності та недискримінаційного доступу до цифрового середовища. Її легітимність визначається не лише відповідністю формальним правовим вимогам, а й фактичним впливом на здатність людини

брати участь у цифровому суспільстві, отримувати публічні послуги та реалізовувати свої конституційні права.

Слід враховувати, що в умовах воєнних викликів та повоєнної цифрової трансформації інформаційна свобода набуває модифікованого змісту. Зберігаючи свою фундаментальну природу як складову людської автономії та демократичного порядку, вона водночас адаптується до потреб національної безпеки, кіберзахисту та стійкості державних інформаційних систем. У таких умовах інформаційна функція держави виходить за межі простого забезпечення доступу до інформації та трансформується у комплекс гарантій цифрової стійкості суспільства, захисту інформаційного суверенітету та забезпечення безперервності публічного управління.

У межах цифрового конституціоналізму особливого значення набуває інституційно-конституційний підхід, відповідно до якого інформаційна функція держави розглядається як елемент системи цифрових правил організації суспільства. Ці правила визначають межі втручання держави в інформаційні процеси, принципи функціонування цифрової інфраструктури, порядок використання даних, стандарти електронного врядування та гарантії цифрових прав людини.

Функціональний підхід у цьому контексті дозволяє розглядати цифрові права як внутрішній критерій здійснення інформаційної функції держави. Державна інформаційна діяльність набуває конституційної легітимності настільки, наскільки вона сприяє розвитку цифрового суспільства, забезпечує баланс між публічними інтересами та автономією особи, гарантує безпечне використання технологій і не створює необґрунтованих обмежень інформаційної свободи.

У феноменологічному вимірі інформаційна функція держави проявляється через конкретні цифрові політики, практики електронного врядування, механізми управління даними, функціонування державних інформаційних систем, цифрову ідентифікацію, електронні послуги та інструменти цифрової

демократії. Її реалізація залежить від рівня цифрової зрілості держави, інституційної спроможності публічної влади, якості правового регулювання інформаційних процесів та рівня довіри суспільства до цифрових механізмів управління.

Системно-структурний підхід дозволяє розглядати інформаційну функцію держави у нерозривному зв'язку з іншими її функціями – політичною, економічною, соціальною, безпековою, правозахисною, організаційною тощо. У цьому сенсі вона виступає інтегруючим елементом сучасного механізму публічного владарювання, оскільки саме інформаційні процеси забезпечують функціонування державних інституцій, комунікацію влади і суспільства та реалізацію конституційних прав.

Аксіологічний підхід акцентує увагу на ціннісному змісті інформаційної функції держави. Вона має оцінюватися через відповідність базовим конституційним цінностям – людській гідності, свободі, демократії, приватності, справедливості, відкритості та відповідальності публічної влади. Це унеможливлює її редукцію до технічного адміністрування інформаційних ресурсів, оскільки цифрове середовище стає простором реалізації фундаментальних прав і свобод.

У феноменологічному аспекті інформаційна функція держави постає як динамічний процес взаємодії правових норм, цифрових технологій, інформаційних потоків та управлінських практик. Вона має гібридний характер, поєднуючи елементи публічно-владного регулювання, технологічного розвитку та горизонтальної взаємодії держави з громадянами і приватними цифровими суб'єктами.

З огляду на це, можна сформулювати ключовий методологічний висновок: у парадигмі цифрового конституціоналізму інформаційна функція держави є багатовимірним конституційно-правовим феноменом, який, по-перше, інтегрує публічну владу, цифрові технології та права людини, та, по-друге, відображає трансформацію державності в умовах інформаційного суспільства. Її

дослідження потребує поєднання функціонального, інституційного, аксіологічного, системного та феноменологічного підходів, що дозволяє розкрити її не лише як напрям державного управління інформацією, а як основу сучасного цифрового конституційного порядку.

У праксеологічному вимірі відповідні парадигмальні підходи знаходять своє відображення у конституційному закріпленні цифрових прав, принципів відкритості держави, гарантій доступу до інформації, правового режиму даних, механізмів електронної демократії та організаційно-правових засад цифрової трансформації публічної влади.

Водночас процес цифровізації конституційного права супроводжується низкою правових викликів, які потребують комплексного вирішення з боку законодавця, правозастосовних органів та наукової спільноти. Ці виклики стосуються як теоретичних аспектів розуміння природи цифрових прав та їх місця в системі конституційного права, так і практичних питань їх реалізації та захисту. Так, одним із основних є відсутність єдиного підходу до розуміння цифрових прав людини. Це створює проблеми як для законодавчого закріплення цих прав, так і для їх судового захисту. Необхідним є вироблення єдиної концептуальної основи цифрових прав, яка б враховувала їх специфіку та зв'язок з традиційними правами людини.

Поряд із цим викликає занепокоєння проблема балансу між цифровими правами та цифровою безпекою. Забезпечення інформаційної безпеки держави нерідко супроводжується обмеженнями в реалізації прав і свобод громадян у цифровому середовищі. Вирішення цієї дилеми потребує створення ефективних механізмів, які дозволили б гарантувати належний рівень безпеки без надмірного втручання у приватну сферу особи.

Складним залишається й питання цифрової нерівності, що проявляється у нерівному доступі громадян до цифрових технологій. Це натомість спричиняє нерівність у реалізації прав людини, зокрема права на доступ до інформації, освіти, адміністративних послуг тощо. У таких умовах право на доступ до

інтернету набуває фундаментального значення, стаючи передумовою для реалізації інших прав.

Водночас потребує переосмислення і правове регулювання в умовах цифровізації. Багато традиційних правових інститутів формувалися в аналоговому середовищі, тому значною мірою не відповідають потребам цифрової епохи. Це стосується, зокрема, норм, що регулюють захист приватності, інтелектуальну власність, договірні відносини тощо. Їх адаптація до нових реалій є однією з актуальних задач сучасного правознавства.

Швидкі темпи технологічного розвитку також зумовлюють технологічну залежність правового регулювання. Норми права часто не встигають за технологічними змінами, що робить законодавство застарілим уже на етапі його прийняття. Це підсилює потребу у гнучких, технологічно нейтральних правових механізмах, які могли б оперативно реагувати на виклики цифрового середовища.

Ще однією важливою проблемою є визначення юрисдикції у цифровому просторі. Глобальна природа інтернету ускладнює ідентифікацію застосовного права у випадках порушення цифрових прав, особливо коли йдеться про транскордонні правопорушення. Така ситуація потребує вироблення міжнародно погоджених підходів до юрисдикційного регулювання у цифровій сфері.

Окрему увагу слід приділити рівню цифрової грамотності населення. Без належних знань і навичок громадяни не можуть ефективно реалізовувати свої цифрові права, а також захищатися від загроз, що виникають у цифровому середовищі. У цьому контексті важливо формувати систему цифрової освіти та підвищувати цифрову культуру суспільства загалом.

Особливої уваги потребує питання захисту дітей у цифровому середовищі. Діти є найбільш вразливою категорією користувачів цифрових технологій і тому потребують спеціальних правових інструментів захисту від потенційних загроз, включаючи кібербулінг, доступ до шкідливого контенту, маніпулятивні алгоритми тощо.

З огляду на ці та інші виклики та ризики, дослідники роблять висновки про те, що сучасні цифрові технології не лише трансформують механізми публічної адміністрації, але й створюють принципово нові інструменти концентрації публічної влади, виходячи за межі традиційних дискусій про цифрові права людини, цифрову демократію чи цифровий суверенітет. Прикладом тому є концепція так званого «цифрового фашизму», яку обґрунтовує К. Фукс [54-55], який пропонує кардинально переосмислити природу сучасної цифрової держави та її функцій. На відміну від історичних форм фашизму, які асоціювалися насамперед із військовою диктатурою, відкритим політичним терором та фізичним насильством, цифровий фашизм, за логікою цього автора, функціонує значно складніше. Його основними інструментами стають цифрові платформи, алгоритми, великі масиви персональних даних, системи рекомендацій та механізми алгоритмічного управління інформаційними потоками. У цьому полягає принципова відмінність нової форми політичного домінування: вона дедалі менше спирається на відкрите примушування і дедалі більше – на непомітне програмування та моделювання соціальної поведінки.

Йдеться, зокрема, по-перше, про концентрацію влади в алгоритмічних системах, які поступово перетворюються із суто технічного інструмента на самостійний механізм формування інформаційного порядку денного; по-друге, тотальну цифрову контрольованість особистості, з огляду на те, що, наприклад, масове накопичення персональних даних, аналіз цифрової поведінки, геолокації, соціальних зв’язків, фінансових операцій та інформаційних уподобань створює безпрецедентний рівень знань про громадянина; по-третє, трансформацію цензури, яка у цифровому середовищі дедалі рідше набуває форми прямої заборони інформації; по-четверте, домінування пост-правди над раціональним дискурсом, коли алгоритмічні моделі оптимізуються не на пошук достовірної інформації, а на максимізацію уваги користувача; по-п’яте, алгоритмічне конструювання образу ворога, коли втрачає будь-який сенс створення внутрішнього або зовнішнього ворога, втім алгоритми інформаційних платформ

підсилюють поляризацію, формують інформаційні «бульбашки», радикалізують політичні позиції та стимулюють дегуманізацію опонентів; по-шосте, культ цифрового лідерства, коли завдяки сучасним цифровим платформам їх власники та окремі політичні діячі отримують практично необмежені можливості впливу на суспільну свідомість через прямий доступ до мільйонів користувачів без традиційних демократичних інституцій-посередників і, нарешті, по-сьоме, інтеграцію цифрового капіталу та політичної влади, в наслідок чого великі технологічні корпорації поступово концентрують не лише економічний, але й політичний, інформаційний та культурний вплив, а цифрова інфраструктура перетворюється на один із ключових інструментів політичного управління сучасним суспільством.

Таким чином, цифровізація конституційного права є багатогранним процесом, що охоплює трансформацію класичних прав і свобод, формування нових – цифрових – прав людини, переосмислення функцій держави та запровадження нових форм публічної адміністрації. Водночас цей процес супроводжується низкою серйозних викликів, серед яких відсутність уніфікованого визначення цифрових прав, проблема балансу між правами і безпекою, цифрова нерівність, відставання правового регулювання від технологічного прогресу, складність юрисдикційного визначення в мережевому середовищі, недостатній рівень цифрової грамотності населення та вразливість окремих соціальних груп, зокрема дітей тощо.

Усі ці фактори потребують комплексної реакції з боку держави, зокрема у вигляді модернізації конституційної доктрини, гармонізації законодавства з міжнародними стандартами, впровадження спеціалізованих інституційних механізмів захисту цифрових прав, а також розвитку цифрової культури суспільства. Без усвідомлення і правового забезпечення цифрових прав неможливо забезпечити реальну ефективність механізмів демократичного врядування в інформаційну епоху.

***Висновки до Розділу 1***

Резюмуючи, можна сформулювати низку висновків та узагальнень:

1. Посилення конституційного регулювання інформаційних та цифрових інститутів (нормативно-прикладний аспект) і формування відповідного доктринального супроводу з позицій цифрового права та цифрового конституціоналізму (теоретико-методологічний аспект) свідчить не лише про зростання ролі інформації, даних і цифрових технологій у механізмі сучасної державності, а й про їх глибинний аксіологічний, синергетичний та функціонально-телеологічний зв'язок із фундаментальними принципами конституційного ладу. Цифровізація змінює саму природу конституційно-правового регулювання, оскільки цифрове середовище стає простором реалізації прав людини, здійснення публічної влади та взаємодії держави і суспільства. Це дозволяє обґрунтовувати формування нової парадигми цифрового конституціоналізму, в межах якої інформаційна функція держави виступає системоутворюючим елементом сучасної державності.

2. Порівняльно-правовий розвиток конституціоналізму демонструє поступовий перехід від фрагментарного регулювання окремих інформаційних відносин (свобода слова, доступ до інформації, захист приватності) до комплексної конституціоналізації цифрової сфери. У процесі цифрової трансформації виникає необхідність нормативного закріплення нових правових категорій – цифрових прав людини, права на доступ до цифрового середовища, права на цифрову участь, права на захист персональних даних, права на цифрову ідентичність, а також гарантій інформаційної автономії особи. Таким чином, цифрові права поступово інтегруються у систему фундаментальних конституційних прав, відображаючи потреби інформаційного суспільства.

3. Посилення конституційного регулювання цифрової сфери не може розглядатися лише як збільшення кількості правових норм або деталізація технологічних процедур. Йдеться про сутнісну трансформацію ролі Конституції як нормативної основи цифрового порядку, що визначає межі використання цифрових технологій, принципи управління даними, стандарти електронного

врядування, гарантії приватності та механізми захисту людини у цифровому середовищі. У цьому сенсі цифрова конституціоналізація охоплює не лише інститути (державні інформаційні системи, цифрові платформи, механізми електронної ідентифікації), а й процедури (прозорість алгоритмічного управління, підзвітність цифрових рішень, відкритість даних) та стандарти (безпека, пропорційність, недискримінація, технологічна нейтральність).

4. Доктринальний розвиток цифрового права як міждисциплінарного напряму дозволяє переосмислити інформаційну функцію держави через взаємодію конституційного права, інформаційних технологій, захисту персональних даних та теорії прав людини. Цифрове право не обмежується регулюванням технологічних процесів, а формує критерії оцінки цифрової політики держави через призму верховенства права, людської гідності, свободи, приватності, демократії та безпеки. У цьому контексті цифрові права набувають не похідного, а самостійного конституційного значення, оскільки забезпечують можливість особи повноцінно брати участь у суспільних процесах цифрової епохи.

5. Синергетичний зв’язок між інформаційними інститутами та принципами конституційного ладу проявляється у взаємному впливі цифрового середовища і конституційних цінностей. З одного боку, принципи демократії, правової держави, відкритості влади та гарантування прав людини визначають межі цифровізації. З іншого – ефективність цифрових механізмів безпосередньо впливає на реальність цих принципів. Доступність цифрових сервісів, якість управління даними, прозорість алгоритмів та рівень цифрової грамотності населення визначають можливість реалізації права на участь у державному управлінні, доступ до публічної інформації та інших конституційних прав. Водночас цифрова нерівність стає новим фактором соціальної нерівності, що потребує конституційно-правових гарантій подолання.

6. Функціонально-телеологічний підхід дозволяє розглядати інформаційну функцію держави як інструмент досягнення стратегічних цілей цифрової

трансформації – забезпечення ефективного публічного управління, розвитку електронної демократії, підвищення прозорості влади, формування цифрової інфраструктури та гарантування інформаційної безпеки. Електронне урядування у цьому контексті є не лише технологічним механізмом надання адміністративних послуг, а новою формою реалізації конституційного принципу демократичної участі та взаємодії держави з людиною.

7. Еволюція зарубіжних моделей цифрового конституціоналізму демонструє формування нових інституційних механізмів захисту цифрових прав: незалежних органів контролю за захистом персональних даних, спеціалізованих інституцій у сфері цифрового нагляду, механізмів контролю за автоматизованим прийняттям рішень та гарантій кібербезпеки. Особливого значення набуває досвід правового регулювання захисту персональних даних у межах профільних європейських правових стандартів. Водночас надмірна деталізація цифрових норм у конституціях може знижувати їх адаптивність через швидкість технологічних змін, що потребує балансу між стабільністю конституційного регулювання та його відкритістю до інновацій.

8. Цифровізація конституційного права означає не просто розширення предмета правового регулювання, а зміну самої логіки сучасного конституціоналізму. Дані, інформаційні потоки та цифрові технології стають складовою конституційної матерії, оскільки через них реалізуються політичні, соціальні, особисті та культурні права людини. Це зумовлює необхідність формування нових конституційних стандартів щодо цифрової грамотності, доступності цифрових технологій, захисту від дискримінації у цифровому середовищі та забезпечення прав особи в умовах алгоритмічного управління.

9. У контексті українського державотворення конституціоналізація цифрових прав та інформаційних відносин перебуває на етапі становлення й потребує системного нормативного розвитку. Актуальними напрямами є гармонізація українського законодавства з міжнародними та європейськими стандартами цифрового права, удосконалення механізмів захисту персональних

даних, формування інституційних гарантій цифрових прав, включаючи можливість створення спеціалізованих механізмів їх захисту, зокрема інституту інформаційного омбудсмана. В умовах війни особливого значення набувають питання кіберстійкості, захисту інформаційного простору та забезпечення безперервності цифрового функціонування держави.

10. Цифровий конституціоналізм у воєнний та повоєнний періоди постає як динамічна система, що поєднує стабілізуючу роль Конституції із її адаптивним потенціалом щодо цифрових трансформацій. Держава має одночасно забезпечувати інформаційну безпеку, захист цифрової інфраструктури та протидію інформаційним загрозам, але водночас гарантувати свободу інформаційного обміну, цифрову автономію особи та розвиток інноваційного середовища. У цьому сенсі цифрові права набувають комплексного характеру, поєднуючи свободу і відповідальність, приватність і безпеку, індивідуальну автономію та публічний інтерес.

11. Перспективи подальших досліджень у профільній сфері пов'язані з формуванням цілісної теорії цифрових прав людини, визначенням їх конституційно-правової природи, розробленням ефективних механізмів їх гарантування та захисту, дослідженням впливу цифрової нерівності на реалізацію основних прав людини, а також пошуком оптимальних моделей юрисдикційного регулювання цифрового простору. Особливого значення набуває подальше осмислення інформаційної функції держави як самостійного напряму її конституційної діяльності, що забезпечує баланс між цифровим розвитком, технологічними інноваціями, інформаційною безпекою та фундаментальними правами людини.

## Список використаних джерел

1. Атаманова Н., Луняченко І. До питання цифровізації публічного управління в Україні. *Науковий вісник Міжнародного гуманітарного*

*університету. Сер.: Юриспруденція.* 2024. № 68. С. 4-11. DOI: https://doi.org/10.32782/2307-1745.2024.68.1

2. Батанов О. В. Цифровізаційні аспекти сучасного конституційного права. *Право.ua.* 2025. № 2. С. 227-236. DOI: https://doi.org/10.71404/LAW.UA.2025.2.36

3. Батанов О. В. Цифровізація сучасного конституційного права в умовах глобалізації. *Держава і право*: Збірник наукових праць. Юридичні і політичні науки. Випуск 98 / Ін-т держави і права імені В. М. Корецького НАН України. Київ : Вид-во «Юридична думка», 2025. С. 77-89. DOI: https://doi.org/10.33663/1563-3349-2025-98-77

4. Батанов О. В., Батанова Н. М. Інформаційний вимір сучасного конституційного права в умовах глобалізації. *Правовий статус учасників бойових дій, військових капеланів, полонених: міжнародні норми, реалії російсько-української війни*: матеріали міжнародної правової школи, м. Ужгород, 21 квітня 2023 р. Ужгород: Ужгородський національний університет, 2023. С. 26-36.

5. Батанов О. Інститут інформаційного омбудсмана на захисті прав людини у сфері інформації та інформаційної безпеки. *Правові засади інформаційної безпеки України в умовах російської воєнної агресії.* Збірник наукових праць / Інститут держави і права імені В.М. Корецького НАН України, Фонд інституційного розвитку української науки. Київ: «Видавництво Людмила», 2023. С. 45-49.

6. Бєлов Д. М., Бєлова М. В., Горнило О. Т. Право людини на забуття. *Науковий вісник Ужгородського національного університету.* Серія : Право. 2024. Вип. 81(2). С. 57-62. DOI: https://doi.org/10.24144/2307-3322.2024.81.2.9

7. Бєлов Д. М., Переш І. Є., Покорба І. Цифрові права людини: доктринальні засади. *Аналітично-порівняльне правознавство.* 2024. № 2. С. 110-115. DOI: https://doi.org/10.24144/2788-6018.2024.02.17

8. Борінштейн Є. Р., Городнюк Л. С. Філософсько-антропологічний феномен Homo Digitalis як онтологічної системи «людина-гаджет». *Studies in History and Philosophy of Science and Technology*. 2024. Vol. 33(1). С. 15-21. DOI: https://doi.org/10.15421/272402

9. Бочарова Н. В. Цифровий конституціоналізм в сучасному інформаційному суспільстві. *Соціальний калейдоскоп*. 2022. Вип. 1. С. 74-84. DOI: https://doi.org/10.47567/bomivit.2-1.2022.05

10. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий електронний журнал.* 2021. № 10. С. 58-61. DOI: https://doi.org/10.32782/2524-0374/2021-10/12

11. Венгер В., Кошман А. Права людини в цифрову епоху: процедурні гарантії та судовий захист. *Наукові записки НаУКМА.* Юридичні науки. 2025. Т. 16. С. 18-28. DOI: https://doi.org/10.18523/2617-2607.2025.16.18-28

12. Верлос Н. В. Конституціоналізація цифрових прав людини: вітчизняна практика та зарубіжний досвід. *Часопис Київського університету права.* 2022. № 2. С. 129-133. DOI: https://doi.org/10.36695/2219-5521.2.2020.21

13. Гавриленко Н. В. Правові засади цифрової ідентифікації і репрезентації особистості. *Актуальні проблеми політики.* 2024. Вип. 73. С. 162-167. DOI: https://doi.org/10.32782/app.v73.2024.23

14. Гачкевич А. О., Хомин В. А. Захист цифрових прав людини: політика та процедури корпорації Google щодо приватності. ***Human rights and public governance in modern conditions*** **:** Scientific monograph. Riga, Latvia : «Baltija Publishing», 2023. P. 99-110. DOI: https://doi.org/10.30525/978-9934-26-320-0-6

15. Гончаренко К. С. Цифрова людина: фантазм втрати ідентичності. *Філософські обрії*. 2019. № 42. С. 137-140.

16. Городнюк Л. С. Цифрова людина в екзистенційній площині соціально-філософської рефлексії : дис. … д-ра філософії за спец. 033 – Філософія. Одеса, 2026. 246 с.

17. Дзьобань О. П. Цифрова людина як філософська проблема. Інформація і право. 2021. № 2(37). С. 9-19. DOI: https://doi.org/10.37750/2616-6798.2021.2(37).238330

18. Ємельянова А. Г. Електронна петиція як форма реалізації конституційного права на участь в управлінні державними справами : дис. ... канд. юрид. наук : 12.00.02 «Конституційне право; муніципальне право». Київ, 2019. 231 с.

19. Жовнірчик Я. Ф., Квасюк В. В. Електронне врядування та електронна демократія стосовно децентралізації в Україні: стратегії реалізації та розвитку. *Інвестиції: практика та досвід.* 2020. № 1. С. 105-113. DOI: https://doi.org/10.32702/2306-6814.2020.1.105

20. Завгородня Ю. В. Кіберконфлікти як сучасна форма політичного протиборства : дис. … д-ра політ. наук : спец. 23.00.02 «Політичні інститути та процеси». Київ, 2024. 378 с.

21. Заярний О. А. До питання щодо виконання Україною міжнародних зобов'язань щодо запровадження інституту інформаційного омбудсмана: деякі концептуально-прикладні аспекти. *Науковий вісник Ужгородського Національного Університету*. Серія Право. 2021. Випуск 64. С. 213-219. DOI: https://doi.org/10.24144/2307-3322.2021.64.39

22. Климентьєв О. П. Інформаційна функція Української держави : автореф. дис. … канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Київ, 2014. 21 с.

23. Коліушко І. Б., Демкова М. С. Електронне урядування – шлях до ефективності та прозорості державного управління. *Інформаційне суспільство. Шлях України.* Київ : Бібліотека інформ. суспільства, 2018. С. 138-143.

24. Концепція розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 20.09.2017 №649-р. *Офіційний портал Верховної Ради України.* URL: http://zakon4.rada.gov.ua/laws/show

25. Костецька Т. А. Інформаційна функція держави: конституційні та інституаційні аспекти. *Держава і право*. Зб. наук. праць. Юрид. і політ. науки. Київ, 2010. Вип. 47. С. 113-119.

26. Костецька Т. А. Про розвиток сучасного конституціоналізму в контексті новітніх інформаційно-комунікаційних процесів. *Правова держава*: Щорічник наукових праць Інституту держави і права імені В. М. Корецького НАН України. Випуск 36. Київ, 2025. С. 351-360. DOI: https://doi.org/10.33663/0869-2491-2025-36-351-360

27. Костецька Т. А. Конституціоналізм в умовах цифрової модернізації національних суспільних відносин. *Досвід, воєнні випробування та повоєнний ренесанс конституційно-правового розвитку незалежної України*: збірник матеріалів міжнародних науково-практичних конференцій «28-річчя Конституції України: досвід, воєнні випробування та повоєнний ренесанс» (м. Київ, 26 червня 2024 року) та «Захист незалежності України: правові засади та виклики сьогодення. До 33-ї річниці проголошення незалежності України» (м. Київ, 22 серпня 2024 року) / відп. ред. акад. НАПрН України, д. ю. н., проф. О. В. Скрипнюк, д. ю. н., проф. А. Р. Крусян та д. ю. н., проф. О. В. Батанов. Київ, 2025. С. 248-251.

28. Костицький М., Бесчастний В., Кушакова-Костицька Н. Цифровий конституціоналізм: нова парадигма та перспективи розвитку в Україні. *Філософські та методологічні проблеми права.* 2022. № 2 (24). С. 9-26. DOI: https://doi.org/10.33270/02222402.9

29. Кудрявцев О. Ю. Електронне урядування у сучасному політико-адміністративному просторі : монографія. Харків : ХНУМГ ім. О. М. Бекетова, 2016. 184 с.

30. Куспляк І. С. Електронне урядування як інструмент формування відкритої та прозорої політичної влади : дис. … канд. політ. наук : спец. 23.00.02. Одеса, 2012. 204 с.

31. Кушакова-Костицька Н. В. Право на інформацію в інформаційну епоху (порівняльне дослідження) : монографія. Київ : Логос, 2018. 271 с.

32. Кушакова-Костицька Н. Вплив цифровізації на конституціоналізм: концептуальні підходи щодо перспектив державного регулювання інформаційного простору. *Філософські та методологічні проблеми права.* 2025. № 1 (29). С. 29-37. DOI: https://doi.org/10.33270/02252901.4

33. Лесько Н., Антонов М. Цифрові права людини в епоху глобалізації. *Вісник Національного університету «Львівська політехніка».* Серія : Юридичні науки. 2021. Т. 8. № 3. С. 160-166. DOI: http://doi.org/10.23939/law2021.31.160

34. Лощихін О. М. Комунікативна функція у системі функцій сучасної держави. *Публічне право*. 2013. № 2. С. 266. С. 263-268.

35. Марко О. В. Цифовізація як форма взаємодії суспільства і держави : дис. … д-ра філософії у галузі знань 05 «Соціальні та поведінкові науки» за спец. С2 «Політологія». Київ, 2026. 213 с.

36. Митко А., Кольцова І. Інформаційна безпека в контексті введення інституту інформаційного комісара (омбудсмена) в Україні. *Медіафорум : аналітика, прогнози, інформаційний менеджмент* : зб. наук. праць. Чернівці : Чернівецький нац. ун-т, 2018. Том 6. С. 112-122.

37. Павленко Ж. О. Поняття інформаційної функції держави. *Проблеми законності.* 2011. Вип. 117. С. 210. С. 202–211.

38. Петришин О. В., Гиляка О. С. Права людини в цифрову епоху: виклики, загрози та перспективи. *Вісник Національної академії правових наук України.* 2021. № 1. С. 15-23. DOI: https://doi.org/10.37635/jnalsu.28(1).2021.15-23

39. Проскура Г. Перспективи створення інституту інформаційного комісара в Україні. *Конституційно-правові академічні студії.* 2016. № 1. С. 118-123.

40. Радутний О. Е. Правовий статус та характеристика цифрової людини. *Інформація і право*. 2021. № 4(39). С. 35-51. DOI: https://doi.org/10.37750/2616-6798.2021.4(39).248552

41. Радутний О. Е. Цифрова людина з точки зору загальної та інформаційної безпеки: філософський та кримінально-правовий аспект.

*Інформація і право*. 2018. № 2(25). С. 158-170. DOI: https://doi.org/10.37750/2616-6798.2018.2(25).273260

42. Сапарова А. О. Цифрові права людини в системі конституційних цінностей: теоретико-правові засади. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2026. Випуск 2. Частина 1. С. 193-198. DOI: https://doi.org/10.24144/2788-6018.2026.02.1.28

43. Скіннер К. Людина цифрова. Четверта революція в історії людства, яка торкнеться кожного. Київ : Фабула, 2020. 272 с.

44. Терлецький Р. В. Держава та релігія в Україні: від історичних витоків до цифрової ери : монографія. Київ : Видавництво Людмила, 2026. 288 с.

45. Тимченко Н. М. Перспективи введення в Україні інституту інформаційного омбудсмана. *Проблеми і перспективи розвитку банківської системи України* : зб. наукових праць / ДВНЗ «УАБС НБУ». Суми, 2012. № 36. С. 265-269.

46. Тихомиров О. О. Права людини: інформаційний вимір : монографія. Одеса : Видавництво «Юридика», 2023. 304 с.

47. Чалчинський В. І. Конституційно-правове забезпечення прав людини в умовах цифровізації : дис. … докт. філос. за спец. 081 Право. Київ, 2025. 299 с.

48. Carta Portuguesa de Direitos Humanos na Era Digital. Lei n.º 27/2021, de 17 de maio. *Assembleia da República*. URL: https://files.diariodarepublica.pt/1s/2021/05/09500/0000500010.pdf

49. Constitución Política de los Estados Unidos Mexicanos. Constitución publicada en el Diario Oficial de la Federación el 5 de febrero de 1917. Última reforma publicada DOF 28-05-2021. *Portal Gob MX*. URL: https://www.gob.mx/cms/uploads/attachment/file/646405/CPEUM_28-05-21.pdf

50. Constitución Política del Perú. Promulgada el 29 de diciembre de 1993. *Congreso de la República Perú.* URL: https://www3.congreso.gob.pe/Docs/constitucion/constitucion/index.html#p=1

51. Constitution of the Portuguese Republic. Seventh revision [2005]. *Assembleia da República.* URL: https://www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf

52. Constitution of the Republic of Ecuador. Published in the Official Registe 20 October 2008. *Political Database of the Americas – Georgetown University.* URL: http://pdba.georgetown.edu/Constitutions/Ecuador/english08.html

53. Court of Justice of the European Union. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12). *EUR-Lex.* 2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131

54. Fuchs C. Digital Fascism and Digital Capitalism. *Philosophy & Social Criticism.* March 26, 2026. DOI: https://doi.org/10.1177/01914537261434922

55. Fuchs C. What is Digital Fascism? *St. Antony's International Review.* 2026. Vol. 20. № 1. DOI: https://doi.org/10.82556/stair.v20i1.550

56. Information Commissioner's Office (ICO). *GDPRhub.* URL: https://gdprhub.eu/ICO_%28UK%29?utm_source

57. Jackson E. The right mix: how Estonia ensures privacy and access to e-services in the digital age. *Estonian World.* URL: https://estonianworld.com/security/right-mix-estonia-ensures-privacy-access-e-services-digital-age/

58. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Ministerio de la Presidencia, Justicia y Relaciones con las Cortes.* URL: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

59. Lisbon Declaration – Digital Democracy with a Purpose. URL: https://cdn.bndlyr.com/saktyd721tavnzm2/_assets/svimXxZTg2Aylr4v.pdf

60. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679

61. The Constitution of Greece. As entered into force by virtue of the XIIth Resolution of June 7, 1975 of the Vth Revisionary Parliament (Revised by Resolution of November 25, 2019 of the IXth Revisionary Parliament). *ΛΕΥΚΗ ΣΕΛΙΔΑ. Hellenic Parliament, 2022.* URL: https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/THE%20CONSTITUTION%20OF%20GREECE.pdf

# РОЗДІЛ 2
# ЕЛЕКТРОННЕ ПРАВОСУДДЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: РЕГУЛЯТОРНІ МОДЕЛІ УКРАЇНИ ТА ЄВРОПЕЙСЬКОГО СОЮЗУ

Автор: ***Васильчук Лариса Богданівна,*** *кандидат юридичних наук, доцент, доцент кафедри конституційного права та порівняльного правознавства ДВНЗ «Ужгородський національний університет»*

Цифрова трансформація правосуддя вже не може розглядатися як допоміжний напрям модернізації судової системи. Упродовж останнього десятиліття інформаційні технології поступово змінили сам спосіб, у який суд, сторони та інші учасники процесу взаємодіють між собою. Електронне подання процесуальних документів, дистанційна участь у судовому засіданні, автоматизований розподіл справ, електронна ідентифікація, цифрові докази, онлайн-доступ до судових рішень і транскордонний обмін юридично значущими даними формують нове середовище здійснення правосуддя. Йдеться вже не лише про перенесення окремих паперових процедур в електронну форму, а про поступову зміну процесуальної архітектури, у межах якої технологія дедалі більше впливає на доступність суду, строки розгляду справ, прозорість процедур, способи підтвердження волевиявлення та навіть на розуміння належної процесуальної форми.

Такі зміни закономірно потребують не лише опису нових технологічних можливостей, а й осмислення їх правової природи та наслідків для самого здійснення правосуддя. Саме тому важливим є звернення до наукових підходів, у межах яких дослідники намагаються визначити, де проходить межа між простою автоматизацією окремих судових процедур і більш глибокою трансформацією судової діяльності. Аналіз доктринальних позицій дає змогу

з'ясувати, які ознаки характеризують сучасне електронне правосуддя, які ризики супроводжують його розвиток та яким чином цифрові інструменти можуть бути узгоджені з традиційними принципами судочинства.

У науковій літературі ця зміна описується через поняття «e-justice», «digital justice», «online courts», «cyberjustice». Richard Susskind, аналізуючи перспективи онлайн-судів, пропонує відмовитися від уявлення, що цифрова технологія має лише відтворювати традиційний фізичний суд у дистанційному форматі. На його думку, справжня трансформація починається тоді, коли технологія дає можливість інакше організувати доступ до правосуддя, комунікацію між учасниками та вирішення спорів [1, p. 55–70, 95–110; 2]. Цю тезу розвивають різні напрями досліджень. Marco Velicogna, Ernst Steigenga, Sandra Taal та Aernout Schmidt показують значення сумісності правових і технологічних рішень для взаємодії юрисдикцій [3, p. 274–294], тоді як Dory Reiling та Francesco Contini акцентують на тому, що цифрові судові платформи впливають на організацію процесу і тому не можуть розглядатися як нейтральна технічна інфраструктура [4].

Для України ця проблематика має подвійне значення. З одного боку, розвиток Єдиної судової інформаційно-комунікаційної системи та підсистеми «Електронний суд» є частиною внутрішньої судової реформи. З іншого – статус держави-кандидата на членство в Європейському Союзі об'єктивно посилює необхідність орієнтації на європейські підходи до цифрової ідентифікації, інтероперабельності, захисту даних, електронної комунікації та транскордонної судової співпраці. Саме тому порівняння України з ЄС доцільно проводити не як механічне зіставлення окремих технічних сервісів, а як аналіз регуляторних моделей, у яких по-різному поєднуються технологічна ефективність і процесуальні гарантії.

Окремої уваги потребує й український досвід функціонування правосуддя в умовах повномасштабної війни. Потреба забезпечити безперервність судового

захисту за умов повітряних тривог, переміщення населення, зміни територіальної підсудності та фізичної недоступності окремих судів надала електронним сервісам не просто зручності, а значення елементу стійкості правосуддя. У цьому контексті праці Ганни Єрмакової, Олександра Сотули, Владислава Бурого та інших українських дослідників переконливо показують, що цифровізація має оцінюватися через призму права на справедливий суд і реальної можливості особи скористатися судовим захистом, а не лише через кількість запущених модулів чи сервісів [5, с. 15–27; 6, с. 53–57; 7, с. 42–49].

Метою цього розділу є визначення особливостей регуляторних моделей електронного правосуддя в Україні та Європейському Союзі, встановлення спільних тенденцій і відмінностей їх розвитку, а також формулювання напрямів удосконалення української моделі з урахуванням сучасних європейських стандартів. Для цього поєднано аналіз законодавства України, актів Європейського Союзу та Ради Європи з дослідженням національних практик Естонії, Австрії й Німеччини. Такий вибір держав дає змогу побачити різні траєкторії цифровізації: від інтегрованої державної цифрової екосистеми до поступового нормативно формалізованого переходу від паперового до електронного провадження.

### 2.1. Електронне правосуддя як регуляторна модель

Поняття електронного правосуддя сьогодні використовується для характеристики досить широкого кола явищ, пов’язаних із застосуванням інформаційно-комунікаційних технологій у діяльності судів. До нього відносять електронне подання процесуальних документів, дистанційне проведення судових засідань, електронний документообіг, автоматизацію окремих процесуальних дій, доступ до матеріалів справи та інші цифрові інструменти. Водночас у сучасних дослідженнях дедалі помітнішою є тенденція розмежовувати просте використання технологій у традиційному судовому процесі та більш глибоку цифрову трансформацію правосуддя [4; 8, с. 72–79; 9,

p. 66–81; 10, c. 3–10]. Такий підхід видається обґрунтованим, оскільки сама по собі заміна паперової кореспонденції електронною ще не змінює сутності судового процесу. Інша ситуація виникає тоді, коли цифрова інфраструктура починає визначати спосіб звернення до суду, порядок ідентифікації учасника, форму подання документа, момент його вручення, доступ до матеріалів справи та інші юридично значущі елементи процесу.

У цьому контексті особливо важливою є позиція Dory Reiling та Francesco Contini. Досліджуючи функціонування e-justice platforms, автори виходять із того, що інформаційна система суду не залишається нейтральним технічним середовищем. Цифрові платформи впливають на організацію процесуальних дій і фактично створюють додатковий рівень регулювання судової діяльності. Саме тому, на думку дослідників, розвиток електронного правосуддя потребує постійного узгодження технологічних рішень із процесуальним законодавством та вимогами справедливої процедури [4]. Такий підхід має принципове значення для розуміння природи електронного правосуддя: технологічний дизайн системи визначає не лише зручність роботи користувача, а й те, які дії він може вчинити, в якій формі, у які строки та з якими юридичними наслідками.

Інший, але тісно пов’язаний аспект простежується у дослідженні Marco Velicogna, Ernst Steigenga, Sandra Taal та Aernout Schmidt. Аналізуючи розвиток електронної взаємодії між юрисдикціями держав – членів Європейського Союзу, автори показують, що ефективність цифрового правосуддя залежить не лише від технологічних можливостей окремої судової системи. Важливого значення набувають сумісність правових і технологічних рішень, можливість взаємодії різних національних систем, а також їх інтеграція у спільний європейський простір електронного правосуддя [3, p. 274–294]. Отже, електронне правосуддя доцільно розглядати не як набір ізольованих цифрових сервісів, а як систему взаємопов’язаних правових, організаційних та технологічних механізмів.

Узагальнення зазначених доктринальних підходів, положень європейських актів та практики функціонування систем електронного правосуддя дає підстави запропонувати для цілей цього дослідження розгляд його регуляторної моделі через декілька взаємопов'язаних складових [4; 11; 12; 13, p. 243–258]. Передусім ідеться про нормативне визначення електронної процесуальної форми, тобто встановлення правил щодо того, які процесуальні документи можуть або повинні подаватися в електронній формі, коли електронне вручення породжує юридичні наслідки та якими засобами підтверджуються особа й волевиявлення учасника процесу. Не менш важливою є інституційна складова, що охоплює систему органів, відповідальних за створення, адміністрування, технічне забезпечення і подальший розвиток цифрової судової інфраструктури.

Наступною складовою є інтероперабельність, оскільки сучасне електронне правосуддя передбачає не лише функціонування окремої інформаційної системи, а й її здатність безпечно взаємодіяти з іншими державними та, у транскордонних відносинах, іноземними системами. Окремого значення набуває блок гарантій основоположних прав – доступу до суду, рівності учасників процесу, публічності судового розгляду, захисту приватності та персональних даних. Нарешті, цифрова система повинна мати механізми адаптації до технологічних змін, нових кіберзагроз та появи інструментів, які ще донедавна не були характерними для судової діяльності, зокрема технологій штучного інтелекту. Для цілей цього дослідження таке структурування використовується як наша аналітична конструкція для послідовного порівняння української та європейської моделей електронного правосуддя.

Необхідність такого структурування стає особливо очевидною при порівнянні України та Європейського Союзу. Архітектура електронного правосуддя ЄС формується з урахуванням того, що держави-члени зберігають власні судові та інформаційні системи. Як показує Elena Alina Onţanu, розвиток e-justice на рівні Європейського Союзу має характер багаторівневого управління,

в якому беруть участь інституції ЄС, держави-члени, національні та місцеві органи, професійні спільноти й інші суб'єкти. Особливого значення за таких умов набуває саме транскордонна інтероперабельність національних інформаційних систем [13, p. 243–258]. Аналогічна логіка закладена і в сучасному нормативному регулюванні ЄС, орієнтованому на цифровізацію судової співпраці та забезпечення електронної взаємодії у транскордонних справах [11].

Українська модель формувалася за дещо іншою логікою. Її основою є створення єдиної національної судової інформаційної інфраструктури, що об'єднує електронну комунікацію учасників із судами та поступово має охопити внутрішні процеси судової діяльності. Dmytro Luchenko та Kristina Piatyhora, аналізуючи розвиток ЄСІТС і перспективи переходу до Єдиної судової інформаційно-комунікаційної системи, характеризують нову концепцію як спробу побудови більш централізованої та інтегрованої цифрової екосистеми правосуддя [9, p. 66–81]. Отже, якщо для європейської моделі одним із визначальних завдань є забезпечення сумісності різних національних систем, то для України першочерговим залишається формування цілісної внутрішньої цифрової інфраструктури. Саме співвідношення внутрішньої інтегрованості та зовнішньої інтероперабельності становить одну з важливих відмінностей цих моделей.

Водночас така відмінність не заперечує поступового зближення українського та європейського підходів у ціннісному вимірі. Регламент (ЄС) 2023/2844 розглядає цифровізацію судової співпраці не лише як спосіб підвищення її оперативності, а в контексті доступу до правосуддя, захисту основоположних прав, недискримінації, захисту персональних даних та інших гарантій належного судочинства [11]. Аналогічний людиноцентричний підхід простежується в Guidelines on electronic court filing (e-filing) and digitalisation of courts, прийнятих CEPEJ у 2021 році. У цих рекомендаціях цифровізація судів

пов'язується із необхідністю збереження доступності правосуддя та недопущення ситуацій, за яких технологічні рішення створюють для користувача нові процесуальні перешкоди [12]. Тому сучасна європейська дискусія фактично зміщується від питання про саму необхідність цифровізації до визначення тих правових умов, за яких цифровий суд зберігає фундаментальні властивості справедливого правосуддя.

Ця зміна дослідницького фокусу простежується і в сучасній українській правовій науці. В. Б. Крикун, аналізуючи трансформацію цивільного процесу в умовах цифровізації, розглядає електронний суд, електронний документообіг і використання відеоконференцзв'язку в контексті зміни способів реалізації процесуальних прав та забезпечення права на справедливий суд [8, с. 72–79]. Dmytro Luchenko та Kristina Piatyhora також наголошують, що e-justice не може зводитися виключно до технологічної модернізації, оскільки його призначення безпосередньо пов'язане із забезпеченням процесуальних прав сторін, доступністю, прозорістю та ефективністю судового провадження [9, p. 66–81]. Подібні проблеми порушуються й у новітніх українських дослідженнях електронного судочинства, в яких поряд із перевагами цифровізації аналізуються нормативні, організаційні та технічні ризики її реалізації [14, с. 337–343; 15, с. 35–42; 16, с. 238–243; 17, с. 38–44; 18, с. 308–312]. Це дозволяє говорити про поступове формування в українській доктрині підходу, за якого цифрова трансформація правосуддя оцінюється не лише через технічну ефективність системи, а насамперед через її здатність забезпечувати належну реалізацію процесуальних прав і принципів верховенства права.

### 2.2. Українська модель електронного правосуддя: становлення та ключові виклики

Формування української моделі електронного правосуддя відбувалося поступово та значною мірою залежало від готовності нормативної й технічної інфраструктури судової влади. Її центральним елементом стала Єдина судова

інформаційно-телекомунікаційна система, а подальший розвиток нормативної моделі пов'язується з переходом до Єдиної судової інформаційно-комунікаційної системи. Законодавчі засади функціонування такої системи закріплені у Законі України «Про судоустрій і статус суддів» та процесуальних кодексах. Одним із ключових етапів цього процесу стало прийняття Закону України від 27 квітня 2021 року № 1416-IX, яким було передбачено можливість поетапного впровадження окремих підсистем і модулів ЄСІТС [19]. Такий законодавчий підхід дозволив відмовитися від моделі одномоментного запуску всієї системи та вводити в експлуатацію окремі функціонально готові компоненти.

Наступним важливим кроком стало затвердження 17 серпня 2021 року Вищою радою правосуддя Положення про порядок функціонування окремих підсистем (модулів) ЄСІТС [20]. Саме цей акт деталізував функціонування таких ключових елементів, як «Електронний кабінет», «Електронний суд» і підсистема відеоконференцзв'язку. Їх запровадження створило базовий цифровий контур взаємодії користувача із судовою системою: реєстрацію та електронну ідентифікацію, подання процесуальних документів, отримання документів суду, доступ до інформації про рух справи, а також можливість дистанційної участі у судовому засіданні [20; 16, с. 238–243; 18, с. 308–312]. Водночас уже на цьому етапі виявилася характерна особливість української моделі: розвиток зовнішніх цифрових сервісів для учасників процесу випереджав завершення повної цифровізації внутрішнього життєвого циклу судової справи. У науковій літературі ця фрагментарність розглядається як одна з проблем подальшого розвитку електронного судочинства [14, с. 337–343; 15, с. 35–42].

Подальша зміна правового статусу електронної взаємодії із судом пов'язана із прийняттям Закону України від 29 червня 2023 року № 3200-IX. Ним було істотно розширено коло суб'єктів, для яких реєстрація електронного кабінету стала обов'язковою. Такий обов'язок поширено, зокрема, на адвокатів,

нотаріусів, державних і приватних виконавців, арбітражних керуючих, судових експертів, органи державної влади, органи місцевого самоврядування та юридичних осіб, тоді як для інших фізичних осіб збережено можливість добровільної реєстрації [21]. Отже, електронний кабінет поступово перестав бути виключно альтернативним способом комунікації із судом і для професійних та інституційних учасників набув характеру нормативно визначеного середовища процесуальної взаємодії.

Ця зміна має значення не лише з технічної, а й із процесуально-правової точки зору. Обов'язок користуватися електронним кабінетом безпосередньо пов'язується із процесуальними наслідками невиконання встановлених законом вимог [21]. Відтак цифрова форма комунікації починає впливати на практичну реалізацію процесуальних прав та обов'язків учасника. На наш погляд, саме в цьому проявляється одна з характерних рис сучасної української моделі електронного правосуддя: технологічна готовність окремих категорій учасників уже не є лише питанням зручності, а набуває значення юридично релевантної передумови належної участі у процесі. Такий висновок водночас актуалізує проблему стабільності інформаційної системи, доступності технічної підтримки та правового регулювання наслідків технічних збоїв.

Українські дослідники звертають увагу саме на цю взаємозалежність технологічного розвитку і нормативної визначеності. Ольга Скочиляс-Павлів, аналізуючи цифрову трансформацію правосуддя, виокремлює дві групи проблем, що супроводжують цей процес: техніко-організаційні та процесуально-правові. До перших авторка відносить, зокрема, недостатнє матеріально-технічне забезпечення, проблеми взаємодії з державними реєстрами, перебої з електропостачанням і відсутність належних механізмів аварійного збереження даних; до других – недостатню визначеність правил роботи з електронними доказами та інших цифрових процедур [14, с. 337–343]. Володимир Логойда також наголошує, що подальший перехід від електронного забезпечення

діяльності судів до цифрового правосуддя потребує не лише технічного оснащення, а й розвитку правової культури користування інформаційними системами та послідовного вдосконалення законодавства [15, с. 35–42]. С. І. Сімакова і В. М. Клочко, досліджуючи функціонування «Електронного суду», акцентують на можливостях дистанційного подання процесуальних документів, ознайомлення з матеріалами справи, отримання судових рішень і використання відеоконференцзв'язку, водночас пов'язуючи ефективність цих механізмів із якістю організації електронного документообігу [16, с. 238–243].

Схожий напрям простежується і в новіших дослідженнях цивільного процесу. Марина Мелянчук розглядає цифровізацію цивільного судочинства через розвиток електронних процедур, електронного документообігу, виконання судових рішень та нові ризики, пов'язані із застосуванням штучного інтелекту [17, с. 38–44]. Василь Парасюк, Оксана Онишко та Ростислав Бориславський зосереджують увагу на теоретико-правових засадах електронного судочинства та значенні цифрової компетентності учасників процесу [10, с. 3–10]. А. М. Горішня аналізує українську систему в контексті євроінтеграційних процесів та необхідності забезпечення безперервності правосуддя в умовах повномасштабної війни [18, с. 308–312]. Узагальнення цих наукових позицій дає підстави стверджувати, що технологічна модернізація сама по собі не гарантує підвищення доступності та ефективності правосуддя: цифрові інструменти мають бути підтримані достатньою нормативною визначеністю, належною організацією та стабільною технічною інфраструктурою.

Особливо виразно ця проблема проявляється тоді, коли технічна обставина може безпосередньо вплинути на процесуальне становище особи. У традиційному паперовому процесі юридичне значення таких фактів, як дата поштового відправлення, відмітка канцелярії або підпис на документі, значною мірою визначене усталеною практикою. В електронному середовищі аналогічного правового значення набувають інші обставини: момент

завантаження документа, час його доставки до електронного кабінету, системне підтвердження відправлення, коректність накладення електронного підпису, технічна сумісність формату файла. Саме тому Ганна Єрмакова, аналізуючи цифровізацію через призму права на справедливий суд, окремо наголошує на необхідності юридичного механізму контролю та відновлення прав у разі технічного збою або цифрової помилки [5, с. 15–27]. Якщо законодавство не визначає юридичного значення таких технічних подій достатньо чітко, технологічна невизначеність може трансформуватися у процесуальну.

Звідси випливає необхідність поступового переходу від регулювання окремих електронних дій до формування цілісного цифрового життєвого циклу судової справи. У межах такого підходу електронне подання документа, його реєстрація, передавання судді, формування матеріалів електронної справи, надсилання процесуальних повідомлень і подальше архівування повинні функціонувати не як відокремлені операції, а як елементи єдиного інформаційного процесу. На наш погляд, наступним етапом цифровізації має бути не стільки розширення кількості електронних сервісів, скільки забезпечення безперервного руху структурованих даних протягом усього циклу розгляду справи. Порівняння з австрійською та естонською практикою далі підтверджує доцільність такого підходу.

Про незавершеність інституційного формування української моделі свідчить і постійне коригування нормативної основи її функціонування. Рішенням Вищої ради правосуддя від 13 січня 2026 року № 26/0/15-26 були внесені чергові зміни до Положення про порядок функціонування окремих підсистем (модулів) ЄСІТС [22]. Сам факт систематичного оновлення підзаконного регулювання можна розглядати як закономірну реакцію на розвиток технологій та накопичення практики їх застосування. Водночас для процесуального права важливо, щоб така адаптивність не призводила до втрати

передбачуваності. Користувач повинен мати можливість наперед визначити не лише технічний спосіб вчинення дії, а й її юридичні наслідки.

Особливе значення цифрова інфраструктура набула після запровадження воєнного стану. Олександр Сотула, досліджуючи організацію судочинства в умовах війни, зазначає, що поряд зі зміною територіальної підсудності одним із ключових механізмів забезпечення безперервності правосуддя стало розширення використання електронного суду та відеоконференцзв'язку. Автор також пов'язує цифровізацію з можливістю зберегти доступ до правосуддя для внутрішньо переміщених осіб, мешканців прифронтових територій та інших вразливих груп [6, с. 53–57]. Ганна Єрмакова розглядає ту саму проблему з конституційно-правової перспективи та наголошує, що цифрові форми здійснення правосуддя в умовах воєнного стану можуть бути допустимими лише за умови збереження функціональної еквівалентності процесуальних гарантій і наявності механізмів юридичного відновлення у разі технічних порушень [5, с. 15–27].

Отже, воєнний досвід водночас продемонстрував і переваги, і вразливість цифрового правосуддя. Можливість дистанційної комунікації дала змогу підтримувати функціонування судової системи за умов переміщення учасників, зміни територіальної підсудності та фізичної недоступності окремих судів. Проте залежність від електропостачання, якості зв'язку, доступності технічних засобів і засобів електронної ідентифікації виявила ризик виникнення нової форми нерівності у доступі до правосуддя. На цю проблему також звертають увагу сучасні українські дослідники, вказуючи на цифрову нерівність, технічну залежність та фрагментарність електронної інфраструктури як фактори, здатні впливати на реалізацію права на судовий захист [5, с. 15–27; 18, с. 308–312].

Саме тому подальший розвиток української моделі, на наш погляд, повинен ґрунтуватися на поєднанні принципу пріоритетності цифрової взаємодії з гарантією реального доступу до суду. Цифровий канал доцільно розглядати як

пріоритетний, але не виключний спосіб взаємодії із судом: він має ставати основним там, де підвищує швидкість, доступність і передбачуваність судової процедури, однак його обов'язковість не повинна створювати непропорційні перешкоди для осіб, які через об'єктивні обставини не можуть повноцінно ним скористатися.

### 2.3. Європейська модель електронного правосуддя: наднаціональна інтероперабельність і національні практики

Європейська модель електронного правосуддя формувалася в інституційних умовах, відмінних від українських. Компетенція Європейського Союзу у сфері правосуддя не передбачає повної уніфікації організації національних судових систем, унаслідок чого розвиток e-justice значною мірою залежить від уже створеної цифрової інфраструктури держав-членів, їхньої готовності до співпраці та здатності забезпечувати транскордонну сумісність інформаційних систем. Саме на цю особливість звертає увагу Elena Alina Onţanu, характеризуючи європейське електронне правосуддя як систему багаторівневого управління, у межах якої різні функції та компетенції розподіляються між інституціями ЄС, державами-членами, національними і місцевими органами, професійними об'єднаннями та іншими суб'єктами [13, p. 243–258]. Отже, на відміну від централізованої моделі єдиної національної судової інформаційної системи, європейський підхід значною мірою формується навколо завдання забезпечити взаємодію вже існуючих національних цифрових середовищ.

Одним із перших видимих для користувача елементів цієї моделі став European e-Justice Portal. Його функція не обмежується поширенням загальної правової інформації: портал акумулює відомості про національні судові системи, процесуальні правила та наявні в окремих державах можливості електронного звернення до суду, подання документів, їх електронного вручення, доступу до справ та інших форм цифрової комунікації [23]. При цьому обсяг таких можливостей істотно відрізняється залежно від конкретної держави-члена та

виду провадження. Тому портал доцільно розглядати передусім як спільний інформаційний і навігаційний рівень європейського e-justice, а не як єдину централізовану систему здійснення судових процедур.

Сам по собі інформаційний портал, однак, не вирішував значно складнішої проблеми, яку можна окреслити як технічну та організаційну взаємодію між національними системами правосуддя. Відповіддю на цю потребу став e-CODEX – e-Justice Communication via Online Data Exchange. Його принципова особливість полягає в тому, що система не замінює національні інформаційні рішення і не вимагає створення єдиної централізованої бази даних. Вона забезпечує можливість безпечного електронного обміну між автономними національними системами через узгоджені точки доступу та стандарти передачі даних. Така логіка прямо закріплена у Regulation (EU) 2022/850, який визначає e-CODEX як децентралізовану та інтероперабельну систему транскордонної комунікації у сфері судової співпраці в цивільних і кримінальних справах [24].

Доктринальне осмислення цього підходу з'явилося ще на ранніх етапах розвитку e-CODEX. Nadia Carboni та Marco Velicogna, аналізуючи проект транскордонного електронного обміну даними, звертали увагу на те, що головна складність полягає не стільки у створенні програмного забезпечення, скільки у необхідності узгодити різні правові, організаційні та технологічні середовища держав-учасниць [25, p. 104–120]. Marco Velicogna, Ernst Steigenga, Sandra Taal та Aernout Schmidt розвивають цю ідею ширше, розглядаючи ІКТ як інструмент «відкриття» національних юрисдикцій для транскордонної взаємодії та підкреслюючи значення сумісності між існуючими національними системами [3, p. 274–294]. Таким чином, e-CODEX доцільно розглядати не лише як технічну платформу, а як інфраструктурний механізм, через який реалізується сама ідея інтероперабельного європейського електронного правосуддя.

Практична життєздатність цього підходу була перевірена ще в межах перших транскордонних пілотів. George Pangalos, Ioannis Salmatzidis та Ioannis

Pagkalos на прикладі European Payment Order e-CODEX pilot показали можливість використання інформаційних технологій для спрощення доступу громадян і юридичних професіоналів до транскордонних юридичних процедур, а також для покращення взаємодії між судами та компетентними органами різних держав [26, p. 43–52]. Йдеться, таким чином, уже не лише про концептуальну можливість цифрового обміну, а про практичне відпрацювання конкретного транскордонного процесуального сценарію.

Подальший розвиток e-CODEX супроводжувався поступовою інституціоналізацією цієї системи на рівні права Європейського Союзу. Regulation (EU) 2022/850 від 30 травня 2022 року встановив спеціальну правову рамку функціонування e-CODEX, визначив його структуру, функції, правила безпеки та розподіл відповідальності між Європейською Комісією, державами-членами, операторами точок доступу й European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) [24]. Регламент також передбачив передачу eu-LISA функцій з управління системою. Це означало перехід e-CODEX від проектної моделі, що розвивалася консорціумом держав та організацій, до стабільнішої інституційної конструкції права ЄС.

Наступним етапом став Regulation (EU) 2023/2844 від 13 грудня 2023 року про цифровізацію судової співпраці та доступу до правосуддя у транскордонних цивільних, комерційних і кримінальних справах [11]. Його значення полягає в тому, що цифрова комунікація перестає розглядатися як сукупність окремих експериментальних рішень і включається у більш цілісну нормативну систему транскордонної судової співпраці. Регламент встановлює єдину правову рамку електронної комунікації між компетентними органами, а також між фізичними чи юридичними особами і такими органами у передбачених ним цивільних та комерційних процедурах [11].

Крім електронної комунікації, Regulation (EU) 2023/2844 регулює використання відеоконференцій та інших засобів дистанційної комунікації, застосування електронних підписів і електронних печаток, юридичні наслідки електронних документів, а також електронну сплату судових зборів [11]. Отже, його комплексність полягає саме в тому, що цифровізація розглядається не як окрема технічна процедура подання документа, а як нормативно взаємопов'язаний комплекс інструментів, що супроводжують різні стадії транскордонної судової взаємодії.

Особливо показовим у цьому контексті є розвиток принципу «digital by default». Stefano Signorin, досліджуючи цифровізацію транскордонного отримання доказів у цивільних і комерційних справах, характеризує цифровий канал як пріоритетний спосіб комунікації між компетентними органами та пов'язує реалізацію цієї моделі з децентралізованою інтероперабельною інфраструктурою, заснованою на e-CODEX [27, p. 603–620]. Водночас автор окремо розглядає питання сумісності такого технологічного рішення із захистом фундаментальних прав. Отже, навіть у межах моделі digital by default цифрова ефективність не може розглядатися ізольовано від процесуальних гарантій.

Подібну логіку простежує Fernando Gascón Inchausti, аналізуючи Regulation (EU) 2023/2844. Автор звертає увагу на те, що новий нормативний акт не лише розширює цифрову комунікацію між компетентними органами через e-CODEX, а й передбачає створення European electronic access point для взаємодії з учасниками процесу та встановлює мінімальну рамку використання відеоконференцій у транскордонних провадженнях [28, p. 535–552]. У сукупності це формує модель, за якої особа поступово отримує можливість взаємодіяти з правосуддям іншої держави-члена через стандартизовані європейські механізми, не будучи змушеною повністю адаптуватися до внутрішньої технічної архітектури кожної окремої національної системи.

Для України така модель має значення передусім як орієнтир майбутньої інтероперабельності. Йдеться не про механічне копіювання інтерфейсів, архітектури European e-Justice Portal чи окремих компонентів e-CODEX. На наш погляд, важливішим є поступове забезпечення сумісності електронної ідентифікації, довірчих послуг, форматів процесуальних документів, механізмів підтвердження доставки, метаданих та правил роботи з електронними доказами. Саме така сумісність у перспективі може забезпечити можливість включення української цифрової судової інфраструктури до ширшого європейського простору судової співпраці.

У цьому сенсі подальший розвиток ЄСІТС може розглядатися не лише як завдання внутрішньої цифровізації судової влади, а й як підготовка до майбутніх транскордонних сценаріїв взаємодії. Особливо актуальними вони є у цивільних і комерційних справах з іноземним елементом, під час вручення процесуальних документів, отримання доказів, визнання та виконання судових рішень і в інших формах міжнародної судової співпраці. Такий висновок є нашим узагальненням порівняльного аналізу європейської нормативної моделі та не означає, що чинне право ЄС уже встановлює для України конкретний обов'язок приєднання до e-CODEX.

Показовим для українського контексту є інший висновок, що випливає з досвіду ЄС: інтероперабельність не потребує повної уніфікації національних інформаційних систем. e-CODEX побудований саме на протилежній логіці – збереженні автономності національної інфраструктури при стандартизації способів транскордонної взаємодії [25, p. 104–120; 24]. Для України це означає, що європейська інтеграція у сфері e-justice потенційно сумісна зі збереженням власної ЄСІТС, за умови розвитку спільних стандартів довіри, електронної ідентифікації, безпеки та обміну структурованими даними.

Звернення до практики окремих держав-членів дозволяє конкретизувати ті підходи, які на рівні Європейського Союзу формулюються переважно як загальні

принципи цифровізації, інтероперабельності та доступу до правосуддя. Для такого порівняння показовими є Естонія, Австрія та Німеччина, оскільки кожна з цих держав формувала електронне правосуддя за дещо іншою інституційною логікою. Естонський досвід демонструє модель, у якій цифровізація судів є частиною цілісної цифрової державної інфраструктури; австрійський – тривалий розвиток стандартизованого електронного правового обігу між судами та професійними учасниками; німецький – поступове нормативне запровадження електронної комунікації та електронної судової справи. Таке зіставлення дозволяє оцінити не лише технічні відмінності, а й різні способи поєднання цифрових сервісів із процесуальним регулюванням.

Найвиразніше зв'язок між електронним правосуддям і загальною моделлю цифрової держави простежується в Естонії. Viljar Peep, аналізуючи становлення digital justice в цій державі, пов'язує розвиток судових технологій із більш широкою трансформацією публічного сектору, централізацією допоміжних сервісів та створенням єдиної цифрової інфраструктури державного управління. Автор звертає увагу на те, що судова система використовує інтегровані інформаційні рішення та спільне цифрове середовище, яке створює умови для дистанційного та електронного провадження. Водночас Peep підкреслює і характерний конституційно-правовий виклик: цифрова ефективність судової діяльності має бути узгоджена з вимогою публічності правосуддя [29, p. 496–508].

Інституційним ядром цієї моделі є система E-File (E-toimik). За офіційною інформацією Centre of Registers and Information Systems, E-File є центральною інформаційною системою, що забезпечує обмін процесуальними даними та документами у цивільних, адміністративних, кримінальних і провадженнях про правопорушення. Через неї учасники можуть подавати документи до суду, поліції та прокуратури, відстежувати перебіг справи й отримувати доступ до матеріалів, що стосуються конкретного провадження. Водночас система

інтегрується з інформаційними системами судів та інших органів правосуддя, що дозволяє уникати повторного введення тих самих даних і забезпечує їх подальше використання в межах єдиного цифрового процесу [30].

Саме ця риса відрізняє E-File від звичайного електронного кабінету користувача. Йдеться не лише про канал подання документів, а про інформаційну систему, що забезпечує рух процесуальних даних між різними інституціями. Офіційний опис системи прямо вказує на її інтегрований характер та на те, що доступ до інформації обмежується відповідно до повноважень і процесуального статусу користувача [30]. Отже, перевага естонської моделі полягає не стільки у кількості електронних сервісів, скільки у здатності поєднати їх у спільний цифровий життєвий цикл справи. Водночас така інтегрованість закономірно підвищує вимоги до контролю доступу, журналювання операцій та захисту персональних даних.

Для України цей досвід є особливо цікавим через схожий загальний вектор розвитку цифрової держави. Розвиток платформи «Дія», засобів електронної ідентифікації та взаємодії державних реєстрів створює передумови для більш глибокої інтеграції судових сервісів у загальне цифрове середовище. О. А. Ярошенко та І. О. Соколова, зіставляючи платформу «Дія» та електронний суд, також звертають увагу на взаємозв’язок цифровізації держави, доступності правосуддя, кібербезпеки та проблеми цифрової нерівності [31, с. 151–156]. Однак у сфері правосуддя така інтеграція потребує особливо обережного правового регулювання, оскільки судові інформаційні системи містять дані, доступ до яких може бути обмежений законом, зокрема інформацію про дітей, стан здоров’я, банківську чи комерційну таємницю, матеріали кримінальних проваджень та інші чутливі дані. Тому принцип повторного використання інформації у судовій сфері не може застосовуватися автоматично лише на тій підставі, що відповідні відомості вже перебувають у розпорядженні держави.

Якщо естонська модель демонструє переваги інтеграції правосуддя у широку цифрову екосистему держави, то австрійський досвід показує інший шлях – поступове перетворення електронної професійної комунікації із судом на усталений елемент процесуальної практики. Система Elektronischer Rechtsverkehr (ERV) функціонує в Австрії з 1990 року. За офіційною інформацією Федерального міністерства юстиції Австрії, ERV забезпечує захищене безпаперове передавання структурованих даних і процесуальних документів між учасниками провадження та судами, а згодом була інтегрована з внутрішніми інформаційними системами судової влади [32].

Через ERV можуть передаватися позови, заяви, процесуальні пояснення, апеляційні документи та додатки, а суди, своєю чергою, можуть надсилати процесуальні документи учасникам. Для низки професійних та інституційних користувачів використання системи є обов'язковим [32]. Саме тривалість функціонування та поступове розширення кола користувачів дозволили ERV стати не допоміжною альтернативою паперовому обігу, а звичним способом процесуальної комунікації. Офіційні матеріали австрійської юстиції прямо пов'язують її ефективність із можливістю автоматично передавати структуровані дані до внутрішніх програм управління судовими справами.

Особливо показовим у цьому аспекті є досвід Конституційного суду Австрії. Із 2013 року Суд перевів внутрішнє та зовнішнє провадження в електронний формат, поєднавши ERV з електронною справою. Офіційні матеріали Конституційного суду зазначають, що метадані, отримані через ERV, можуть автоматично використовуватися у внутрішній системі, завдяки чому зменшується обсяг ручного введення інформації, спрощується пошук документів і зникає необхідність фізичного переміщення матеріалів справи [33; 34].

У цьому полягає одна з найбільш корисних для України рис австрійського досвіду. Цифровий ефект виникає не в момент, коли процесуальний документ просто надсилається до суду в електронній формі, а тоді, коли дані з нього без

додаткового дублювання включаються у внутрішній цифровий процес. Саме тому австрійську модель доцільно розглядати як приклад поступового переходу від електронної комунікації до інтегрованого електронного провадження. На наш погляд, ця особливість має значення і для розвитку ЄСІТС, оскільки дозволяє змістити акцент із кількості зовнішніх сервісів на безперервність руху інформації всередині судової системи.

З австрійського досвіду випливає ще один важливий висновок – значення професійної обов'язковості. Коли адвокати, нотаріуси та інші професійні учасники постійно використовують один стандартизований канал, електронний документообіг перестає існувати паралельно з паперовим як факультативна можливість. Водночас сама по собі нормативна обов'язковість не є достатньою умовою успіху. Вона має спиратися на стабільність електронного каналу, зрозумілі технічні стандарти та передбачувані процесуальні наслідки використання системи. У цьому сенсі український Закон № 3200-IX, який розширив коло осіб, зобов'язаних мати електронні кабінети, рухається в подібному напрямі, хоча інституційна зрілість української системи поки є іншою.

Якщо австрійська модель значною мірою виросла з тривалої практики електронного обміну між професійними учасниками і судами, німецький шлях характеризується більш поетапним нормативним запровадженням цифрових інструментів. За офіційною інформацією Bundesministerium der Justiz und für Verbraucherschutz, центральними напрямами цифровізації німецького правосуддя є електронний правовий обіг, електронна судова справа та дистанційні форми участі; з 1 січня 2026 року всі нові судові справи мають вестися в електронній формі [35].

Одним із центральних компонентів цієї моделі є elektronischer Rechtsverkehr, а для адвокатської професії – besonderes elektronisches Anwaltspostfach (beA). Bundesrechtsanwaltskammer підтверджує, що кожен

адвокат, допущений до практики в Німеччині, має персональний beA для захищеної електронної комунікації. Із 1 січня 2018 року діє обов'язок забезпечувати технічну готовність до отримання повідомлень через beA, а з 1 січня 2022 року – загальний обов'язок професійного електронного подання документів до судів [36].

Юридичне значення beA виходить за межі звичайної електронної поштової скриньки: захищений канал безпосередньо пов'язаний із професійним статусом конкретного адвоката. Для електронного правосуддя це показує важливість надійного зв'язку між цифровою ідентичністю користувача, його процесуальним статусом та повноваженнями.

Німецький досвід водночас демонструє складність цифровізації федеративної та юрисдикційно розгалуженої системи. Його перевагою є нормативна поступовість: електронна комунікація, професійні цифрові канали та електронна справа впроваджувалися як юридично визначені компоненти, а перехід до обов'язкової електронної справи завершився для нових проваджень з 1 січня 2026 року [35; 36]. Така послідовність підвищує передбачуваність переходу, хоча потребує постійної координації між різними рівнями судової системи.

Зіставлення трьох моделей дозволяє сформулювати кілька загальних висновків. Естонський досвід показує переваги інтеграції електронного правосуддя у зрілу загальнодержавну цифрову інфраструктуру; австрійський – значення довготривалої, стандартизованої та значною мірою обов'язкової професійної електронної комунікації; німецький – роль послідовного нормативного впровадження окремих компонентів e-justice. Жодна з цих моделей не може бути механічно перенесена в українське середовище, оскільки вони сформувалися за різних інституційних, правових і технологічних умов.

Водночас їх порівняння дозволяє зробити висновок щодо можливого напряму розвитку української системи. Україна потенційно має передумови для

поєднання окремих переваг усіх трьох моделей: розвиток загальнодержавної цифрової інфраструктури наближає її до естонського підходу; запровадження обов'язкових електронних кабінетів для професійних учасників має певну функціональну подібність до австрійської та німецької практики; подальше нормативне формування ЄСІТС створює можливість поступового переходу до повного електронного життєвого циклу судової справи. Ключовим завданням при цьому є не просте накопичення цифрових сервісів, а їх поєднання в узгоджену систему, в якій зовнішня комунікація користувача, внутрішня електронна справа та взаємодія з іншими інформаційними ресурсами функціонують як складові єдиного процесу.

### 2.4. Процесуальні гарантії цифрового правосуддя: доступ, ідентифікація, докази та безпека

Однією з головних переваг електронного правосуддя є розширення практичних можливостей звернення до суду. Онлайн-подання документів зменшує залежність від географічної відстані, скорочує витрати на поштове пересилання та особисті поїздки, а також дозволяє користувачеві взаємодіяти із судом поза межами фізичної канцелярії. Для осіб, які перебувають за кордоном, мають обмежену мобільність або проживають далеко від суду, цифровий канал може істотно полегшити реалізацію права на судовий захист. Саме з цієї перспективи Richard Susskind розглядає онлайн-суди як один із способів подолання частини системних бар'єрів, властивих традиційній моделі правосуддя [1, p. 55–70, 95–110].

Водночас сама наявність електронного сервісу ще не означає рівного доступу до нього. Для повноцінної участі у цифровому процесі потрібні технічний пристрій, стабільне інтернет-з'єднання, засоби електронної ідентифікації та певний рівень цифрової грамотності. У деяких випадках додатковим бар'єром стає складність процесуального інтерфейсу або необхідність працювати з файлами, електронними підписами та іншими

технічними інструментами. Тому цифровізація може одночасно усувати традиційні перешкоди і створювати нові.

На цю проблему звертає увагу Владислав Бурий, який пропонує оцінювати доступ до правосуддя не як формальну можливість скористатися електронною платформою, а як реальну здатність особи ефективно реалізувати своє право на судовий захист [7, с. 42–49]. Такий підхід видається принципово важливим, оскільки зміщує акцент із самої наявності цифрового сервісу на його фактичну доступність для конкретного користувача.

Ця логіка простежується і в сучасному праві Європейського Союзу. Regulation (EU) 2023/2844 пов'язує цифровізацію судової співпраці із необхідністю дотримання фундаментальних прав, ефективного доступу до правосуддя, права на справедливий суд, недискримінації, приватності та захисту персональних даних [11]. Окремо враховується доступність цифрових систем для осіб з інвалідністю. Отже, цифрова ефективність у європейській моделі не розглядається окремо від процесуальних гарантій.

Подібний користувацько-центричний підхід закладений і в Guidelines on electronic court filing (e-filing) and digitalisation of courts, прийнятих CEPEJ у 2021 році. У них підкреслюється, що система електронного подання повинна бути зрозумілою, передбачуваною та дозволяти користувачеві отримати підтвердження вчиненої дії і встановити статус поданого документа [12]. Особливого значення набуває і реакція системи на технічний збій, оскільки в цифровому процесі саме від коректності технічної фіксації часто залежить збереження процесуального строку або підтвердження факту звернення до суду.

Для України це має безпосередній практичний вимір. У міру розширення обов'язкової електронної комунікації необхідно чітко визначати, який системний запис підтверджує подання документа, який момент має юридичне значення для обчислення строків і яким чином фіксується недоступність сервісу.

На наш погляд, саме правова визначеність таких технічних подій є однією з передумов довіри до електронного правосуддя.

Окремий аспект доступу до правосуддя пов'язаний із публічністю судового розгляду. У традиційному процесі відкритість значною мірою забезпечується можливістю бути фізично присутнім у залі суду. У дистанційному або гібридному форматі цього вже недостатньо, тому виникає потреба в інших механізмах забезпечення відкритості та контролю за перебігом судового засідання. Viljar Peep, аналізуючи естонський досвід digital justice, звертає увагу саме на необхідність узгодження цифрової ефективності із конституційною вимогою публічності правосуддя [29, p. 496–508].

Схожі питання виникають і при використанні відеоконференцій. CEPEJ наголошує, що дистанційний формат не повинен погіршувати можливість особи бути почутою, конфіденційно спілкуватися із представником, стежити за перебігом засідання та реагувати на докази [37]. Відтак якість звуку, стабільність зв'язку, можливість бачити інших учасників і належна організація дистанційного слухання мають не лише технічне, а й процесуальне значення.

Це дозволяє сформулювати важливий висновок: для цифрового судового провадження значення має не формальна наявність підключення до засідання, а функціональна еквівалентність дистанційної участі фізичній присутності. Якщо учасник не може повноцінно чути виступи, ознайомлюватися з матеріалами або конфіденційно комунікувати з представником, дистанційна форма фактично не забезпечує того самого рівня процесуальних гарантій.

Саме тому найбільш переконливою видається не модель повної заміни традиційного судочинства цифровим, а гнучкий підхід, за якого форма участі визначається з урахуванням характеру справи, процесуальної ролі учасника та необхідності безпосереднього дослідження доказів. Такий висновок узгоджується з підходом Richard Susskind, який розглядає онлайн-правосуддя як

спосіб переосмислення доступу до суду, а не як механічне перенесення всіх елементів традиційного процесу в цифрове середовище [1, p. 55–70, 95–110; 2].

Електронне правосуддя неможливе без надійного встановлення того, хто саме вчинив процесуальну дію. У традиційному паперовому процесі цю функцію забезпечують підпис, документи, особиста присутність або підтвердження повноважень представника. У цифровому середовищі ідентифікація стає складнішою, оскільки юридично значуща дія підтверджується сукупністю технологічних і правових механізмів: електронною ідентифікацією, автентифікацією, електронним підписом, реєстраційними даними та технічними записами інформаційної системи.

В українській моделі ключове значення мають кваліфікований електронний підпис та інші засоби електронної ідентифікації. Закон України № 3200-IX пов'язує функціонування електронного кабінету із процедурою електронної ідентифікації користувача [21]. Таким чином, можливість вчинення процесуальної дії в електронній формі безпосередньо залежить від належного підтвердження особи. Водночас розвиток мобільних і хмарних засобів ідентифікації свідчить про необхідність технологічно нейтрального підходу: для права принциповим має бути не конкретний технічний носій, а достатній рівень довіри та можливість достовірно встановити автора юридично значущої дії.

У транскордонному вимірі ця проблема набуває ще більшого значення. Європейська модель електронної ідентифікації та довірчих послуг сформована Regulation (EU) No 910/2014 (eIDAS) і була розвинена Regulation (EU) 2024/1183, яким створено European Digital Identity Framework [38; 39]. Для електронного правосуддя принципово важливе взаємне визнання засобів ідентифікації та довірчих послуг, адже транскордонна взаємодія потребує не лише технічного прийняття документа, а й перевірюваної довіри до його походження та підпису.

Цей підхід отримав подальший розвиток у Regulation (EU) 2023/2844, який закріплює правові наслідки використання електронних підписів, електронних

печаток та електронних документів у межах цифрової судової співпраці [11]. Для України це означає, що гармонізація має охоплювати не лише законодавство про електронні довірчі послуги, а й процесуальні правила перевірки електронного підпису, встановлення його належності та оцінки наслідків його оспорювання.

Питання ідентифікації безпосередньо пов'язане з іншим елементом цифрового процесу – електронними доказами. На відміну від традиційного письмового документа, цифрові дані можуть легко копіюватися, змінюватися, переноситися між різними носіями, а частина відомостей про їх походження та цілісність міститься у метаданих. Саме тому до електронного доказу не завжди можна механічно застосовувати ті самі підходи, що й до паперового документа. О. О. Герасименко, досліджуючи використання доказів у господарському процесі в умовах цифровізації, звертає увагу на проблеми їх допустимості, достовірності та належної процесуальної оцінки [40, с. 71–77].

Подібна проблема простежується і в зарубіжних дослідженнях. Eneli Laurits, аналізуючи цифрові докази у кримінальному процесі Естонії, звертає увагу на необхідність поєднання нових технологічних можливостей роботи з доказовою інформацією із належним захистом фундаментальних прав [41, p. 113–120]. Хоча її дослідження стосується кримінального провадження, сама постановка проблеми має ширше значення: цифровий доказ повинен бути придатним для перевірки його походження, цілісності та контексту, але вимоги до такої перевірки не повинні перетворюватися на непропорційний технічний бар'єр для учасника процесу.

Особливо виразно ця проблема проявляється при використанні інформації з онлайн-платформ, месенджерів, хмарних сервісів та соціальних мереж. У таких випадках суд часто має справу не з електронним документом у традиційному розумінні, а з цифровим об'єктом, зміст і властивості якого можуть змінюватися. Скриншот відтворює видимий зміст, але сам по собі не завжди підтверджує його походження; електронний лист містить технічні заголовки та метадані;

повідомлення у месенджері може бути відредаговане або видалене. Тому оцінка цифрового доказу потребує врахування не лише його змісту, а й способу отримання, технічних характеристик та зв'язку з іншими доказами. [40, с. 71–77; 41, p. 113–120].

Цифрова компетентність суддів і представників у таких умовах набуває нового значення, однак вона не повинна підміняти процесуальні правила. Суддя не має самостійно виконувати функції технічного експерта; у спірних випадках потрібні зрозумілі стандарти оцінки цифрових даних і можливість залучення спеціальних знань.

Водночас доцільно розмежовувати допустимість цифрового доказу та його доказову вагу. Недосконалість технічної форми не завжди означає автоматичну неприйнятність, але може впливати на переконливість доказу у сукупності з іншими матеріалами справи. Такий підхід дозволяє уникнути як надмірного формалізму, так і некритичного прийняття цифрової інформації.

Наступний рівень проблеми виходить уже за межі окремого доказу і стосується взаємодії інформаційних систем. Подальша інтероперабельність українського електронного правосуддя з європейськими механізмами потребуватиме стандартизації не лише форматів документів, а й метаданих та способів їх опису. Дослідження Nadia Carboni і Marco Velicogna та Stefano Signorin показують, що функціонування e-CODEX ґрунтується саме на узгоджених механізмах електронного обміну, які дозволяють різним національним системам правильно інтерпретувати передані дані [25, p. 104–120; 27, p. 603–620].

Для України це означає поступовий перехід від моделі, у якій електронний процес зводиться переважно до передавання файла, до роботи зі структурованими юридично значущими даними. Якщо відомості про сторони, судовий збір, процесуальний статус документа та інші реквізити передаються у стандартизованій формі, вони можуть автоматично використовуватися на

наступних етапах провадження без повторного введення. Це зменшує кількість ручних операцій і ризик технічних помилок.

Водночас структуризація не повинна перетворювати процесуальний документ на набір жорстко заданих полів, які обмежують можливість сторони сформулювати складну правову позицію. Тому найбільш перспективною видається комбінована модель, за якої структуровані дані забезпечують автоматизований обмін і внутрішню обробку інформації, а повнотекстові документи зберігають можливість повного викладення юридичних аргументів. Чим глибше правосуддя інтегрується у цифрову інфраструктуру, тим менш переконливим стає сприйняття кібербезпеки як суто технічного питання. Недоступність інформаційної системи, втрата або пошкодження даних, несанкціонований доступ до матеріалів справи здатні безпосередньо впливати на реалізацію права на судовий захист. Тому в цифровому судочинстві кібербезпека набуває не лише організаційного, а й процесуального значення.

Для України ця проблема має особливу гостроту. Судова інфраструктура функціонує в умовах підвищених кіберризиків, а вимоги до захищеного зберігання, обміну та обробки інформації прямо закріплені у нормативному регулюванні ЄСІТС [22]. Однак сама наявність таких вимог не гарантує стійкості системи. Практичне значення мають резервування даних, контроль доступу, аудит операцій і здатність швидко відновити роботу після інциденту. У цьому сенсі цифрова стійкість стає однією з передумов безперервності правосуддя.

Із питанням кібербезпеки безпосередньо пов’язаний захист персональних даних. Судові матеріали можуть містити відомості про стан здоров’я, сімейні відносини, дітей, майновий стан, банківську або комерційну таємницю, а в окремих категоріях справ – інформацію, розголошення якої може завдати особі істотної шкоди. Цифрова форма робить такі дані значно придатнішими до копіювання, пошуку та автоматизованої обробки. Саме тому принципи законності, прозорості, цільового використання, мінімізації даних та обмеження

їх обробки мають враховуватися вже на етапі проектування цифрової судової системи. У праві Європейського Союзу ці вимоги безпосередньо випливають із Regulation (EU) 2016/679 (General Data Protection Regulation), зокрема зі ст. 5, яка закріплює основні принципи обробки персональних даних [42]. Regulation (EU) 2023/2844, своєю чергою, прямо пов'язує цифровізацію судової співпраці з необхідністю дотримання права на захист персональних даних [11].

Особливо складно знайти баланс між захистом приватності та принципом відкритості правосуддя. Публікація судових рішень є важливою гарантією прозорості, однак цифрові реєстри створюють можливість масового пошуку, агрегування та автоматизованого аналізу відомостей, які раніше були формально відкритими, але фактично складнодоступними. Саме тому CEPEJ у Guidelines on the online publication of judicial decisions звертає увагу на необхідність узгодження публічності судової практики із захистом приватності та належною анонімізацією [43].

Для України це має особливе значення через масштаб Єдиного державного реєстру судових рішень та зростання можливостей автоматизованого аналізу судової практики. Формальне вилучення прізвища чи інших очевидних ідентифікаторів не завжди виключає повторну ідентифікацію особи, якщо сукупність фактичних обставин залишається унікальною. Тому подальший розвиток цифрових аналітичних інструментів, у тому числі із застосуванням штучного інтелекту, потребуватиме більш складного підходу до анонімізації, ніж просте приховування окремих персональних даних.

Інший вимір довіри до електронного правосуддя пов'язаний із можливістю користувача простежити юридично значущу цифрову дію. Особа не повинна знати внутрішню технічну архітектуру системи, однак має мати змогу встановити, чи було документ подано, коли саме він надійшов, чи підтверджено його доставку та чи виникла технічна помилка. У цьому сенсі підтвердження

подання, журнали доставки та інші системні записи виконують функцію цифрових процесуальних слідів.

Показовим у цьому контексті є e-CODEX. Nadia Carboni та Marco Velicogna, аналізуючи електронний обмін даними у європейському правосудді, звертають увагу не лише на сам факт передавання інформації, а й на необхідність надійної та контрольованої взаємодії між різними системами [25, p. 104–120]. European e-Justice Portal також передбачає інформування користувача про результат передачі документа або її невдачу в процедурах, що використовують e-CODEX [44]. Такий підхід демонструє, що в електронному процесі технічне підтвердження може мати самостійне юридичне значення.

Узагальнення цих вимог дозволяє запропонувати для цілей цього дослідження принцип, який умовно можна визначити як process guarantees by design: підтвердження юридично значущих дій, контроль доступу, збереження доказової історії, захист персональних даних і механізми реагування на технічні інциденти мають закладатися в цифрову архітектуру ще на етапі її проектування [11; 12; 43; 42].

Окремим, але не центральним для дослідження питанням є використання штучного інтелекту. Regulation (EU) 2024/1689 відносить окремі AI-системи, призначені для допомоги судовим органам у дослідженні й тлумаченні фактів і права та застосуванні права до конкретних обставин, до категорії високого ризику [45]. Галина Заболотна також пов’язує перспективи використання ШІ в адміністративному судочинстві України з ризик-орієнтованим підходом і людським наглядом [46, с. 182–192]. Для судів найбільш прийнятною видається модель assisted justice: алгоритмічні інструменти можуть допомагати у пошуку, класифікації, транскрибуванні чи узагальненні матеріалів, але юридична оцінка, мотивування рішення та відповідальність за нього мають залишатися за суддею. Така логіка відповідає і рекомендаціям CEPEJ щодо генеративного ШІ [47; 45].

## 2.5. Напрями розвитку та критерії ефективності електронного правосуддя в Україні

Проведений порівняльний аналіз показує, що Україна та Європейський Союз рухаються в одному напрямі цифрової трансформації правосуддя, але виходять із різних інституційних передумов. Українська модель орієнтована насамперед на створення єдиного національного цифрового середовища судової влади, тоді як європейська значною мірою формується навколо інтероперабельності національних систем, транскордонного обміну та взаємного визнання цифрових юридичних дій. Саме тому перспективу розвитку ЄСІТС доцільно пов'язувати не з механічним запозиченням окремих європейських рішень, а з поступовим поєднанням внутрішньої інтегрованості та зовнішньої сумісності.

Першочергового значення в цьому контексті набуває завершення переходу від електронного обміну документами до повноцінної електронної справи. Досвід Австрії показує переваги моделі, у якій зовнішнє електронне подання безпосередньо інтегрується з внутрішньою системою роботи суду [33; 34], тоді як естонська практика демонструє ефективність ширшої міжвідомчої інтеграції та повторного використання структурованих даних [29, p. 496–508; 30]. Для України це означає, що подальший розвиток «Електронного суду» має оцінюватися не лише за кількістю доступних сервісів, а й за тим, наскільки вони усувають дублювання, ручне перенесення інформації та паралельне існування електронної і паперової справи.

Логічним продовженням цього процесу є розвиток інтероперабельності. e-CODEX у цьому сенсі становить важливий орієнтир не як програмне рішення, яке необхідно буквально відтворити, а як модель взаємодії автономних інформаційних систем через узгоджені стандарти та довірені канали обміну [3, p. 274–294; 25, p. 104–120; 27, p. 603–620; 24]. У перспективі це потребуватиме

від України сумісності форматів документів, метаданих, засобів електронної ідентифікації та довірчих послуг із європейською цифровою інфраструктурою.

Однак технологічна сумісність має сенс лише тоді, коли вона не послаблює процесуальні гарантії. У міру розширення обов'язкової електронної комунікації особливого значення набувають юридичні наслідки технічних збоїв, момент подання документа та доказове значення системних повідомлень. На наш погляд, кожна юридично значуща електронна дія повинна залишати стандартизований цифровий слід, який дозволяє встановити час подання, результат доставки та можливу технічну помилку. Такий механізм зменшує потребу дублювати електронне звернення паперовим і водночас захищає користувача від негативних наслідків несправності системи.

Не менш важливо зберегти баланс між цифровою ефективністю та доступністю. Обов'язкова електронна комунікація є виправданою для професійних учасників, однак щодо фізичних осіб повна відмова від альтернативного каналу може створити непропорційний бар'єр. Тому розвиток цифрового правосуддя має орієнтуватися не лише на принцип digital by default, а й на фактичну можливість конкретної особи скористатися судовим захистом. Це передбачає доступність інтерфейсу, зрозумілі процесуальні форми, адаптацію для осіб з інвалідністю та можливість отримати допомогу у випадках, коли цифрова взаємодія об'єктивно ускладнена.

Водночас успішність цифровізації не може вимірюватися лише кількістю електронних кабінетів, поданих онлайн-документів або запущених модулів. Значно важливішими є практичні результати: чи скорочується кількість дій, необхідних для звернення до суду; чи зменшується адміністративне навантаження; чи стає зрозумілішим процесуальний статус електронної дії; як часто виникають технічні інциденти і наскільки швидко система відновлюється після них.

Особливого значення набуває й те, чи спрощує цифровізація роботу користувача, а не переносить на нього адміністративні функції суду. Якщо електронне звернення потребує багаторазового введення одних і тих самих даних, конвертації документів або дублювання їх на папері, формальна наявність цифрового сервісу ще не свідчить про його ефективність. Зрілою можна вважати систему, яка використовує вже наявні структуровані дані, автоматизує технічні операції та дозволяє учасникам і працівникам суду зосередитися на юридично значущих діях.

Саме тому оцінювання цифрової трансформації має спиратися на вимірювані й публічні показники. До них можуть належати стабільність роботи сервісів, частота технічних збоїв, середній час обробки електронних звернень, кількість документів, повернутих з технічних причин, рівень використання дистанційних процедур та фактичне скорочення адміністративного навантаження. Регулярне оприлюднення таких даних дозволило б оцінювати розвиток ЄСІТС не за кількістю нових функцій, а за їхнім впливом на доступність і якість правосуддя.

У підсумку критерієм успішності електронного правосуддя має бути не ступінь «безпаперовості» суду, а якість здійснення правосуддя. Цифрова система є справді ефективною тоді, коли особі простіше реалізувати право на судовий захист, судді – працювати з матеріалами справи, а державі – забезпечувати стабільне, безпечне та прозоре функціонування судової влади. У цьому сенсі цифровізація повинна не просто переносити традиційні процедури в електронне середовище, а переосмислювати їх так, щоб технологія зменшувала, а не відтворювала існуючі процесуальні бар’єри. Саме такий трансформаційний підхід відповідає загальній логіці, яку Richard Susskind пов’язує з майбутнім онлайн-правосуддя [1, p. 55–70, 95–110; 2].

Електронне правосуддя є одним із найбільш показових прикладів того, як цифрові технології змінюють не лише інструменти діяльності держави, а й саму

логіку юридичної процедури. Проведений аналіз дає підстави стверджувати, що сучасна цифровізація судочинства поступово виходить за межі допоміжної автоматизації окремих операцій. Йдеться про формування самостійної регуляторної моделі, у якій юридичного значення набувають спосіб ідентифікації користувача, форма передавання та фіксації даних, підтвердження процесуальної дії, правила доступу до інформації, архітектура цифрової системи та межі використання алгоритмічних інструментів.

Порівняння українського та європейського підходів показало, що вони формуються за різних інституційних умов, але поступово зближуються за основними напрямами розвитку. Українська модель має перевагу у вигляді централізованої побудови ЄСІТС та швидкого поширення електронної взаємодії з учасниками процесу. Водночас її подальша ефективність залежить від того, наскільки зовнішні цифрові сервіси будуть поєднані з повноцінною внутрішньою електронною справою і безперервним рухом структурованих даних у межах усього судового провадження.

Європейська модель, навпаки, розвивається в умовах збереження автономності національних судових систем, тому її ключовим принципом стала інтероперабельність. Досвід e-CODEX та Regulation (EU) 2023/2844 показує, що цифрова інтеграція не потребує повної уніфікації внутрішніх систем. Значно важливішими є узгоджені стандарти електронної ідентифікації, довірчих послуг, форматів документів, метаданих, підтвердження доставки та безпечного обміну інформацією. Для України саме такий підхід може стати основою майбутньої сумісності ЄСІТС із європейським цифровим простором правосуддя.

Практика Естонії, Австрії та Німеччини додатково підтверджує, що універсальної моделі цифровізації суду не існує. Естонський досвід демонструє переваги інтеграції правосуддя у загальну цифрову інфраструктуру держави, австрійський – ефективність довготривалого стандартизованого електронного обігу, а німецький – значення поступового нормативного впровадження окремих

компонентів e-justice. Спільним для цих моделей є те, що електронний канал перестає бути факультативним доповненням до традиційного процесу і стає елементом його системної організації.

Водночас проведений аналіз показує, що цифровізація правосуддя не повинна оцінюватися за принципом «чим більше технологій, тим краще». Технологічна ефективність має сенс лише тоді, коли вона не послаблює фундаментальні процесуальні гарантії. Доступність суду, рівність учасників, публічність, конфіденційність, захист персональних даних, можливість оскарження технічної помилки та збереження незалежного суддівського контролю повинні залишатися визначальними орієнтирами будь-якої цифрової трансформації.

Саме тому для розвитку електронного правосуддя в Україні доцільно виходити із запропонованого в цьому дослідженні принципу process guarantees by design. Його зміст полягає в тому, що процесуальні гарантії мають враховуватися не після виникнення технічних проблем або судових спорів, а ще на етапі проектування цифрової системи. Механізми підтвердження юридично значущих дій, контроль доступу, збереження доказової історії, реагування на технічні збої, захист персональних даних і можливість людського контролю повинні бути частиною самої архітектури електронного правосуддя.

З огляду на це перспективна модель електронного правосуддя для України має поєднувати три взаємопов’язані якості: внутрішню цілісність, зовнішню інтероперабельність і людиноцентричність. Внутрішня цілісність означає безперервний електронний життєвий цикл справи та мінімізацію дублювання інформації; зовнішня інтероперабельність – здатність взаємодіяти з іншими державними та європейськими системами; людиноцентричність – орієнтацію цифрових процедур на реальну можливість особи ефективно реалізувати право на судовий захист.

Успішність такої моделі повинна визначатися не кількістю запроваджених модулів і не формальним рівнем «безпаперовості» суду, а практичним результатом цифрової трансформації. Йдеться про те, чи стає шлях від звернення до суду до отримання та виконання судового рішення більш передбачуваним, доступним, безпечним і справедливим. Саме за цієї умови цифровізація перестає бути технічним оновленням судової системи і перетворюється на інструмент підвищення якості правосуддя.

Таким чином, європейська інтеграція у сфері електронного правосуддя для України має розглядатися не як необхідність копіювання окремих технічних рішень, а як поступове наближення до спільних стандартів довіри, інтероперабельності та захисту прав. Такий підхід дозволяє зберегти національну архітектуру ЄСІТС і водночас розвивати її як відкриту, стійку та сумісну з європейським правовим простором систему цифрового правосуддя.

***Висновки до Розділу 2***

Проведене дослідження засвідчує, що цифрова трансформація правосуддя поступово виходить за межі технічної модернізації судової діяльності та набуває ознак самостійної регуляторної моделі. Її зміст визначається не лише використанням електронних сервісів, а й нормативним закріпленням електронної процесуальної форми, цифрової ідентифікації, способів подання та вручення документів, доступу до матеріалів справи, взаємодії інформаційних систем і юридичних наслідків цифрових дій. За таких умов технологічна архітектура безпосередньо впливає на реалізацію процесуальних прав і тому має розвиватися у нерозривному зв’язку з вимогами справедливого судочинства.

Порівняння української та європейської моделей електронного правосуддя виявило відмінність їх інституційної логіки. Українська модель орієнтована передусім на формування єдиного національного цифрового середовища судової влади на основі ЄСІТС, тоді як модель Європейського Союзу ґрунтується на збереженні автономності національних систем та забезпеченні їх транскордонної

інтероперабельності. Водночас відмінність організаційних підходів не виключає їх поступового зближення у частині електронної ідентифікації, довірчих послуг, структурованого обміну даними, захисту персональних даних та гарантування доступу до правосуддя.

Українська модель електронного правосуддя пройшла значний шлях від запровадження окремих цифрових сервісів до нормативного закріплення електронного кабінету як основного середовища процесуальної взаємодії для окремих категорій учасників. Водночас її подальший розвиток потребує переходу від фрагментарної цифровізації окремих процесуальних дій до формування цілісного електронного життєвого циклу судової справи. Електронне подання документа, його реєстрація, передавання судді, формування матеріалів справи, повідомлення учасників та архівування повинні функціонувати як елементи єдиного інформаційного процесу без необґрунтованого дублювання даних і паралельного відтворення паперових процедур.

Європейський досвід підтверджує, що ефективність цифрового правосуддя не потребує повної уніфікації національних судових інформаційних систем. Визначальне значення має їх здатність взаємодіяти на основі спільних стандартів електронної ідентифікації, довірчих послуг, форматів документів, метаданих та безпечного обміну інформацією. Досвід Естонії, Австрії та Німеччини водночас демонструє різні, але функціонально сумісні напрями цифрової трансформації: інтеграцію судової системи у загальнодержавну цифрову інфраструктуру, стандартизацію професійного електронного обігу та послідовне нормативне впровадження електронної справи. Для України доцільним є не механічне запозичення окремої моделі, а використання відповідних підходів з урахуванням особливостей національної судової системи.

Встановлено, що цифровізація правосуддя повинна оцінюватися насамперед через здатність забезпечувати належний рівень процесуальних

гарантій. Електронна форма не може звужувати доступ до суду, порушувати рівність учасників, обмежувати можливість бути почутим, конфіденційно спілкуватися з представником або ефективно реагувати на докази. Тому пріоритетність цифрової взаємодії має поєднуватися з фактичною доступністю відповідних сервісів, урахуванням цифрової нерівності та збереженням альтернативних способів взаємодії для осіб, які з об'єктивних причин не можуть повноцінно користуватися електронними інструментами.

Особливого значення в цифровому судочинстві набувають правова визначеність електронної ідентифікації, правила роботи з цифровими доказами, інформаційна безпека та захист персональних даних. Юридично значущі електронні дії повинні бути достовірно зафіксовані, а користувач повинен мати можливість встановити час подання документа, факт його доставки, виникнення технічної помилки та інші обставини, здатні впливати на процесуальні наслідки. З огляду на це кібербезпека, фіксація операцій, резервування даних, контроль доступу та можливість відновлення системи мають розглядатися не лише як технічні вимоги, а як складові забезпечення безперервності й надійності правосуддя.

Обґрунтованим є запропонований у розділі підхід process guarantees by design, відповідно до якого процесуальні гарантії повинні закладатися безпосередньо в архітектуру цифрової судової системи ще на етапі її проектування. Підтвердження юридично значущих дій, збереження цифрової доказової історії, захист персональних даних, контроль доступу, реагування на технічні інциденти та можливість людського контролю за алгоритмічними інструментами мають становити внутрішні характеристики електронного правосуддя, а не компенсаторні механізми, що застосовуються вже після виникнення порушень.

Таким чином, перспективна модель електронного правосуддя в Україні має поєднувати внутрішню цілісність цифрової судової інфраструктури, її зовнішню

інтероперабельність та людиноцентричну спрямованість. Результативність цифрової трансформації доцільно визначати не кількістю впроваджених сервісів чи ступенем відмови від паперових документів, а тим, наскільки цифрові інструменти спрощують реалізацію права на судовий захист, зменшують адміністративне навантаження, забезпечують стабільність і передбачуваність процесу та підвищують якість здійснення правосуддя. Саме за такого підходу цифровізація судової системи може розглядатися не як самоціль, а як інструмент удосконалення правосуддя та поступової інтеграції України до європейського цифрового правового простору.

## Список використаних джерел

1. Susskind R. Online Courts and the Future of Justice. Oxford : Oxford University Press, 2019. 368 p. DOI: 10.1093/oso/9780198838364.001.0001. URL: https://academic.oup.com/oxford-law-pro/book/41081.

2. Susskind R. The Future of Courts. The Practice. Harvard Law School Center on the Legal Profession. 2020. July/August. URL: https://clp.law\.harvard.edu/knowledge-hub/magazine/issues/remote-courts/the-future-of-courts/.

3. Velicogna M., Steigenga E., Taal S., Schmidt A. Connecting EU Jurisdictions: Exploring How to Open Justice Across Member States Through ICT. Social Science Computer Review. 2020. Vol. 38, no. 3. P. 274–294. DOI: 10.1177/0894439318786949. URL: https://journals.sagepub.com/doi/10.1177/0894439318786949.

4. Reiling D., Contini F. E-Justice Platforms: Challenges for Judicial Governance. International Journal for Court Administration. 2022. Vol. 13, no. 1. Article 6. DOI: 10.36745/ijca.445. URL: https://iacajournal.org/articles/10.36745/ijca.445.

5. Єрмакова Г. С. Конституційно-правові гарантії права на справедливий суд за умов цифровізації правосуддя та воєнного стану. Київський юридичний

журнал. 2026. № 9. С. 15–27. DOI: 10.32782/klj-2026-9.02. URL: https://journals.fpk.kyiv.ua/index.php/kyivlawjournal/article/view/91.

6. Сотула О. С. Організація судочинства в умовах воєнного стану: правові засади, цифрова трансформація та доступ до правосуддя в Україні. Науковий вісник Херсонського державного університету. Серія «Юридичні науки». 2026. № 2. С. 53–57. DOI: 10.32999/ksu2307-8049/2026-2-8. URL: https://lj.journal.kspu.edu/index.php/lj/article/view/514.

7. Бурий В. Право на доступ до правосуддя в умовах розвитку цифрових засобів. Наукові записки НаУКМА. Юридичні науки. 2026. Т. 17. С. 42–49. DOI: 10.18523/2617-2607.2026.17.42-49. URL: https://nrplaw\.ukma.edu.ua/article/view/366564.

8. Крикун В. Б. Трансформація цивільного процесу в умовах цифровізації правосуддя. Сучасна доктрина права. 2026. № 2(96). С. 72–79. DOI: 10.25313/2520-2308-2026-2-11935. URL: https://doi.org/10.25313/2520-2308-2026-2-11935.

9. Luchenko D. V., Piatyhora K. V. From Concept to Reality: UJICS as the Next Stage in the Development of E-Justice in Ukraine. Theory and Practice of Jurisprudence. 2025. No. 2(28). P. 66–81. DOI: 10.21564/2225-6555.2025.28.346098. URL: https://tlaw\.nlu.edu.ua/article/view/346098.

10. Парасюк В. М., Онишко О. Б., Бориславський Р. А. Теоретико-правові засади електронного судочинства в цивільному процесі України: сучасні виклики. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2025. Вип. 1. С. 3–10. DOI: 10.32782/2311-8040/2025-1-1. URL: https://journals.lvduvs.lviv.ua/index.php.

11. Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters and amending certain acts in the

field of judicial cooperation. Official Journal of the European Union. 2023. L, 2023/2844. URL: https://eur-lex.europa.eu/eli/reg/2023/2844/oj.

12. European Commission for the Efficiency of Justice (CEPEJ). Guidelines on electronic court filing (e-filing) and digitalisation of courts. CEPEJ(2021)15. Strasbourg, 9 December 2021. URL: https://www\.coe.int/en/web/cepej/cyberjustice-and-artificial-intelligence-used-in-the-field-of-justice.

13. Onţanu E. A. e-Justice Governance in the EU. E-Governance in the European Union: Strategies, Tools, and Implementation / ed. by D. R. Troitiño. Cham : Springer, 2024. P. 243–258. DOI: 10.1007/978-3-031-56045-3_16. URL: https://research.tilburguniversity.edu/en/publications/e-justice-governance-in-the-eu/.

14. Скочиляс-Павлів О. Цифрова трансформація правосуддя в Україні: виклики та перспективи. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2026. Т. 13, № 1(49). С. 337–343. DOI: 10.23939/law2026.49.337. URL: https://science.lpnu.ua/uk/law/vsi-vypusky/vypusk-13-nomer-1-49-2026/cyfrova-transformaciya-pravosuddya-v-ukrayini-vyklyky-ta.

15. Логойда В. М. Проблеми цифровізації судочинства в Україні. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 92, т. 5. С. 35–42. DOI: 10.24144/2307-3322.2025.92.5.4. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/350486.

16. Сімакова С. І., Клочко В. М. Електронний суд як інструмент сучасного правосуддя: досвід, труднощі та перспективи розвитку. Аналітично-порівняльне правознавство. 2026. Т. 2, № 2. С. 238–243. DOI: 10.24144/2788-6018.2026.02.2.38. URL: https://journal-app.uzhnu.edu.ua/article/view/357642.

17. Мелянчук М. Цифровізація цивільного судочинства: новели та перспективи. Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. 2025. Т. 129, № 1. С. 38–44. DOI: 10.17721/1728-2195/2025/1.129-7. URL: https://legal.bulletin.knu.ua/uk/article/view/3639.

18. Горішня А. М. Електронне судочинство України: сучасний стан та тенденції розвитку. Аналітично-порівняльне правознавство. 2025. № 6, ч. 1. С. 308–312. DOI: 10.24144/2788-6018.2025.06.1.45. URL: https://journal-app.uzhnu.edu.ua/article/view/346030.

19. Про внесення змін до деяких законодавчих актів України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи: Закон України від 27.04.2021 № 1416-IX. URL: https://zakon.rada.gov.ua/laws/show/1416-20#Text.

20. Про затвердження Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи : рішення Вищої ради правосуддя від 17.08.2021 № 1845/0/15-21. URL: https://zakon.rada.gov.ua/rada/show/v1845910-21#Text.

21. Про внесення змін до деяких законодавчих актів України щодо обов'язкової реєстрації та використання електронних кабінетів в Єдиній судовій інформаційно-телекомунікаційній системі або її окремій підсистемі (модулі), що забезпечує обмін документами : Закон України від 29.06.2023 № 3200-IX. URL: https://zakon.rada.gov.ua/laws/show/3200-20#Text.

22. Про затвердження Змін до Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи : рішення Вищої ради правосуддя від 13.01.2026 № 26/0/15-26. URL: https://zakon.rada.gov.ua/rada/show/v0026910-26#Text.

23. European e-Justice Portal. Online processing of cases and e-communication with courts. URL: https://e-justice.europa.eu/280/EN.

24. Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726. Official Journal of the European Union. 2022. L 150. P. 1–19. URL: https://eur-lex.europa.eu/eli/reg/2022/850/oj

25. Carboni N., Velicogna M. Electronic Data Exchange within European Justice: A Good Opportunity? International Journal for Court Administration. 2012. Vol. 4, no. 3. P. 104–120. DOI: 10.18352/ijca.90. URL: https://doaj.org/article/765fa9a7a1534322a697ca1c90596485.

26. Pangalos G., Salmatzidis I., Pagkalos I. Using IT to Provide Easier Access to Cross-Border Legal Procedures for Citizens and Legal Professionals – Implementation of a European Payment Order e-CODEX Pilot. International Journal for Court Administration. 2014. Vol. 6, no. 2. P. 43–52. DOI: 10.18352/ijca.137. URL: https://iacajournal.org/articles/10.18352/ijca.137.

27. Signorin S. Digitalisation of judicial cooperation in civil and commercial matters within the European Union: Cross-border taking of evidence through the prism of decentralised IT platform e-CODEX. Cuadernos de Derecho Transnacional. 2024. Vol. 16, no. 1. P. 603–620. DOI: 10.20318/cdt.2024.8437. URL: https://e-revistas.uc3m.es/index.php/CDT/en/article/view/8437.

28. Gascón Inchausti F. The new regulation on the digitalisation of judicial cooperation in the European Union: something old, something new, something borrowed and something blue. ERA Forum. 2024. Vol. 24. P. 535–552. DOI: 10.1007/s12027-024-00782-z. URL: https://link.springer.com/article/10.1007/s

29. Peep V. Digital Justice in Estonia. The Cambridge Handbook of AI and Technologies in Courts / ed. by M. Zalnieriute, A. Limante. Cambridge : Cambridge University Press, 2026. P. 496–508. DOI: 10.1017/9781009744225.039. URL: https://www\.cambridge.org/core/books.

30. Centre of Registers and Information Systems. Introduction to E-File. Registrite ja Infosüsteemide Keskus. URL: https://www\.rik.ee/en/e-file/introduction-e-file.

31. Ярошенко О. А., Соколова І. О. Цифрова трансформація правової системи України: роль платформи «Дія» та електронного суду. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 92, ч. 1. С.

151–156. DOI: 10.24144/2307-3322.2025.92.1.21. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/350067.

32. Bundesministerium für Justiz. Elektronischer Rechtsverkehr (ERV). Wien: Bundesministerium für Justiz. URL: https://www\.justiz.gv.at/html/default/2c9484852308c2a60123708554d203e7.de.html

33. Constitutional Court of Austria. E-Government at a Glance. URL: https://www\.vfgh.gv.at/service/e-government/e-government_at_a_glance.en.html.

34. Constitutional Court of Austria. Electronic Filing. URL: https://www\.vfgh.gv.at/service/e-government/electronic_filing.en.html.

35. Bundesministerium der Justiz und für Verbraucherschutz. Digitalisierung der Justiz. Berlin : Bundesministerium der Justiz und für Verbraucherschutz. URL: https://www\.bmj.de/DE/themen/digitales/digitalisierung_justiz/digitalisierung_justiz_node.html (дата звернення: 30.08.2026).

36. Bundesrechtsanwaltskammer. beA & ERV: besonderes elektronisches Anwaltspostfach und elektronischer Rechtsverkehr. URL: https://www\.brak.de/anwaltschaft/bea-erv.

37. European Commission for the Efficiency of Justice (CEPEJ). Guidelines on videoconferencing in judicial proceedings. CEPEJ(2021)4. Strasbourg, 17 June 2021 ; Guide on the Use and Development of Remote Hearings. CEPEJ(2025)3. Strasbourg, 5 June 2025. URL: https://www\.coe.int/en/web/cepej/cyberjustice-and-artificial-intelligence-used-in-the-field-of-justice.

38. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union. 2014. L 257. P. 73–114. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

39. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. 2024. L, 2024/1183, 30 April 2024. URL: [https://eur-lex.europa.eu/eli/reg/2024/1183/oj](https://eur-lex.europa.eu/eli/reg/2024/1183/oj).

40. Герасименко О. О. Актуальні проблеми використання доказів у господарському процесі, зокрема в умовах цифровізації правосуддя та розвитку електронних технологій. Legal Bulletin. 2026. № 2(20). С. 71–77. DOI: 10.31732/2708-339X-2026-20-A9. URL: https://lbku.krok.edu.ua/index.php/legal-bulletin/article/view/619.

41. Laurits E. Criminal procedure and digital evidence in Estonia. Digital Evidence and Electronic Signature Law Review. 2016. Vol. 13. P. 113–120. DOI: 10.14296/deeslr.v13i0.2301. URL: https://journals.sas.ac.uk/deeslr/article/view/2301.

42. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

43. European Commission for the Efficiency of Justice (CEPEJ). Guidelines on the online publication of judicial decisions. Strasbourg, 2024. URL: https://www\.coe.int/en/web/cepej/cyberjustice-and-artificial-intelligence-used-in-the-field-of-justice.

44. European e-Justice Portal. Legal notice: electronic submission of claims using e-CODEX. URL: https://e-justice.europa.eu/.

45. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU)

2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union. 2024. L, 2024/1689, 12 July 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

46. Заболотна Г. Штучний інтелект в адміністративному судочинстві: класифікація ризиків, людський нагляд та перспективи імплементації в Україні. Вісник Львівського університету. Серія юридична. 2026. Вип. 82. С. 182–192. DOI: 10.30970/vla.2026.82.182. URL: https://publications.lnu.edu.ua/bulletins/index.php/law/article/view/14154.

47. European Commission for the Efficiency of Justice (CEPEJ). Information Note on the Use of Generative Artificial Intelligence by Judicial Professionals. 2024 ; Guidelines on the Use of Generative Artificial Intelligence for Courts. CEPEJ(2025)18Final. Strasbourg, 19 December 2025. URL: https://www\.coe.int/en/web/cepej/cyberjustice-and-artificial-intelligence-used-in-the-field-of-justice.

# РОЗДІЛ 3

# ЦИФРОВА ТРАНСФОРМАЦІЯ МІЖНАРОДНОГО ПРАВА: ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЦИФРОВИХ ДОКАЗІВ НА СУЧАСНЕ МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ

Автор: ***Карвацька Світлана Богданівна,*** *доктор юридичних наук, професор, в.о. завідувача кафедри міжнародного права та порівняльного правознавства Чернівецький національний університет імені Юрія Федьковича*

## 3.1. Цифровізація міжнародно-правового простору та трансформація традиційних моделей правового регулювання

Цифровізація міжнародно-правового простору вже не може розглядатися виключно як технологічний супровід глобалізаційних процесів. Вона перетворилася на самостійний фактор еволюції міжнародного права, який впливає на зміст його принципів, механізми реалізації норм та інструменти міжнародного правозастосування. Як наслідок, класичні концепції доказування, автентичності, допустимості та належності доказів потребують концептуального оновлення з урахуванням особливостей цифрового середовища, що відкриває новий етап розвитку міжнародно-правової доктрини [1].

Особливого значення набуває впровадження систем штучного інтелекту, технологій аналізу великих масивів даних, цифрових платформ і засобів автоматизованого прийняття рішень, які дедалі активніше використовуються у сферах міжнародної безпеки, дипломатії, міжнародного правосуддя та захисту прав людини. Такі процеси зумовлюють необхідність переосмислення традиційних підходів міжнародного права, оскільки чинні міжнародно-правові механізми не завжди здатні забезпечити належне врегулювання нових цифрових явищ, визначити межі відповідальності суб'єктів міжнародного права та

гарантувати дотримання фундаментальних принципів законності, суверенної рівності держав і верховенства права.

Децентралізований характер кіберпростору істотно ускладнює встановлення суб'єктів, відповідальних за здійснення кібератак, а також визначення належної юрисдикції. Унаслідок цього притягнення винних осіб до відповідальності залишається складним завданням у межах чинних міжнародно-правових механізмів [2, с. 875].

Особливу роль у цих процесах відіграє стрімке впровадження систем штучного інтелекту, алгоритмів машинного навчання, технологій аналізу великих масивів даних (Big Data), автоматизованих систем підтримки прийняття рішень та інших цифрових інструментів. Їх використання суттєво змінює механізми міжнародного правозастосування на всіх його етапах – від виявлення потенційних порушень міжнародного права та фіксації відповідних фактів до їх цифрової верифікації, юридичної кваліфікації, оцінки доказового матеріалу і прийняття остаточних рішень міжнародними судовими чи квазісудовими органами. Таким чином, цифрові технології дедалі активніше інтегруються у процес реалізації міжнародного права, змінюючи його процедурні та інституційні засади.

Варто відзначити дослідницький висновок, що в умовах збройних конфліктів «кібертаки є інструментом впливу, який також активно виступає елементом спеціальних розвідувальних операцій для маніпулювання населенням та дискредитації України як держави» [3]. Саме тому сучасний розвиток міжнародного права потребує не фрагментарної адаптації окремих процедур, а комплексного концептуального переосмислення підходів до доказування, процедурної справедливості, юридичної визначеності та меж міжнародно-правового регулювання в умовах цифрової трансформації.

У дослідженнях наголошується, що «військова агресія рф проти України призвела до посилення трансатлантичної співпраці та координації з метою

запобігання, виявлення та реагування на зловмисну кібердіяльність» [4]. Для України дослідження цифрової трансформації міжнародного права має не лише теоретичне, а й безпосереднє практичне значення в умовах широкого використання цифрових технологій для документування міжнародних злочинів, фіксації порушень міжнародного гуманітарного права та збирання доказової бази для міжнародних судових процесів [5]. Саме тому комплексне дослідження впливу штучного інтелекту й цифрових доказів на розвиток сучасного міжнародно-правового регулювання є своєчасним, науково значущим і перспективним напрямом розвитку міжнародно-правової доктрини, здатним сприяти формуванню нових концептуальних підходів до адаптації міжнародного права до викликів цифрової епохи.

Цифрова трансформація являє собою комплексний процес інтеграції сучасних цифрових технологій, зокрема мережевих платформ, систем штучного інтелекту, великих масивів даних та інших інноваційних рішень, у практично всі сфери суспільного життя. Її вплив охоплює комунікацію, міжнародну торгівлю, державне управління, економічні процеси та соціальну взаємодію, докорінно змінюючи способи створення, обробки й поширення інформації. Для міжнародного права ці процеси мають принципове значення, оскільки цифрове середовище формує нові види транскордонних відносин, які дедалі важче регулювати за допомогою традиційних правових підходів.

На відміну від класичних міжнародно-правових моделей, що історично ґрунтувалися на принципах територіальної юрисдикції та державного суверенітету, сучасні цифрові процеси мають глобальний характер і не обмежуються державними кордонами. Це особливо проявляється у сфері міжнародного обігу даних, використання технологій штучного інтелекту, електронної комерції та цифрових послуг, де виникають численні колізії між національними правовими режимами. Відмінності у законодавчих підходах окремих держав до регулювання цифрових технологій ускладнюють вироблення

узгоджених правил поведінки та сприяють подальшій фрагментації міжнародного правового простору.

Додатковим викликом є те, що значна частина сучасних міжнародних інституцій і договірних механізмів створювалася в умовах, коли цифрова економіка ще не визначала глобальні процеси. Зокрема, окремі міжнародні організації, серед яких і Світова організація торгівлі, стикаються з обмеженими можливостями ефективного врегулювання питань, пов'язаних із цифровою торгівлею, транскордонними потоками даних та новими цифровими бізнес-моделями. У зв'язку з цим подальший розвиток міжнародного права потребує не лише оновлення матеріально-правових норм, а й модернізації міжнародних інституцій та механізмів співробітництва. Лише такий комплексний підхід дасть змогу усунути наявні прогалини у правовому регулюванні, зменшити нормативні суперечності між державами та сформувати ефективну систему міжнародного управління глобальним цифровим простором [6 ].

Стрімкий розвиток Інтернету та цифрових технологій істотно змінив традиційне розуміння державного суверенітету. Незважаючи на те, що держави й надалі здійснюють суверенні повноваження в межах власної території, глобальний і транскордонний характер цифрового середовища значно ускладнює реалізацію цих повноважень у кіберпросторі. Цифрові комунікації, транскордонний обіг даних і функціонування міжнародних онлайн-платформ виходять за межі класичних територіальних юрисдикцій, що обмежує можливість держав самостійно та ефективно регулювати цифрові процеси лише засобами національного права. Унаслідок цього міжнародне право дедалі більше стикається з необхідністю вироблення нових підходів до узгодження принципу державного суверенітету з реаліями глобального цифрового простору [7, с. 213].

Якщо державні кордони чітко визначають межі здійснення юрисдикції у фізичному світі, то цифрове середовище не має аналогічних просторових обмежень. Інформація, цифрові сервіси, програмні продукти та електронні

ресурси циркулюють між державами практично безперешкодно, що значно ускладнює застосування класичних механізмів територіального регулювання.

Така специфіка цифрового простору зумовила появу численних міжнародно-правових колізій. З одного боку, держави прагнуть реалізовувати свої суверенні повноваження шляхом встановлення правил щодо поширення цифрового контенту, діяльності онлайн-платформ і доступу до інформації в межах власної юрисдикції. З іншого боку, глобальна архітектура Інтернету не відповідає територіальній логіці національних правових систем, що ускладнює ефективне застосування таких обмежень і потребує розвитку узгоджених міжнародно-правових механізмів регулювання цифрового середовища.

На відміну від усталених сфер міжнародного співробітництва, у яких нормативні правила значною мірою ґрунтуються на узгоджених міжнародних договорах і сформованих механізмах правового регулювання, кіберпростір характеризується значно вищим рівнем нормативної фрагментації. Його транскордонна природа, технологічна динамічність та участь у формуванні правил різноманітних державних і недержавних суб'єктів ускладнюють вироблення універсальних правових стандартів. Багатостороння модель управління кіберпростором, з одного боку, розширює можливості для представництва інтересів різних учасників та сприяє більш інклюзивному характеру нормативного процесу, а з іншого – може породжувати розбіжності між правовими підходами та ускладнювати формування узгодженого міжнародного регуляторного середовища. Наслідком цього стає відмінність національних моделей цифрового врядування, які можуть суттєво різнитися за принципами, обсягом державного контролю та підходами до забезпечення цифрових прав.

Сучасний стан міжнародно-правового регулювання штучного інтелекту характеризується відсутністю універсальної нормативної конструкції, яка б системно визначала правила його розроблення, впровадження та використання у

різних сферах суспільного життя. Наявні міжнародні акти, рекомендаційні документи та окремі регуляторні ініціативи охоплюють лише певні аспекти функціонування технологій ШІ, не утворюючи при цьому цілісного механізму міжнародно-правового контролю за їх застосуванням. Особливої уваги потребують питання встановлення етичних і правових меж використання алгоритмічних систем, визначення суб'єктів та підстав відповідальності за рішення або наслідки, пов'язані із застосуванням ШІ, а також забезпечення ефективних гарантій реалізації фундаментальних прав і свобод людини.

Актуальність зазначених проблем посилюється поступовим поширенням алгоритмічних технологій на процеси, які раніше перебували переважно у сфері безпосереднього людського контролю. Застосування ШІ дедалі частіше впливає на визначення можливостей особи у сфері працевлаштування, отримання фінансових послуг, доступу до соціальних благ, здійснення правосуддя та реалізації інших юридично значущих прав. За таких умов виникає потреба у виробленні міжнародних стандартів, здатних забезпечити належний рівень прозорості алгоритмічних процедур, підзвітності їх розробників і користувачів, можливості людського контролю та недопущення дискримінаційних наслідків.

Отже, формування міжнародно-правового підходу до регулювання ШІ має відбуватися з урахуванням не лише технологічних особливостей відповідних систем, а передусім необхідності збереження пріоритету прав людини в умовах поширення алгоритмічного управління. Йдеться про створення такого нормативного середовища, у якому технологічна автономність не усуватиме вимог юридичної відповідальності, а впровадження інновацій супроводжуватиметься належними гарантіями законності, справедливості, недискримінації та поваги до людської гідності [8, с. 49].

Особливо виразно проблема нормативної неоднорідності проявляється у сфері транскордонного обігу інформації та персональних даних. Відмінності між національними режимами їх збирання, оброблення, зберігання та передачі

створюють ситуації, за яких одна й та сама операція з даними може відповідати вимогам законодавства однієї юрисдикції, але суперечити нормативним приписам іншої. Така правова асиметрія породжує невизначеність для держав, міжнародних організацій і приватних суб'єктів, які здійснюють діяльність у цифровому середовищі, а також підвищує ризик виникнення юрисдикційних колізій. У цьому контексті відсутність узгоджених міжнародних підходів до транскордонної передачі даних залишається одним із ключових чинників регуляторної нестабільності та міждержавних правових суперечностей.

Європейський Союз належить до числа найбільш послідовних суб'єктів у формуванні концептуальних і нормативних засад цифрового суверенітету, що проявляється насамперед у прагненні встановити високі стандарти регулювання цифрових відносин та захисту прав людини в інформаційному середовищі. Важливим прикладом такого підходу є Загальний регламент про захист даних (GDPR), який сформував уніфіковані вимоги до оброблення та захисту персональних даних і визначив правила їх застосування не лише до суб'єктів, розташованих у межах Європейського Союзу. За передбачених Регламентом умов його положення можуть поширюватися також на організації, що перебувають за межами ЄС, якщо їхня діяльність пов'язана з обробленням персональних даних осіб, які перебувають у відповідній сфері дії законодавства ЄС. Такий підхід демонструє прагнення Європейського Союзу забезпечити ефективність власних регуляторних стандартів у глобальному цифровому середовищі та посилити контроль над транскордонними процесами оброблення даних [9, с. 78].

Транскордонний характер цифрового середовища створює істотні перешкоди для ефективного застосування та забезпечення виконання національних і регіональних нормативних вимог у сфері обігу даних. Особливо складними є ситуації, за яких окремі етапи життєвого циклу цифрової інформації – від її збору та первинної обробки до зберігання, передачі й подальшого

використання – реалізуються із застосуванням технологічної інфраструктури, розосередженої між декількома державами. За таких обставин одна й та сама операція з даними фактично може підпадати під дію кількох правопорядків, кожен із яких встановлює власні правила щодо доступу до інформації, умов її оброблення, забезпечення конфіденційності та порядку передачі третім особам.

Наявність різних, а в окремих випадках суперечливих регуляторних вимог ускладнює встановлення меж юрисдикції держави та визначення правового режиму, який має застосовуватися до конкретних цифрових операцій. Додаткові труднощі виникають під час контролю за виконанням відповідних приписів суб'єктами, діяльність яких фактично не обмежується територією однієї держави. Це особливо актуально для великих технологічних платформ і операторів цифрової інфраструктури, діяльність яких може охоплювати значну кількість правових юрисдикцій одночасно.

На відміну від традиційних сфер міжнародного регулювання, заснованих на відносно усталених договірних механізмах, кіберпростір характеризується фрагментарністю та відсутністю уніфікованого нормативно-правового підходу. Залучення широкого кола державних і недержавних суб'єктів до процесів цифрового врядування забезпечує більшу репрезентативність та інклюзивність, однак водночас не усуває проблеми правової несистемності. Це, зокрема, зумовлює істотні відмінності у підходах держав до формування національної політики у сфері цифрового управління. Особливо виразно така нормативна фрагментація проявляється у регулюванні транскордонного обігу та передачі даних, де відмінності між національними правовими режимами породжують регуляторну невизначеність і створюють передумови для виникнення юрисдикційних та міждержавних суперечностей.

За наведених обставин застосування класичних територіальних моделей правозастосування не завжди дає змогу забезпечити належну дієвість нормативних приписів у цифровому просторі. Віртуальний характер значної

частини цифрових процесів, їхня транскордонність та розподіленість технологічної інфраструктури істотно ускладнюють встановлення меж державної юрисдикції й практичне виконання правових вимог щодо суб'єктів, діяльність яких виходить за межі одного національного правопорядку. Це зумовлює необхідність адаптації традиційних міжнародно-правових механізмів до специфіки цифрового середовища та пошуку нових форм міждержавної взаємодії.

У цьому контексті перспективним напрямом є поглиблення міжнародного співробітництва з питань визначення юрисдикції, взаємного визнання та виконання регуляторних вимог, а також забезпечення ефективного обміну інформацією між компетентними органами різних держав. Важливим завданням міжнародно-правового розвитку стає формування узгоджених підходів до транскордонного обігу цифрових даних, які дозволили б мінімізувати колізії між національними правовими режимами та забезпечити передбачуваність правового регулювання для всіх учасників цифрових відносин.

Водночас гармонізація відповідних правил не повинна розглядатися виключно як інструмент полегшення транскордонного обігу інформації. Її фундаментальним призначенням має залишатися забезпечення належного рівня захисту особи в цифровому середовищі. Саме тому міжнародні стандарти у сфері даних мають поєднувати легітимні інтереси держав щодо здійснення регуляторних повноважень із гарантіями приватності, інформаційної безпеки, недискримінації та інших цифрових прав людини. Такий баланс є необхідною передумовою формування ефективної міжнародно-правової моделі управління цифровим простором, здатної враховувати як суверенні інтереси держав, так і глобальний характер сучасних інформаційних процесів [6].

Проблематика цифрового суверенітету є одним із найбільш показових проявів трансформації традиційних уявлень про співвідношення державної юрисдикції та транскордонного характеру цифрового середовища. Класична

модель міжнародного права значною мірою сформована на основі територіального принципу здійснення державної влади, однак специфіка кіберпростору суттєво ускладнює застосування такого підходу до відносин, у яких створення, передача, оброблення та зберігання цифрової інформації можуть відбуватися одночасно на території декількох держав. Відсутність фізичної прив'язаності значної частини цифрових процесів до конкретної території створює нові виклики для визначення меж національної юрисдикції та забезпечення ефективності правового регулювання транскордонних операцій.

У цьому контексті концепція цифрового суверенітету відображає прагнення держав адаптувати традиційні суверенні повноваження до умов цифрової трансформації та забезпечити більш ефективний контроль над даними, цифровою інфраструктурою і діяльністю суб'єктів, що функціонують у цифровому середовищі. Показовим прикладом такого підходу є правове регулювання Європейського Союзу у сфері захисту персональних даних, зокрема Загальний регламент про захист даних (GDPR), положення якого за певних умов поширюються і на діяльність суб'єктів, що перебувають за межами території ЄС. Такий механізм демонструє тенденцію до використання екстериторіальних регуляторних інструментів для забезпечення захисту прав та інтересів осіб у цифровому середовищі.

### 3.2. Міжнародно-правові засади регулювання штучного інтелекту

Поява та стрімке поширення новітніх цифрових технологій, зокрема систем штучного інтелекту (ШІ), блокчейну та технологій розподіленого реєстру, зумовлюють виникнення нових правовідносин, які не завжди можуть бути належним чином врегульовані за допомогою традиційних нормативних підходів. Специфіка функціонування таких технологій, їх транскордонний характер і здатність змінювати усталені механізми прийняття рішень, обміну інформацією та здійснення управлінських процесів актуалізують потребу у формуванні

адаптивних правових механізмів, здатних реагувати на технологічні зміни без надмірного обмеження інноваційного розвитку.

Застосування ШІ породжує комплекс взаємопов'язаних питань, що стосуються визначення меж юридичної відповідальності, забезпечення етичності алгоритмічних рішень, дотримання принципів недискримінації, прозорості та захисту фундаментальних прав людини. Водночас використання блокчейн-технологій і розподілених реєстрів актуалізує інші групи правових проблем, серед яких особливого значення набувають забезпечення конфіденційності інформації, кібербезпеки, належного управління цифровими системами та визначення відповідальних суб'єктів у децентралізованих мережах. Відсутність єдиного центру контролю в таких технологічних середовищах істотно ускладнює застосування традиційних моделей правового регулювання та визначення меж відповідальності учасників відповідних систем.

Транскордонний характер цифрових технологій зумовлює необхідність виходу за межі виключно національного регулювання та посилення міжнародної нормативної координації. Розроблення узгоджених міжнародних принципів і стандартів у цій сфері може сприяти формуванню передбачуваного правового середовища, забезпеченню належного рівня захисту прав людини та мінімізації ризиків, пов'язаних із неконтрольованим використанням технологічних інновацій. Водночас міжнародне регулювання має враховувати динамічність технологічного розвитку та залишатися достатньо гнучким для адаптації до появи нових форм цифрової діяльності.

Формування концепції «цифрового суверенітету» відображає прагнення держав адаптувати традиційні механізми суверенної влади до умов цифрової трансформації. Її становлення значною мірою пов'язане з необхідністю забезпечення державного контролю над обігом даних, транскордонними інформаційними потоками, цифровою інфраструктурою та функціонуванням технологічних систем. Водночас реалізація такого контролю в глобальному

цифровому середовищі потребує пошуку балансу між юрисдикційними повноваженнями держав і транскордонною природою сучасних цифрових технологій.

Водночас транскордонна природа кіберпростору створює істотні труднощі для ефективного забезпечення виконання відповідних правових вимог, особливо у випадках, коли зберігання, передача чи обробка даних здійснюються одночасно або послідовно в межах декількох юрисдикцій. Така ситуація ускладнює визначення застосовного права, меж державної юрисдикції та механізмів забезпечення відповідальності суб'єктів цифрових відносин.

Регулювання кіберпростору є одним із найбільш складних напрямів сучасного міжнародно-правового розвитку, що зумовлено передусім його технологічною специфікою, відсутністю єдиного центру управління та транскордонним характером цифрових процесів. На відміну від окремих традиційних сфер міжнародного регулювання, для яких сформовано спеціальні договірні режими та визначено базові принципи здійснення державами відповідних прав і обов'язків, кіберпростір не охоплений універсальним міжнародним договором, який би комплексно встановлював правила його функціонування та визначав межі поведінки всіх зацікавлених суб'єктів.

Особливість кіберпростору полягає також у тому, що його інфраструктура, інформаційні ресурси та цифрові операції не обмежуються територією окремої держави. Передача даних, функціонування цифрових платформ, розміщення серверів та діяльність користувачів можуть одночасно бути пов'язані з декількома юрисдикціями. Це ускладнює застосування традиційного територіального принципу юрисдикції та створює колізії між національними правовими режимами. Відсутність універсального договірного механізму, своєю чергою, призводить до формування фрагментарної системи регулювання, у межах якої окремі питання вирішуються за допомогою регіональних актів,

двосторонніх і багатосторонніх домовленостей, національного законодавства та міжнародних рекомендацій.

Таким чином, специфіка кіберпростору потребує подальшого розвитку міжнародно-правових механізмів, здатних забезпечити належне співвідношення державного суверенітету, міжнародної безпеки, свободи цифрової взаємодії та захисту прав людини. Основним викликом залишається формування узгоджених міжнародних правил, які враховували б динамічність технологічного середовища та водночас забезпечували достатній рівень юридичної визначеності для держав, міжнародних організацій, приватних суб'єктів і користувачів цифрових послуг [10, с. 78].

Водночас особливістю сучасного управління кіберпростором є відсутність єдиного суб'єкта, наділеного виключною компетенцією щодо встановлення та реалізації правил його функціонування. Нормативне й інституційне формування цифрового середовища здійснюється за участю широкого кола державних і недержавних акторів, серед яких провідне місце посідають органи державної влади, міжнародні організації, представники приватного технологічного сектору та інституції громадянського суспільства. Їхня взаємодія охоплює розроблення технічних стандартів, формування регуляторних підходів, визначення принципів цифрової безпеки та вироблення механізмів захисту прав користувачів. Така багатосуб'єктна модель управління дає змогу враховувати різноманітні інтереси учасників цифрових відносин, однак водночас ускладнює досягнення універсальної нормативної узгодженості та чіткого розмежування відповідальності між відповідними суб'єктами [11, с. 67].

Таким чином, взаємодія міжнародного права з новітніми цифровими технологіями потребує комплексного переосмислення традиційних регуляторних підходів. Ефективне врядування у сфері ШІ, блокчейну та інших децентралізованих технологій можливе за умови поєднання національних правових механізмів із міжнародними стандартами та належними формами

міждержавної співпраці. Саме міжнародна координація має стати одним із ключових інструментів забезпечення відповідального технологічного розвитку, за якого інноваційний потенціал цифрових технологій узгоджується з вимогами правової визначеності, безпеки та поваги до фундаментальних прав людини [6].

Сучасний етап цифрової трансформації міжнародного права характеризується комплексними змінами, які відбуваються у трьох взаємопов'язаних вимірах. Насамперед відбувається переосмислення матеріально-правових норм, що поступово інтегрують регулювання суспільних відносин, пов'язаних із застосуванням цифрових технологій. Водночас удосконалюються процесуальні інструменти міжнародного правосуддя, зокрема механізми отримання, збереження, перевірки та оцінки цифрових доказів. Крім того, формуються нові міжнародні стандарти, спрямовані на забезпечення належної обачності, відкритості діяльності суб'єктів міжнародного права та обов'язкового збереження вирішальної ролі людини у процесі прийняття рішень із використанням сучасних цифрових систем [12].

Водночас практична реалізація подібних регуляторних моделей стикається з об’єктивними труднощами, зумовленими глобальною структурою цифрової інфраструктури, розподіленим характером зберігання даних та діяльністю технологічних компаній одночасно в багатьох юрисдикціях. Унаслідок цього виникають ситуації, за яких застосування національних норм може перетинатися або вступати в колізію з правовими вимогами інших держав. Зазначені тенденції зумовлюють необхідність переосмислення традиційних підходів до визначення юрисдикції, меж екстериторіальної дії національного законодавства та механізмів міжнародної нормативної координації. Відтак подальший розвиток міжнародного права у цифрову епоху потребує пошуку балансу між збереженням суверенних повноважень держав та необхідністю забезпечення функціонування глобального цифрового простору на основі узгоджених правових принципів і взаємно визнаних регуляторних стандартів [6].

Міжнародне право історично формувалося як правова система, у якій основне значення надавалося письмовим міжнародним договорам, дипломатичному листуванню, офіційним міждержавним комунікаціям та традиційним способам підтвердження юридично значущих обставин. Проте стрімкий розвиток цифрових технологій суттєво змінив підходи до встановлення фактів у міжнародно-правових відносинах. Сьогодні дедалі частіше доказова база ґрунтується на цифрових матеріалах, зокрема відеозаписах, зроблених за допомогою мобільних пристроїв, супутникових зображеннях, метаданих, інформації з відкритих джерел (OSINT), даних із соціальних платформ, а також результатах автоматизованого аналізу великих масивів інформації. Найбільш виразно така трансформація проявляється під час розслідування міжнародних злочинів, документування порушень прав людини та вирішення міждержавних спорів, де цифрові докази дедалі частіше набувають вирішального значення для встановлення фактичних обставин справи [1].

З огляду на це можна дійти висновку, що цифрова трансформація не підриває засад міжнародного права, а стимулює його еволюцію відповідно до нових технологічних реалій. Такий розвиток сприяє зміцненню інституційної та технічної спроможності міжнародно-правових механізмів, розширює можливості використання сучасних засобів доказування та підвищує адаптивність процесуальних процедур. Водночас інтеграція цифрових технологій породжує нові правові виклики, пов'язані із забезпеченням права на приватність, дотриманням процесуальних гарантій, недопущенням дискримінації та підтриманням довіри до механізмів прийняття рішень. Особливої уваги потребують випадки, коли держави або міжнародні інституції використовують непрозорі алгоритмічні системи чи спираються на цифрові матеріали, достовірність, походження або цілісність яких не пройшли належної правової та технічної перевірки [12].

Штучний інтелект став предметом міжнародного правового регулювання передусім через призму прав людини, безпеки, недискримінації та відповідальності. Регулювання штучного інтелекту в міжнародному праві розвивається на перетині кількох правових площин: захисту прав людини, приватності, недискримінації, безпеки, цифрового суверенітету та відповідальності за шкоду. Міжнародно-правова проблема полягає в тому, що системи ШІ можуть впливати на права та інтереси людей без безпосереднього людського втручання, а отже, традиційні моделі відповідальності потребують переосмислення.

Рекомендація ЮНЕСКО про етику штучного інтелекту, схвалена 193 державами-членами, стала першим глобальним нормативним інструментом, який заклав засадничі принципи людоцентричного підходу до ШІ. Вона закріплює людоцентричний підхід, відповідно до якого розвиток і використання ШІ повинні узгоджуватися з правами людини, гідністю, справедливістю, гендерною рівністю, культурною різноманітністю та інклюзивністю. Вона наголошує на повазі до людської гідності, прав людини, прозорості, справедливості, відповідальності та на необхідності державної політики, що забезпечує етичне застосування ШІ. Важливо, що цей документ спрямований не лише на приватний сектор, а й на держави як головних носіїв міжнародно-правових зобов'язань. ЮНЕСКО не створює жорстко обов'язкових правил, але її рекомендація має значну нормативну вагу як універсальний орієнтир для національних законодавців і міжнародних інституцій. Її значення полягає у формуванні спільної мови для глобального діалогу: штучний інтелект не може розглядатися лише як інструмент інновацій; він є технологією, здатною впливати на фундаментальні права людини, на доступ до правосуддя та на якість правового рішення.

Сучасне міжнародно-правове регулювання штучного інтелекту ще не набуло форми єдиного універсального кодифікованого режиму, однак його

поступово формують взаємопов'язані нормативні механізми різного рівня. Така система охоплює універсальні міжнародні стандарти, регіональні правові інструменти та спеціалізоване галузеве регулювання, що разом створюють основу для формування узгоджених підходів до використання технологій ШІ. На універсальному рівні вагоме значення має Рекомендація ЮНЕСКО щодо етики штучного інтелекту, яка визначає базові орієнтири відповідального розвитку та застосування відповідних технологій, акцентуючи увагу на захисті прав людини, людській гідності, прозорості та недискримінації. На регіональному рівні істотний внесок у розвиток нормативної бази становить Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права, яка безпосередньо пов'язує регулювання ШІ із фундаментальними принципами демократичного правопорядку. Водночас у праві Європейського Союзу особливе місце посідає Регламент (ЄС) 2024/1689 про встановлення гармонізованих правил у сфері штучного інтелекту (AI Act), що запроваджує диференційований підхід залежно від рівня ризику, пов'язаного з використанням конкретних систем [13].

Сукупний розвиток зазначених нормативних інструментів свідчить про поступовий перехід від переважно декларативного визначення бажаних принципів до формування більш структурованих моделей правового регулювання. У центрі таких моделей перебувають категорії ризику, прозорості, підзвітності, безпеки та забезпечення можливості людського контролю. Водночас багаторівневість регулювання відображає складність самого феномену ШІ, який одночасно має технологічний, економічний, соціальний та правовий виміри й тому не може бути ефективно врегульований виключно в межах одного нормативного рівня. Як наголошує М. Яцишин, «норми сучасного міжнародного права, зокрема, основні принципи міжнародного права є чинними і для кіберпростору, і це означає заборону здійснювати акти агресії у кіберпросторі на

підставі принципів суверенної рівності держав, незастосування сили і погрози силою, невтручання у внутрішні справи» [14, с. 22–32.]

Поширення Інтернету та стрімкий розвиток цифрових технологій істотно вплинули на традиційне розуміння державного суверенітету, оскільки цифрові процеси дедалі менше обмежуються фізичними та територіальними межами держав. Незважаючи на збереження за державами суверенної юрисдикції в межах їхньої території, транскордонний характер кіберпростору суттєво ускладнює реалізацію цієї юрисдикції щодо цифрових процесів, інформаційних ресурсів та діяльності суб'єктів, пов'язаної з використанням мережевих технологій [7, с. 213].

З міжнародно-правової точки зору такий підхід має принципове значення. По-перше, він демонструє, що використання ШІ виходить далеко за межі суто технічного або приватноправового регулювання та безпосередньо пов'язується із забезпеченням фундаментальних прав і свобод людини. По-друге, розвиток відповідних нормативних інструментів засвідчує поступове поєднання юридично обов'язкових норм із механізмами «м'якого права», рекомендаціями та міжнародними стандартами. По-третє, сучасна практика свідчить про те, що адаптація міжнародного права до технологічних змін відбувається переважно шляхом конкретизації та поширення вже сформованих фундаментальних принципів – поваги до людської гідності, рівності, недискримінації, справедливості, безпеки та верховенства права – на нові технологічні контексти.

У цьому аспекті штучний інтелект можна розглядати як своєрідний індикатор здатності міжнародного права реагувати на структурні зміни суспільства та технологічного середовища. Ефективність правового регулювання визначатиметься не лише кількістю прийнятих нормативних актів, а передусім спроможністю існуючих механізмів забезпечувати реальний контроль за використанням алгоритмічних систем, запобігати дискримінаційним і непрозорим практикам та встановлювати відповідальність за заподіяну ними

шкоду. Якщо правові механізми виявляться неспроможними своєчасно реагувати на автономізацію процесів прийняття рішень, може сформуватися ситуація нормативної асиметрії, за якої технологічні можливості розвиватимуться швидше, ніж механізми їх правового контролю. Саме тому подальша адаптація міжнародно-правових стандартів до розвитку ШІ є необхідною умовою збереження ефективності права в умовах цифрової трансформації.

Правове забезпечення захисту персональної інформації перетворилося на один із пріоритетних напрямів сучасного міжнародно-правового регулювання, що зумовлено стрімким зростанням масштабів транскордонного збирання, зберігання, обробки та обміну даними про фізичних осіб. Попри те, що окремі держави та регіональні об'єднання сформували власні нормативні механізми у цій сфері, відповідні підходи істотно різняться за змістом і рівнем правового захисту. Серед найбільш розвинених моделей можна виокремити режим, встановлений Загальним регламентом Європейського Союзу про захист даних (GDPR), а також американське законодавство, зокрема Каліфорнійський закон про захист приватності споживачів (CCPA). Водночас універсального міжнародного механізму, який забезпечував би єдині стандарти захисту персональних даних у глобальному масштабі, наразі не сформовано [15, с. 246].

Важливим етапом у розвитку міжнародно-правового регулювання штучного інтелекту стало поступове переміщення акценту від рекомендаційних і декларативних підходів до формування юридично обов'язкових механізмів. У цьому контексті особливе значення має Рамкова конвенція Ради Європи про штучний інтелект і права людини, демократію та верховенство права [16]. Її принципова новизна полягає у комплексному підході до регулювання діяльності, пов'язаної із системами ШІ, крізь призму фундаментальних цінностей європейського правопорядку. Документ орієнтований на забезпечення того, щоб використання технологій штучного інтелекту не призводило до послаблення

гарантій прав людини, демократичних процедур та принципу верховенства права.

Нормативна конструкція Конвенції ґрунтується на низці фундаментальних засад, серед яких особливе місце посідають повага до людської гідності та автономії особи, рівність і недискримінація, захист приватного життя та персональних даних, прозорість, підзвітність, надійність і безпека технологічних систем. Її значення полягає не лише у визначенні загальних принципів, а й у встановленні орієнтирів для державної політики щодо розроблення, впровадження та використання систем ШІ. Таким чином, технологічний розвиток розглядається не як автономний процес, відокремлений від права, а як сфера, що має здійснюватися в межах уже сформованих міжнародних стандартів захисту прав людини.

Паралельно важливий напрям розвитку регулювання ШІ сформувався в межах права Європейського Союзу. Особливе місце тут належить Регламенту (ЄС) 2024/1689, відомому як AI Act, який запроваджує ризик-орієнтовану модель нормативного регулювання . Її сутність полягає у диференціації юридичних вимог залежно від характеру та потенційного рівня ризику, пов’язаного з конкретною системою ШІ. Така модель передбачає посилення регуляторних обов’язків щодо технологій, використання яких може створювати значні загрози для безпеки, здоров’я або фундаментальних прав людини, водночас не встановлюючи однакових обмежень для всіх видів ШІ.

Значення цього підходу виходить за межі внутрішнього правопорядку Європейського Союзу. Враховуючи глобальний характер цифрових ринків та транскордонну діяльність технологічних компаній, європейські регуляторні вимоги здатні впливати на практику суб’єктів, які здійснюють діяльність за межами ЄС. У результаті формується тенденція до поширення ризик-орієнтованої моделі як одного з можливих орієнтирів для національного та міжнародного регулювання ШІ. У ширшому міжнародно-правовому контексті

це сприяє зближенню підходів до забезпечення безпеки, прозорості, підзвітності та захисту фундаментальних прав у процесі використання алгоритмічних технологій.

Регулювання транскордонного переміщення даних потребує пошуку оптимального співвідношення між економічною необхідністю забезпечення міжнародного інформаційного обміну та імперативом належного захисту персональних даних і приватності. Вільний рух інформації є важливою передумовою функціонування глобальної торгівлі та цифрової економіки, однак його реалізація не повинна нівелювати встановлені правові гарантії захисту прав суб'єктів даних. У цьому аспекті показовим є правовий режим, закріплений Загальним регламентом Європейського Союзу про захист даних (GDPR), який встановлює особливі умови передачі персональної інформації за межі ЄС. Відповідні положення спрямовані на недопущення зниження рівня захисту даних унаслідок їх передачі до іншої юрисдикції та забезпечення належних гарантій під час подальшого зберігання й обробки персональної інформації [9, с. 80].

Окремим напрямом цифрової трансформації міжнародного права є формування нових підходів до використання цифрових доказів. Під ними доцільно розуміти електронну інформацію, яка може бути використана для встановлення фактів та обставин, що мають юридичне значення у конкретному провадженні. До цієї категорії можуть належати цифрові фото- та відеоматеріали, дані геолокації, метадані, матеріали соціальних мереж, супутникові зображення, електронне листування, інформація з цифрових пристроїв та інші відомості, отримані в електронній формі. Їхнє значення особливо зросло у міжнародних розслідуваннях, судових процесах та документуванні міжнародних злочинів.

Специфіка цифрової інформації зумовлює необхідність застосування до неї особливих критеріїв оцінювання. На відміну від багатьох традиційних форм

доказування, цифрові матеріали можуть бути відносно легко скопійовані, змінені, видалені або представлені поза первісним контекстом. Тому сама наявність цифрового матеріалу не є достатньою підставою для визнання його доказової переконливості. Важливого значення набувають встановлення походження інформації, перевірка її автентичності, збереження цілісності, документування способу отримання та забезпечення безперервності ланцюга зберігання. Додатковими інструментами перевірки виступають зіставлення інформації з незалежними джерелами та застосування методів цифрової криміналістики.

У сфері міжнародного кримінального права цифрові матеріали дедалі активніше використовуються для документування та доведення обставин, пов'язаних із воєнними злочинами, злочинами проти людяності та геноцидом. Особливого практичного значення у цьому контексті набув Берклійський протокол про цифрові відкриті джерела, який містить методологічні рекомендації щодо виявлення, збирання, перевірки, аналізу та збереження інформації з відкритих цифрових джерел. Його положення мають значення для діяльності слідчих, прокурорів, адвокатів, журналістів та правозахисних організацій, оскільки спрямовані на підвищення надійності цифрових матеріалів і можливості їх подальшого використання у правових процедурах.

Цифрова інформація сьогодні посідає вагоме місце в системі доказування у міжнародно-правових процедурах. До категорії цифрових доказів можуть бути віднесені електронні документи та інші цифрові дані, інформація про їх технічні характеристики, фото- й відеоматеріали, записи систем відеоспостереження, публікації та інші матеріали з соціальних платформ, супутникові зображення, відомості про місцезнаходження пристроїв, а також інші дані, що функціонують у цифровому середовищі. Залежно від характеру провадження такі матеріали можуть набувати доказового значення під час вирішення міждержавних спорів,

розгляду справ міжнародними кримінальними юрисдикціями та здійснення міжнародних механізмів захисту прав людини.

Водночас основна складність використання цифрової інформації як доказового матеріалу пов'язана не з її масштабністю, а з необхідністю підтвердження достовірності, незмінності та джерела її походження. Цифрові дані, на відміну від багатьох традиційних форм доказів, характеризуються високою технологічною вразливістю: вони можуть піддаватися редагуванню, технічній обробці, частковому видаленню, маніпулятивному монтажу або поширюватися без належного контексту. Окрему загрозу становлять технології, здатні генерувати синтетичний цифровий контент. У зв'язку з цим у міжнародній судовій та квазісудовій практиці посилюється увага до процедур отримання й фіксації цифрових матеріалів, належного документування всіх етапів їх зберігання та передачі, зіставлення інформації з незалежними джерелами, а також технічної перевірки метаданих та інших характеристик цифрового об'єкта.

Одним із найбільш дискусійних аспектів застосування штучного інтелекту у сфері правосуддя є ймовірність виникнення та відтворення алгоритмічної упередженості. Використання моделей штучного інтелекту, навчених на даних, що містять структурні або статистичні викривлення, може призводити до систематичного відтворення відповідних тенденцій під час аналізу інформації та формування рекомендацій для учасників судового процесу. Унаслідок цього існує ризик, що первинні упередження, закладені в навчальних масивах або алгоритмічних моделях, опосередковано впливатимуть на оцінювання обставин справи та, зрештою, позначатимуться на змісті судових рішень [17].

Важливим елементом формування міжнародно-правової архітектури регулювання ШІ є Рекомендація ЮНЕСКО щодо етики штучного інтелекту. Попри її рекомендаційний характер, цей документ має істотне значення для вироблення загальних нормативних орієнтирів у сфері відповідального використання технологій. Серед ключових положень Рекомендації –

необхідність поваги до прав людини та основоположних свобод, забезпечення належного людського контролю, запобігання дискримінації та шкідливим формам алгоритмічної упередженості, захист приватності й персональних даних, забезпечення прозорості та підзвітності суб'єктів, які розробляють або використовують системи ШІ [18].

З міжнародно-правової точки зору значення таких положень не обмежується сферою етичних рекомендацій. Вони сприяють формуванню спільного нормативного підходу до оцінювання допустимості використання алгоритмічних технологій і можуть доповнювати вже існуючі міжнародні стандарти у сфері прав людини. Зокрема, у ситуаціях, коли застосування ШІ впливає на приватність, рівність, недискримінацію, свободу вираження поглядів або гарантії справедливого судового розгляду, сформульовані ЮНЕСКО принципи можуть використовуватися як додатковий нормативний орієнтир під час оцінювання відповідності відповідної практики міжнародним стандартам.

Наступним етапом цього процесу стало формування юридично обов'язкової договірної основи на рівні Ради Європи. Рамкова конвенція про ШІ та права людини, демократію і верховенство права має на меті забезпечити узгодження технологічного розвитку з фундаментальними принципами правового порядку. Її підхід не передбачає загальної заборони використання штучного інтелекту. Натомість акцент зроблено на встановленні таких умов його розроблення та застосування, за яких технологічні рішення не створюватимуть непропорційних загроз для прав людини, демократичних інститутів та верховенства права.

Особливої ваги цей підхід набуває у сферах публічного управління, правосуддя, правоохоронної діяльності та забезпечення безпеки, де використання алгоритмічних систем потенційно може мати безпосередній вплив на правове становище людини. Саме тут вимоги щодо прозорості, підзвітності, можливості людського контролю та оцінювання ризиків набувають не лише етичного, а й безпосереднього правового значення.

У сукупності зазначені міжнародні та регіональні інструменти свідчать про формування багаторівневої моделі регулювання штучного інтелекту. Її особливістю є поєднання рекомендаційних стандартів, міжнародних договорів та регіонального законодавства, що поступово створює систему взаємопов'язаних правових і нормативних орієнтирів. Водночас така модель не усуває всіх проблем, пов'язаних із транскордонним характером ШІ, визначенням юрисдикції, розподілом відповідальності та забезпеченням однакового рівня захисту прав людини. Саме тому подальший розвиток міжнародно-правового регулювання має бути спрямований на узгодження існуючих механізмів та їх адаптацію до технологічних змін, не допускаючи виникнення ситуації, за якої автономність цифрових систем випереджатиме можливості правового контролю.

Сучасне міжнародно-правове регулювання штучного інтелекту (ШІ) поступово переходить від переважно рекомендаційних підходів до формування більш структурованої системи нормативних вимог. Важливим етапом цього процесу стала Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права, відкрита для підписання у 2024 році. Її значення полягає у встановленні зв'язку між використанням ШІ та фундаментальними засадами правового порядку. Конвенція орієнтує держави на забезпечення поваги до людської гідності та автономії, рівності й недискримінації, приватності та захисту персональних даних, а також прозорості, підзвітності, безпеки й належного контролю за технологічними системами.

Важливим доповненням до цього підходу є Регламент (ЄС) 2024/1689 (AI Act), який запровадив ризик-орієнтовану модель регулювання. Її сутність полягає у встановленні різного рівня юридичних вимог залежно від потенційного ризику конкретної системи ШІ для безпеки, здоров'я та фундаментальних прав [19]. З огляду на глобальний характер цифрових ринків та діяльність технологічних компаній у різних юрисдикціях, європейська модель набуває

значення не лише для держав-членів ЄС, а й як орієнтир для розвитку інших національних і міжнародних регуляторних підходів. Водночас на універсальному рівні важливу нормативну функцію виконує Рекомендація ЮНЕСКО щодо етики штучного інтелекту, яка формує спільні принципи відповідального використання ШІ, зокрема у сфері прав людини, недискримінації, приватності, людського контролю, прозорості та підзвітності.

Поряд із регулюванням ШІ важливим проявом цифрової трансформації міжнародного права є поширення цифрових доказів. До них належать фото- й відеоматеріали, метадані, дані геолокації, супутникові зображення, матеріали соціальних мереж, електронне листування та інші цифрові відомості, здатні підтверджувати юридично значущі факти. Їхнє використання набуває особливого значення під час міжнародних розслідувань і документування воєнних злочинів, злочинів проти людяності та геноциду.

Специфіка цифрових матеріалів зумовлює підвищені вимоги до встановлення їх доказової цінності. Оскільки цифрова інформація може бути змінена, скопійована або вилучена з первісного контексту, принципового значення набувають її автентичність, цілісність, походження та можливість незалежної перевірки. Важливими інструментами забезпечення надійності таких матеріалів є належне документування способу їх отримання, збереження ланцюга зберігання, зіставлення з іншими джерелами та застосування цифрової криміналістики. У цьому контексті Берклійський протокол про цифрові відкриті джерела сформував практичні орієнтири для збору, перевірки, аналізу та збереження інформації з відкритих цифрових джерел [1].

Таким чином, сучасна міжнародно-правова архітектура у цифровій сфері формується як багаторівнева система, у якій поєднуються міжнародні договори, акти «м’якого права», регіональне законодавство та спеціалізовані стандарти доказування. Її подальший розвиток залежатиме від здатності узгодити технологічні інновації з вимогами прав людини, юридичної відповідальності,

прозорості та безпеки. Основним завданням міжнародного права при цьому залишається забезпечення такого рівня нормативного контролю, за якого технологічна автономність не створюватиме прогалин у захисті особи та не випереджатиме механізми юридичної відповідальності.

### 3.3. Перспективи розвитку міжнародно-правового регулювання цифрового середовища та стратегічні орієнтири для України

Посилення глобальної цифрової взаємозалежності істотно трансформує предмет міжнародно-правового регулювання, ставлячи перед ним завдання забезпечення належного балансу між стимулюванням інноваційного розвитку та збереженням міжнародних стандартів захисту прав людини. Інтенсивний розвиток цифрових технологій актуалізує необхідність консолідації зусиль держав, міжнародних інституцій, суб'єктів господарювання та громадянського суспільства щодо формування інклюзивної й ефективної системи правового регулювання. Такий підхід має унеможливити ситуації, за яких технологічний прогрес відбувається за рахунок обмеження фундаментальних прав людини, забезпечуючи належні гарантії захисту приватного життя, рівності, недискримінації та інших базових свобод. У цьому вступі розглядається зміна функції міжнародного права у вирішенні цих складних глобальних викликів [6].

Стрімке поширення технологій штучного інтелекту істотно змінює підходи до міжнародно-правового забезпечення прав людини. Використання алгоритмічних систем уже виходить далеко за межі технічної сфери, оскільки їх застосування дедалі частіше впливає на реалізацію права на приватне життя, справедливий судовий розгляд, свободу вираження поглядів, рівність і недискримінацію, а також право на доступ до інформації. За таких умов питання використання штучного інтелекту набуває характеру не лише технологічної, а й міжнародно-правової проблеми, що безпосередньо пов'язана з обсягом позитивних зобов'язань держав щодо забезпечення та захисту основоположних прав людини. У сучасній цифровій економіці інформаційні ресурси набули

статусу одного з ключових чинників розвитку міжнародної торгівлі, інноваційної діяльності та транскордонної економічної взаємодії. Ефективне функціонування глобальних ринків дедалі більше залежить від безперешкодного переміщення даних між державами, що забезпечує розвиток цифрових сервісів, міжнародного бізнесу та новітніх технологій. Водночас інтенсивне поширення транскордонних потоків інформації актуалізує низку складних правових питань, пов'язаних із захистом персональних даних, інформаційною безпекою та гарантуванням права на приватне життя [6].

Подальша цифровізація суспільних відносин обумовлює необхідність переосмислення підходів міжнародного права до регулювання новітніх технологій. Одним із ключових завдань стає вироблення такого правового механізму, який одночасно сприятиме розвитку інновацій та забезпечуватиме ефективний захист фундаментальних прав і свобод людини. Застосування штучного інтелекту, технологій блокчейну та інших цифрових рішень створює нові можливості для економічного зростання, модернізації державного управління та розвитку міжнародної співпраці. Водночас їх широке впровадження супроводжується появою нових правових ризиків, пов'язаних із захистом приватного життя, збереженням автономії особи, забезпеченням рівності, недискримінації та дотриманням принципів справедливості. Саме тому подальша еволюція міжнародно-правового регулювання має бути спрямована на формування нормативної моделі, здатної поєднати технологічний прогрес із надійними гарантіями прав людини [20, с. 155].

Принципове значення має забезпечення того, щоб розроблення, використання та подальше вдосконалення цифрових технологій здійснювалися із безумовним дотриманням міжнародно визнаних стандартів прав людини. Лише за таких умов можливо підтримувати суспільну довіру до цифрових інновацій, мінімізувати ризики їх неправомірного використання та запобігати виникненню негативних наслідків для прав і свобод людини. Фундаментом

такого підходу виступає міжнародне право прав людини, яке формує систему універсальних принципів і юридичних орієнтирів для відповідального застосування сучасних цифрових технологій. Визначальну роль у цьому відіграють універсальні міжнародно-правові акти, насамперед Загальна декларація прав людини 1948 року та Міжнародний пакт про громадянські і політичні права 1966 року, положення яких закріплюють базові гарантії поваги до гідності людини, права на приватне життя, свободи вираження поглядів, рівності та ефективного правового захисту [21]. Саме ці міжнародні стандарти слугують нормативною основою для формування сучасних підходів до правового регулювання цифрових технологій і штучного інтелекту. Водночас більшість базових міжнародних договорів у сфері захисту прав людини була розроблена ще до стрімкого розвитку цифрових технологій, тому їхні положення не враховували специфічних ризиків, пов'язаних із цифровізацією суспільних відносин. У зв'язку з цим актуалізується потреба в подальшому розвитку та адаптації міжнародно-правових механізмів до нових технологічних реалій. Така модернізація має забезпечити ефективне реагування на виклики, що виникають унаслідок використання штучного інтелекту, великих даних, алгоритмічних систем та інших цифрових технологій, зберігаючи при цьому належний рівень гарантій основоположних прав і свобод людини [22, с. 31]. Одним із перспективних напрямів удосконалення міжнародно-правового регулювання може стати розроблення нових універсальних нормативних підходів, міжнародних стандартів і рекомендацій, спрямованих на забезпечення відповідального використання технологій штучного інтелекту. Їх основною метою має бути формування єдиних принципів захисту персональних даних, гарантування права на приватне життя, забезпечення прозорості та підзвітності алгоритмічних систем, а також утвердження засад цифрової справедливості й недискримінації у глобальному цифровому середовищі. Такий підхід сприятиме

гармонізації національного законодавства та зміцненню міжнародного співробітництва у сфері регулювання цифрових технологій [15, с. 248].

Стрімкий розвиток цифрових технологій обумовлює необхідність модернізації міжнародно-правових підходів до регулювання транскордонного обігу даних. У цих умовах міжнародне право має виробити ефективні правові механізми, які б одночасно сприяли безперешкодному міжнародному обміну інформацією та гарантували належний рівень захисту конфіденційності, кібербезпеки й інших основоположних прав людини. Вирішення цього завдання потребує пошуку оптимального балансу між економічними інтересами, пов'язаними з розвитком глобальної цифрової економіки, та забезпеченням високих стандартів правового захисту особи у цифровому середовищі.

За таких обставин особливого значення набуває дослідження міжнародно-правових моделей управління даними, принципів їх транскордонного переміщення та правових інструментів, покликаних гарантувати належний рівень охорони персональних даних і права на приватність у процесі глобальної цифрової взаємодії. Аналіз цих підходів є необхідним для формування сучасної системи міжнародно-правового регулювання, здатної забезпечити одночасно відкритість цифрового простору, довіру до міжнародного обміну даними та ефективний захист прав людини в умовах цифрової трансформації.

Інтенсивний розвиток технологій штучного інтелекту (ШІ) зумовлює глибоку трансформацію широкого спектра суспільних відносин та поступово змінює усталені підходи до функціонування окремих секторів, зокрема охорони здоров’я, фінансової діяльності, освіти, правосуддя та зайнятості. Водночас розширення сфер практичного застосування алгоритмічних систем актуалізує низку правових, етичних і соціальних проблем, пов’язаних із характером та наслідками їх використання. Особливе значення має тенденція до залучення ШІ у процеси прийняття рішень, результати яких можуть безпосередньо визначати правове, економічне або соціальне становище окремої особи чи певних груп

населення. Алгоритмічні інструменти вже можуть використовуватися під час оцінювання здобувачів освіти, прогнозування судових рішень, визначення кредитоспроможності, відбору кандидатів на працевлаштування та здійснення інших процедур, що мають істотний вплив на реалізацію прав і законних інтересів людини.

Зростання функціональної автономності таких систем, здатних самостійно обробляти значні масиви інформації та формувати результати без безпосереднього втручання людини на кожному етапі, водночас ускладнює визначення механізмів контролю за їх діяльністю. У зв’язку з цим особливої актуальності набувають вимоги щодо зрозумілості алгоритмічних процесів, можливості перевірки обґрунтованості отриманих результатів, визначення відповідального суб’єкта та запобігання дискримінаційним наслідкам автоматизованого прийняття рішень. Таким чином, поширення ШІ потребує не лише технологічного вдосконалення відповідних систем, а й формування належних правових гарантій, які забезпечували б їх прозоре, підзвітне та справедливе застосування з урахуванням пріоритету захисту прав і свобод [20, с. 152].

Особливого значення міжнародні стандарти набувають у тих випадках, коли алгоритмічні системи використовуються для прийняття або підтримки рішень, здатних впливати на правовий статус особи. Це стосується автоматизованого оцінювання ризиків, біометричної ідентифікації, прогнозної аналітики, аналізу цифрових доказів та інших форм алгоритмічного опрацювання інформації. Якщо результати роботи таких систем породжують юридично значущі наслідки, вони повинні відповідати вимогам прозорості, можливості незалежної перевірки, обґрунтованості та обов'язкового людського контролю. Саме тому новітні міжнародні документи дедалі більше акцентують увагу не лише на підтримці технологічного розвитку, а й на необхідності ефективного механізму нагляду за функціонуванням систем штучного інтелекту.

Однією з найбільш складних проблем правового регулювання систем штучного інтелекту є встановлення належного суб'єкта юридичної відповідальності за шкоду або інші негативні наслідки, спричинені функціонуванням алгоритмічних систем. Особливість цієї проблеми зумовлена тим, що процес формування рішення може охоплювати декілька взаємопов'язаних суб'єктів: розробників технології, її виробників і постачальників, операторів та організації, які інтегрують відповідну систему у власну діяльність, а також кінцевих користувачів. У разі отримання системою ШІ помилкового, упередженого або такого, що спричинив шкоду, результату виникає питання щодо того, на кого саме має покладатися юридичний обов'язок щодо відшкодування завданої шкоди чи усунення наслідків такого рішення.

Додаткову складність становить технологічна автономність сучасних систем ШІ, здатних самостійно обробляти значні обсяги даних, виявляти закономірності та генерувати результати, які не завжди можуть бути безпосередньо передбачені особою, що їх розробила або використовує. За таких обставин встановлення причинно-наслідкового зв'язку між конкретною поведінкою людини та негативним результатом роботи алгоритму може бути істотно ускладненим. Це ставить під сумнів достатність традиційних моделей юридичної відповідальності, побудованих переважно на можливості ідентифікувати конкретну протиправну поведінку та її суб'єкта.

Відтак формування ефективного механізму відповідальності у сфері ШІ потребує чіткого розмежування обов'язків і ризиків між усіма учасниками життєвого циклу відповідної технології. Правове регулювання має визначати не лише умови відповідальності за безпосередньо заподіяну шкоду, а й вимоги до належного проєктування, тестування, впровадження, моніторингу та контролю за функціонуванням систем ШІ. Особливого значення набуває забезпечення можливості встановити, на якому етапі виникла передумова для негативного результату та який суб'єкт мав реальну можливість запобігти його настанню.

Такий підхід сприятиме формуванню більш передбачуваної та справедливої моделі відповідальності, здатної враховувати специфіку автономних технологій і водночас не допускати виникнення правових прогалин у захисті прав та законних інтересів людини [23, с. 10].

Характерною тенденцією сучасного міжнародного права є поступовий перехід від рекомендацій етичного характеру до запровадження комплексних механізмів управління ризиками, пов'язаними із застосуванням штучного інтелекту. Нормативне регулювання дедалі більше орієнтується на встановлення чітких процедур оцінювання ризиків, незалежного аудиту алгоритмічних систем, документування процесів їх функціонування та визначення відповідальності за можливі негативні наслідки використання цифрових технологій. Такий підхід свідчить про еволюцію міжнародного права від проголошення загальних принципів до формування практичних інструментів забезпечення безпечного й правомірного використання інновацій.

Одночасно штучний інтелект створює нові виклики для міжнародної системи гарантування прав людини. Застосування алгоритмів для прогнозування поведінкових моделей, розпізнавання облич, аналізу великих масивів даних, моніторингу цифрових комунікацій та інших форм автоматизованої обробки інформації здатне призводити до надмірного втручання у приватне життя, відтворення або посилення дискримінаційних практик, необґрунтованого обмеження свободи вираження поглядів, а також порушення гарантій справедливого судового розгляду. Саме тому формування міжнародно-правових механізмів, спрямованих на забезпечення прозорості, підзвітності та контролю за використанням технологій штучного інтелекту, стає одним із ключових напрямів розвитку сучасного міжнародного права.

За сучасних умов міжнародне право змушене переосмислювати традиційні правові механізми та адаптувати їх до стрімкого розвитку цифрових технологій. Якщо алгоритмічні системи здатні суттєво впливати на реалізацію прав, свобод

чи законних інтересів людини, їх функціонування повинно відповідати вимогам прозорості, підконтрольності, можливості незалежної перевірки та зрозумілості прийнятих рішень. Міжнародні стандарти дедалі послідовніше виходять із того, що технологічний прогрес не може виправдовувати обмеження або нівелювання фундаментальних прав людини. З цієї причини сучасні міжнародно-правові акти закріплюють необхідність забезпечення ефективного людського контролю за використанням систем штучного інтелекту, проведення попередньої оцінки їхнього впливу на права людини та гарантування права на перегляд і оскарження рішень, ухвалених із застосуванням автоматизованих або частково автоматизованих технологій.

Поширення штучного інтелекту впливає не лише на механізми правозастосування, а й на концептуальні засади міжнародно-правової відповідальності. Класичний підхід, який пов'язує виникнення відповідальності насамперед із винною поведінкою конкретної особи, дедалі частіше виявляється недостатнім у випадках, коли негативні наслідки є результатом функціонування складних алгоритмічних систем, особливостей машинного навчання, використання недостовірних даних або помилок у програмному забезпеченні. За таких умов міжнародно-правова доктрина та практика поступово зміщують акцент із виключно оцінки поведінки окремої особи на відповідальність за весь життєвий цикл технології – від її проєктування та розроблення до впровадження, незалежного аудиту, постійного моніторингу та належного контролю за її функціонуванням.

Чинні правові механізми не повною мірою відповідають специфіці правовідносин, що виникають у зв’язку із застосуванням систем штучного інтелекту. Значна частина традиційних нормативних конструкцій формувалася з розрахунком на те, що юридично значущі рішення приймаються людиною, яка може усвідомлювати їхні наслідки, контролювати процес їх формування та нести за них відповідальність. Натомість автономні алгоритмічні системи

функціонують на основі складних технологічних процесів, у межах яких остаточний результат може бути сформований без безпосереднього втручання людини. Така специфіка ускладнює застосування усталених підходів до визначення відповідальності, забезпечення прозорості алгоритмічних процедур та встановлення меж належного людського контролю.

У цьому контексті особливого значення набуває комплекс проблем, пов'язаних із правовою визначеністю, підзвітністю суб'єктів, залучених до створення та використання ШІ, прозорістю алгоритмічного прийняття рішень і визначенням юрисдикції у випадках, коли відповідні технології функціонують одночасно в декількох правових просторах. Водночас твердження про повну відсутність нормативної основи для регулювання ШІ було б надмірно категоричним. Сучасне міжнародне право вже містить низку положень і принципів, які можуть застосовуватися до окремих аспектів функціонування систем штучного інтелекту, зокрема у сфері захисту прав людини, недискримінації, приватності, інформаційної безпеки та відповідальності.

Важливу роль у формуванні такого нормативного підґрунтя відіграють акти «м'якого права» та міжнародні стандарти, серед яких особливе місце посідають Рекомендація ЮНЕСКО щодо етики штучного інтелекту та Принципи ОЕСР щодо штучного інтелекту. Хоча зазначені документи не створюють універсального юридично обов'язкового режиму регулювання ШІ, вони формують спільні нормативні орієнтири щодо прозорості, відповідального використання технологій, людського контролю, безпеки та поваги до фундаментальних прав. Крім того, відповідні положення міжнародного права прав людини та галузевих міжнародних договорів можуть забезпечувати правову основу для регулювання конкретних ситуацій, у яких застосування ШІ впливає на права та свободи людини. Як наголошує І.М. Берназюк, « Конвенція про ШІ має суттєве значення для України в контексті реформування національної правової системи та виконання міжнародних зобов'язань у сфері прав людини,

оскільки її поло-ження створюють нормативну основу для перегляду галузевого законодавства, зокрема у сфері публічного управління, судочинства, кримінальної юстиції та захисту персональних даних» [24, с. 28].

Отже, основна проблема полягає не стільки у цілковитій відсутності правового регулювання штучного інтелекту, скільки у фрагментарності та недостатній узгодженості наявних нормативних механізмів. Сучасне міжнародне право потребує подальшого розвитку з урахуванням технологічної автономності систем ШІ та пов'язаних із нею нових форм ризику. Перспективним видається формування багаторівневої моделі регулювання, яка поєднувала б обов'язкові норми міжнародного права, стандарти у сфері прав людини, інструменти «м'якого права» та спеціалізовані міжнародні домовленості. Такий підхід дасть змогу не замінювати вже існуючі правові механізми, а адаптувати й доповнювати їх відповідно до специфіки алгоритмічних технологій.

У сучасному міжнародному правопорядку зберігається істотна нормативна прогалина, пов'язана з відсутністю універсального механізму регулювання захисту персональних даних. Такі правові інструменти, як GDPR у Європейському Союзі, забезпечують високий рівень захисту в межах відповідних юрисдикцій, однак їх транскордонне застосування породжує додаткові юридичні та практичні труднощі для суб'єктів, діяльність яких охоплює декілька держав. Відмінності між національними правовими режимами ускладнюють забезпечення узгодженого рівня захисту персональної інформації, створюють ризики виникнення регуляторних прогалин і можуть негативно впливати на безпеку даних. З огляду на глобалізацію цифрових інформаційних потоків та зростання економічної цінності персональних даних актуалізується питання вироблення універсальних міжнародних стандартів і формування юридично обов'язкового міжнародного механізму їх захисту [6].

Попри формування міжнародних механізмів, спрямованих на посилення протидії кіберзагрозам, зокрема прийняття Конвенції Ради Європи про кіберзлочинність (Будапештської конвенції), сучасна система міжнародно-правового регулювання у цій сфері залишається неповною. На сьогодні відсутній універсальний міжнародний договір, який комплексно визначав би правові засади ведення кібероперацій у контексті збройних конфліктів, а також встановлював би узгоджені міжнародні стандарти щодо запобігання кібернападам на об'єкти критичної інфраструктури та реагування на них [10, с. 241].

Не менш вагомою тенденцією є трансформація інституту міжнародного доказування. Стрімке збільшення обсягу цифрової інформації, що використовується під час документування міжнародних злочинів, порушень міжнародного гуманітарного права, міжнародного кримінального переслідування та захисту прав людини, обумовлює перегляд традиційних критеріїв оцінювання доказів. Цифрові дані більше не мають допоміжного характеру, а дедалі частіше становлять основне джерело встановлення юридично значущих обставин. Відповідно міжнародне процесуальне право потребує подальшого вдосконалення процедур перевірки походження цифрової інформації, підтвердження її цілісності, забезпечення належного зберігання, простежуваності та процесуальної допустимості. Це сприятиме підвищенню довіри до результатів міжнародного судочинства та зміцненню ефективності механізмів міжнародної відповідальності.

Аналіз сучасної міжнародної нормативної бази свідчить про поступове формування багаторівневої системи регулювання цифрової сфери. Універсальні стандарти, закріплені, зокрема, в Рекомендації ЮНЕСКО щодо етики штучного інтелекту, регіональні механізми, сформовані в межах Ради Європи, наднаціональне регулювання, запроваджене Європейським Союзом через Акт про штучний інтелект, а також процесуальні стандарти, відображені у

Берклійському протоколі та практиці міжнародних судових інституцій, демонструють поступовий перехід від фрагментарного нормативного реагування до комплексної моделі міжнародного цифрового врядування [1]. Особливістю цієї моделі є взаємодія міжнародних договорів, актів рекомендаційного характеру, етичних принципів і спеціалізованих процесуальних правил, які не конкурують між собою, а взаємно доповнюють один одного, забезпечуючи більш ефективне регулювання нових цифрових відносин.

Проведене дослідження дає підстави стверджувати, що цифрова трансформація міжнародного права є одним із визначальних напрямів еволюції сучасного міжнародного правопорядку. Її зміст полягає не лише у впровадженні новітніх цифрових технологій у діяльність міжнародних інституцій, а насамперед у глибокому перегляді концептуальних засад міжнародно-правового регулювання. Використання штучного інтелекту, технологій машинного навчання, автоматизованого аналізу даних та цифрових інформаційних ресурсів поступово змінює механізми реалізації міжнародно-правових норм, підходи до встановлення юридично значущих фактів, особливості міжнародного доказування та процедури прийняття рішень. У результаті цифрові технології перетворюються з допоміжних інструментів на один із чинників розвитку міжнародного права, що безпосередньо впливає на його інституційні, процедурні та доктринальні засади.

Поширення систем штучного інтелекту актуалізує необхідність формування нової моделі міжнародно-правового регулювання, у центрі якої мають перебувати принципи прозорості алгоритмічних процесів, можливість зовнішнього контролю, людський нагляд за автоматизованими рішеннями, відповідальність розробників і користувачів таких систем, а також оцінювання ризиків залежно від сфери їх застосування. У сучасних умовах вже недостатньо розглядати штучний інтелект виключно як об'єкт правового регулювання. Значно важливішим стає питання визначення міжнародно-правових гарантій, які

забезпечуватимуть збереження балансу між технологічними інноваціями, міжнародною безпекою, правами людини та принципом верховенства права. Саме тому подальший розвиток міжнародного права повинен відбуватися у напрямі створення комплексної системи міжнародних стандартів, здатних мінімізувати ризики цифровізації без обмеження її потенціалу.

***Висновки до Розділу 3***

Узагальнюючи результати дослідження, можна дійти висновку, що подальша цифрова еволюція міжнародного права потребуватиме не лише оновлення окремих міжнародно-правових норм, а й формування нової концепції міжнародно-правового регулювання цифрового середовища. Її основою мають стати поєднання технологічної ефективності з безумовним дотриманням міжнародно визнаних стандартів прав людини, забезпечення юридичної визначеності алгоритмічних процесів, уніфікація підходів до використання цифрових доказів, розвиток міжнародної співпраці у сфері цифрового правосуддя та вироблення універсальних принципів відповідального застосування штучного інтелекту. Лише за умови випереджального розвитку міжнародно-правових механізмів цифрові технології зможуть стати інструментом зміцнення міжнародного правопорядку, а не джерелом нових правових ризиків. Отже, ключовим викликом для сучасної міжнародно-правової доктрини є забезпечення такого балансу, за якого право не стримуватиме інноваційний розвиток, але водночас збереже свою визначальну роль у гарантуванні справедливості, міжнародної безпеки, захисту прав людини та ефективного функціонування глобальної системи правосуддя.

Для України результати цього дослідження мають особливу цінність, оскільки сучасні умови збройної агресії обумовили безпрецедентне використання цифрових технологій у сфері міжнародного правосуддя та міжнародної відповідальності. У контексті європейської інтеграції України Конвенція про ШІ є важливим інструментом виконання міжнародних

зобов'язань держави та наближення національного законодавства до європейських стандартів цифрового регулювання. Її імплементація сприятиме формуванню узгодженої національної моделі регулювання ШІ, сумісної з європейським правовим простором і практикою міжнародних судових інституцій. Відповідний підхід уже окреслено Міністерством цифрової трансформації України у Білій книзі з регулювання ШІ, що передбачає поступовий перехід від добровільних стандартів та оцінювання впливу до запровадження обов'язкових регуляторних вимог [25]. Саме український досвід став каталізатором практичного випробування нових способів фіксації, накопичення, перевірки та процесуального використання цифрової інформації, яка дедалі частіше набуває статусу ключового доказового джерела у справах про міжнародні злочини. Це означає, що Україна сьогодні виступає не лише суб'єктом застосування вже сформованих міжнародних стандартів, а й своєрідною платформою для їх подальшого вдосконалення. Від ефективності правового врегулювання цифрового доказування значною мірою залежить здатність міжнародних судових інституцій забезпечити належне документування фактів, встановлення індивідуальної та державної відповідальності, а також реалізацію принципу невідворотності покарання за найтяжчі порушення міжнародного права.

Не менш важливим є стратегічний вимір цифрової трансформації міжнародного права для майбутнього розвитку України як європейської правової держави. Інтеграція до єдиного цифрового правового простору Європи, адаптація до міжнародних стандартів регулювання штучного інтелекту та участь у виробленні універсальних правил функціонування цифрових технологій відкривають можливість для посилення ролі України у формуванні нової міжнародно-правової архітектури. За таких умов особливого значення набуває розвиток вітчизняної міжнародно-правової науки, здатної запропонувати власні доктринальні підходи до врегулювання алгоритмічного управління,

використання цифрових доказів, забезпечення цифрової довіри та захисту фундаментальних прав людини в умовах стрімкого технологічного розвитку. Саме поєднання наукових досліджень, міжнародної практики та законодавчих ініціатив може забезпечити Україні не лише ефективну адаптацію до цифрових викликів, а й можливість стати одним із активних учасників формування міжнародних стандартів цифрової доби.

## Список використаних джерел

1. Berkeley protocol on digital open source investigations : a practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law / OHCHR; University of California, Berkeley, Human Rights Center. 2022. CORE/HRP/7/9. URL: https://searchlibrary.ohchr.org/record/30334?ln=ar26

2. Hathaway O. A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J. The Law of Cyber-Attack. *California Law Review*. 2012. Vol. 100, No. 4. P. 817–885. URL: https://lawcat.berkeley.edu/record/1125126/files/fulltext.pdf

3. Поліщук В. П., Панасевич Л. А. Міжнародне право і кібербезпека: визначення правового статусу кібератак та кібервійськових операцій. *Юридичний науковий електронний журнал.* 2024. № 2. С. 503–506. DOI: https://lsej.org.ua/2_2024/126.pdf

4. Карвацька С. Б., Маник А. З., Лабик А. Р. Право на кібербезпеку: співпраця щодо протидії кіберзагрозам в Україні та ЄС. *Юридичний науковий електронний журнал.* 2025. № 2. С. 381–383. DOI: https://doi.org/10.32782/2524-0374/2025-2/89. URL: http://www.lsej.org.ua/2_2025/91.pdf

5. Безпечний ШІ для мільйонів українців: Україна підписала Рамкову конвенцію про штучний інтелект та права людини : Урядовий портал. 15 травня 2025 р. URL: https://www.kmu.gov.ua/news/bezpechnyi-shi-dlia-milioniv-

ukraintsiv-ukraina-pidpysala-ramkovu-konventsiiu-pro-shtuchnyi-intelekt-ta-prava-liudyny

6. Brahimi S., Beziz M. The Digital Transformation of International Law: Navigating the Legal Implications of a Hyperconnected World. *Revue des Sciences Humaines & Sociales.* 2025. Vol. 11, No. 2. P. 216–228. URL: https://asjp.cerist.dz/en/article/284820

7. Cohen J. E. Between Truth and Power: The Legal Construction of Informational Capitalism. Oxford: Oxford University Press, 2018. URL: https://global.oup.com/academic/product/between-truth-and-power-9780190246693?cc=ua&lang=en

8. Binns R. Fairness in Machine Learning: Lessons from Political Philosophy. Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency. 2018. P. 49–58. DOI: https://doi.org/10.1145/3287560.3287593

9. González Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Cham: Springer, 2014. DOI: https://doi.org/10.1007/978-3-319-05023-1

10. Schmitt M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017. URL: https://library.icrc.org/library/docs/DOC/irrc-910-schmitt.pdf

11. Kurbalija J. An Introduction to Internet Governance. 7th ed. Geneva: DiploFoundation, 2016. URL: https://dspace.diplomacy.edu/items/4f2850f0-d64c-42ed-b967-5761e06c6129

12. Key facts: UNESCO's Recommendation on the Ethics of Artificial Intelligence. UNESCO. 2023. URL: https://unesdoc.unesco.org/ark:/48223/pf0000385082

13. Загальний регламент про захист даних (GDPR) : офіційний переклад українською мовою. URL: https://www.kmu.gov.ua/storage/app/media/upload

14. Яцишин М. Ю. Використання сили у кіберпросторі в рамках міжнародного права. *Інформація і право.* 2018. № 4 (27). С. 22–32. DOI: https://doi.org/10.37750/2616-6798.2018.4(27).273367

15. Tene O., Polonetsky J. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property.* 2013. Vol. 11, No. 5. P. 239–273. URL: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip

16. Рамкова Конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права, прийнята на 133-му засіданні Комітету міністрів Ради Європи (Страсбург, 17 травня 2024 року). CM (2024) 52. URL: https://vkksu.gov.ua/sites/default/files/rye_ramkova_konvenciya_zi_shtuchnogo_intelektu_prav_lyudyny_demokratiyi_ta_verh._prava.pdf

17. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias. In: Ethics of Data and Analytics. *Auerbach Publications.* 2022. P. 254–264. DOI: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003278290-37/machine-bias-julia-angwin-jeff-larson-surya-mattu-lauren-kirchner

18. UNESCO. Recommendation on the Ethics of Artificial Intelligence. UNESCO's first-ever global standard on AI ethics, adopted in 2021, is applicable to all 194 member states of UNESCO. 2023. URL: https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

19. 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). 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

20. Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge, Mass: Harvard University Press, 2015. URL: https://www.jstor.org/stable/j.ctt13x0hch

21. United Nations. International Covenant on Civil and Political Rights. 1966. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

22. Gasser U., Almeida V. A Layered Model for AI Governance. IEEE Internet Computing. 2017. Vol. 21, No. 6. P. 58–62. DOI: https://doi.org/10.1109/MIC.2017.4180835

23. De Filippi P., Wright A. Blockchain and the Law: The Rule of Code. Cambridge, Mass.: Harvard University Press, 2018. URL: https://www.hup.harvard.edu/books/9780674241596

24. Берназюк І. М. Рамкова Конвенція Ради Європи про штучний інтелект у контексті захисту прав людини: виклики та значення для України. *Науковий вісник Ужгородського Національного Університету. Серія: Право.* 2026. Вип. 93, ч. 3. С. 18–30. DOI: https://doi.org/10.24144/2307-3322.2026.93.3.2

25. Біла книга з регулювання штучного інтелекту в Україні. Міністерство цифрової трансформації України. 2024. URL: https://thedigital.gov.ua/news/technologies/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-bilu-knigu

# РОЗДІЛ 4
# ЦИФРОВА МОДЕРНІЗАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ ПОДАТКОВОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

**Автори:**

**Пирога Ігор Степанович,** *професор кафедри конституційного права та порівняльного правознавства, доктор юридичних наук, професор, Ужгородський національний університет, ORCID: https://orcid.org/0000-0002-2798-7795*

**Бисага Юрій Михайлович,** *доктор юридичних наук, професор, завідувач кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородськиӣ національниӣ університет», Заслужениӣ юрист України, ORCID: https://orcid.org/0000-0002-8797-5665*

**Пирога Сергій Степанович,** *професор кафедри права, доктор юридичних наук, доцент, Волинський інститут імені В'ячеслава Липинського, ПрАТ «ВНЗ МАУП», ORCID: https://orcid.org/0000-0002-7093-3207*

**Щербатюк Ірина Олександрівна,** *кандидат юридичних наук, доцент кафедри права, Заступник директора, Волинський інститут імені В'ячеслава Липинського ПрАТ «ВНЗ «МАУП, ORCID: https://orcid.org/0009-0008-5943-6104*

Цифрова трансформація суспільних відносин упродовж останніх років істотно змінила умови функціонування держави, економіки та права. Цей процес особливо виразно проявляється у сфері публічних фінансів, де цифрові технології поступово перестають бути лише технічним засобом автоматизації адміністративних процедур і перетворюються на важливий фактор зміни самого механізму формування та реалізації фінансової політики держави. Податкова сфера в цьому відношенні є однією з найбільш чутливих, оскільки саме тут перетинаються публічний інтерес держави у забезпеченні достатніх бюджетних

доходів, економічні інтереси суб'єктів господарювання та приватні інтереси фізичних осіб. Відповідно, цифрова модернізація податкового регулювання повинна розглядатися не як вузькотехнологічна проблема, а як комплексне правове та інституційне явище, пов'язане з трансформацією способів реалізації податкової функції держави, здійснення податкового контролю, забезпечення прав платників та узгодження приватних і публічних інтересів [13; 17; 18].

Для України актуальність зазначеної проблематики визначається сукупністю обставин, які істотно відрізняють сучасний етап реформування податкової системи від попередніх періодів. Повномасштабна збройна агресія Російської Федерації спричинила безпрецедентне навантаження на систему публічних фінансів, зумовивши необхідність одночасного забезпечення обороноздатності держави, соціального захисту населення, функціонування органів державної влади та місцевого самоврядування, підтримання критичної інфраструктури і створення фінансових передумов для майбутнього відновлення. За цих умов стабільність податкових надходжень набуває значення не лише фінансово-економічної, а й безпекової категорії. Податкова система повинна забезпечувати достатню мобілізацію внутрішніх ресурсів, водночас не створюючи такого рівня фіскального навантаження, який би перешкоджав збереженню економічної активності, інвестиціям та відновленню підприємницького сектору [2; 19]. Саме тому пошук нових можливостей підвищення ефективності податкового адміністрування без механічного посилення податкового тиску стає одним із ключових завдань сучасної фінансової політики України.

Важливим інструментом його вирішення виступає цифровізація. Використання інформаційних систем, електронного документообігу, автоматизованої обробки великих масивів даних, ризикоорієнтованих алгоритмів, електронного аудиту та цифрових платформ створює можливість істотно змінити традиційну модель взаємодії між державою і платником

податків. Якщо класична система адміністрування значною мірою базувалася на періодичному декларуванні інформації, документальних перевірках та опрацюванні значних масивів паперових документів, то цифрова модель передбачає постійне використання структурованих даних, автоматизоване виявлення невідповідностей, прогнозування податкових ризиків та більш адресне застосування контрольних заходів [13–18]. При цьому цифровізація здатна одночасно підвищувати ефективність державного контролю та зменшувати адміністративне навантаження на сумлінного платника, що має особливе значення для забезпечення принципів справедливості, рівності та правової визначеності у податкових правовідносинах.

Українська модель цифровізації податкової сфери розвивається в тісному взаємозв'язку з процесом європейської інтеграції. Національна стратегія доходів до 2030 року була сформована саме як рамковий документ реформування податкової та митної сфер, що передбачає зміцнення фіскальної спроможності держави, адаптацію національного законодавства до законодавства Європейського Союзу, удосконалення податкового адміністрування та створення умов для післявоєнного економічного відновлення [2]. Таким чином, цифрова модернізація податкової системи повинна розглядатися у ширшому контексті інституційної адаптації України до європейського правового та адміністративного простору. Європейська інтеграція у цій сфері передбачає не лише формальне наближення законодавчих норм, а й формування спроможної адміністрації, здатної забезпечувати ефективне застосування відповідних правил, здійснювати міжнародний обмін інформацією та використовувати сучасні інструменти податкового контролю [8–12].

Особливе значення у цьому процесі має розвиток електронного аудиту. Впровадження стандартизованих електронних даних бухгалтерського та податкового обліку створює передумови для переходу від переважно документарної моделі контролю до цифрового аналізу господарської діяльності

[17; 18]. Такий підхід дозволяє здійснювати більш комплексний аналіз облікової інформації, виявляти логічні та арифметичні невідповідності, визначати податкові ризики та концентрувати контрольні ресурси на найбільш проблемних операціях. Разом із тим автоматизований аналіз не може підміняти юридичну оцінку поведінки платника. Виявлений інформаційною системою ризик має розглядатися як підстава для подальшої перевірки, а не як автоматично встановлений факт податкового правопорушення.

Водночас саме практичне впровадження цифрових технологій актуалізує низку правових проблем, які не можуть бути вирішені лише шляхом технічної модернізації інформаційних систем. Зростання обсягу даних, що використовуються державою для податкового адміністрування, потребує належного правового визначення порядку їх збору, обробки, зберігання та передачі [5; 6]. Автоматизоване визначення податкових ризиків породжує питання щодо прозорості алгоритмів та можливості особи зрозуміти підстави прийняття рішення щодо неї. Інтеграція інформаційних ресурсів різних державних органів потребує гарантій достовірності інформації та процедур її виправлення. Використання цифрових платформ і великих масивів даних, своєю чергою, посилює значення захисту персональних даних, податкової таємниці та комерційної інформації [5; 11]. Тому цифрова модернізація податкової політики повинна відбуватися в межах правової системи, яка не допускає підміни законності технологічною доцільністю.

Особливого значення набуває проблема співвідношення цифрової ефективності та прав платника податків. Автоматизована система здатна швидше за людину виявляти нетипові операції, розбіжності між різними інформаційними масивами або інші ознаки потенційного ризику, однак наявність цифрового сигналу про ризик не може автоматично ототожнюватися з фактом податкового правопорушення. Юридична оцінка поведінки особи повинна здійснюватися відповідно до визначеної законом процедури та з урахуванням права платника

на пояснення, доказування своєї позиції та оскарження рішення контролюючого органу [1; 5; 39; 40]. Отже, цифровізація має змінювати інформаційну та організаційну основу податкового адміністрування, але не повинна змінювати фундаментальні принципи правового статусу платника.

Актуальність цифрової модернізації посилюється також трансформацією самої структури економіки. Поширення електронної комерції, цифрових послуг, платформної економіки, безготівкових розрахунків та транскордонного руху капіталу ускладнює визначення реальної податкової бази та держави, в якій виникає відповідний об'єкт оподаткування. Економічна діяльність дедалі частіше не прив'язана до одного фізичного місця здійснення господарських операцій, а цифрові активи та дистанційні форми роботи створюють нові форми мобільності доходів. За таких умов ефективність національної податкової системи дедалі більше залежить від можливості держави отримувати, зіставляти та аналізувати інформацію, у тому числі інформацію, що формується за межами національної юрисдикції [17–20; 27–30].

Саме тому цифрова трансформація податкової системи нерозривно пов'язана з розвитком міжнародного інформаційного обміну. Україна поступово інтегрується у міжнародну систему автоматичного обміну податковою інформацією, а сучасна діяльність ДПС включає розвиток інструментів, пов'язаних із виконанням міжнародних зобов'язань у сфері оподаткування. У межах європейського напряму особливе значення мають механізми адміністративного співробітництва, регулювання цифрових платформ та цифровізації ПДВ [8–10]. Це має безпосереднє значення для протидії приховуванню доходів, агресивному податковому плануванню та незаконному переміщенню капіталу.

Інший вимір проблеми пов'язаний із соціальною функцією податків. Податкова система є не лише механізмом наповнення бюджету, а й інструментом реалізації соціальної функції держави. Саме за рахунок податкових надходжень

формується фінансова база соціального захисту, освіти, охорони здоров'я, підтримки населення та функціонування публічних інституцій. Відповідно, ефективність цифрового адміністрування має оцінюватися також через його здатність забезпечувати стабільність доходів бюджету, зменшувати масштаби ухилення від оподаткування та створювати умови для більш справедливого розподілу податкового навантаження [24; 25; 34].

Окремого наукового осмислення потребує цифровізація оподаткування природних ресурсів. Україна володіє значним ресурсним потенціалом, а рентні платежі мають важливе значення для формування доходів державного і місцевих бюджетів. Водночас ефективність рентного оподаткування безпосередньо залежить від достовірності інформації про обсяги видобування, характеристики родовищ, фактичне використання природних ресурсів та економічні показники відповідної діяльності. Тому цифровий облік природних ресурсів, геоінформаційні технології, дистанційний моніторинг та інтеграція даних різних державних реєстрів можуть стати важливими інструментами підвищення прозорості рентних відносин [1; 6; 41; 42]. Для України це має додаткове значення у контексті європейської інтеграції, відновлення економіки та формування сучасної політики управління стратегічними ресурсами.

Насамкінець, цифрова трансформація змінює саму модель взаємодії між учасниками податкових правовідносин. Традиційна модель передбачала переважно вертикальну взаємодію, у якій держава встановлювала податкові правила, а платник був зобов'язаний їх виконувати. Сучасні цифрові платформи створюють передумови для більш складної моделі, у якій поряд із владним регулюванням існують постійна електронна комунікація, автоматизоване інформування, цифрове оскарження, обмін даними та використання сервісних механізмів [8; 17; 21; 24; 40]. Це змінює не саму природу владних податкових повноважень, але спосіб їх реалізації, створюючи передумови для більшої прозорості та передбачуваності взаємодії держави і платника.

У цьому контексті важливого значення набуває проблема узгодження законних інтересів суб'єктів податкових правовідносин. Публічний інтерес полягає у забезпеченні належного надходження податків та фінансової спроможності держави, тоді як приватний інтерес платника пов'язаний із можливістю здійснювати господарську діяльність, користуватися передбаченими законом правами, зберігати конфіденційність інформації та бути захищеним від надмірного втручання держави [21; 24]. Цифрові платформи за належного правового регулювання здатні забезпечувати баланс між цими інтересами, оскільки дозволяють одночасно підвищувати інформаційну спроможність держави та спрощувати реалізацію прав платника.

Таким чином, цифрова модернізація правового регулювання податкової політики України в умовах європейської інтеграції є комплексним процесом, що охоплює не лише технологічну трансформацію податкового адміністрування, а й зміну правових, організаційних та інституційних механізмів реалізації податкової функції держави. Її особливістю є одночасний вплив воєнних викликів, завдань післявоєнного відновлення, європейської інтеграції, глобалізації економічних процесів та розвитку цифрової економіки [2; 17–19]. Саме ця сукупність факторів обумовлює необхідність комплексного дослідження пріоритетів цифровізації податкової політики, її соціальної спрямованості, зарубіжного досвіду цифрового моніторингу капіталів і великих статків, цифрового обліку природних ресурсів та можливостей цифрових платформ для узгодження інтересів учасників податкових правовідносин.

Метою дослідження є визначення сучасних напрямів цифрової модернізації правового регулювання податкової політики України з урахуванням завдань європейської інтеграції, забезпечення фінансової стійкості держави в умовах війни та повоєнного відновлення, а також формулювання пропозицій щодо вдосконалення правового механізму цифрового податкового адміністрування. Для досягнення цієї мети необхідно дослідити сучасні

пріоритети цифровізації податкової політики України та їх відповідність європейським підходам, визначити значення цифрових інструментів для реалізації соціальної функції держави, проаналізувати зарубіжні механізми цифрового контролю транскордонного руху капіталу та оподаткування великих статків, розкрити можливості цифровізації рентних відносин і запропонувати правові підходи до використання цифрових платформ у взаємодії держави та платників податків.

Наукова цінність такого підходу полягає у розгляді цифровізації податкової сфери не як сукупності відокремлених технічних нововведень, а як нового етапу розвитку правового механізму оподаткування. Такий підхід дозволяє поєднати питання цифрового адміністрування, податкового контролю, захисту прав платників, міжнародного інформаційного обміну, соціальної функції оподаткування та управління природними ресурсами в межах єдиної концепції модернізації податкової політики України [17; 19; 24; 41]. Саме це, на нашу думку, відповідає сучасним потребам української держави, яка одночасно проходить складний період війни, реформування публічних фінансів та інституційного наближення до Європейського Союзу.

### 4.1. Пріоритети цифровізації податкової політики України в контексті адаптації до стандартів ЄС

Цифровізація податкової політики України в сучасних умовах повинна розглядатися як складова системної трансформації публічного управління, а не лише як технічне оновлення способів подання податкової звітності або комунікації платника з контролюючим органом. Її зміст визначається одночасним впливом технологічних, економічних, правових та інституційних факторів, серед яких особливе місце посідають європейська інтеграція України, необхідність забезпечення фінансової стійкості держави в умовах повномасштабної війни, розвиток цифрової економіки, зростання

транскордонної мобільності капіталу та необхідність створення сприятливого середовища для післявоєнного відновлення [2; 17–19]. За таких обставин цифрова модернізація податкової сфери набуває значення одного з інструментів забезпечення спроможності держави виконувати свої фінансові та соціальні функції, одночасно дотримуючись принципів верховенства права, правової визначеності, пропорційності та належного врядування.

Європейська інтеграція істотно змінює вимоги до функціонування української податкової адміністрації. У процесі наближення до Європейського Союзу Україна повинна забезпечувати не тільки поступову гармонізацію законодавства з acquis ЄС, а й створення інституційної спроможності для практичної реалізації відповідних норм. У податковій сфері це означає розвиток сучасної адміністрації, здатної працювати з великими масивами інформації, здійснювати ефективний ризикоорієнтований контроль, забезпечувати міжнародний обмін податковими даними та використовувати сумісні з європейськими системами цифрові рішення [8–10; 17–19]. Стратегічний характер цього напряму безпосередньо випливає з Національної стратегії доходів до 2030 року, яка визначає модернізацію адміністрування та адаптацію до європейських стандартів як складові реформування податкової системи [2].

У цьому контексті принципове значення має зміна самої парадигми податкового адміністрування. Традиційна модель передбачала, що основна інформація про діяльність платника надходить до держави через податкову звітність, а її достовірність перевіряється переважно під час контрольних процедур. Цифрова модель поступово ґрунтується на значно ширшій інформаційній базі, що формується з різних державних реєстрів, електронних документів, даних про розрахункові операції, бухгалтерської інформації, міжнародного обміну та інших джерел, використання яких дозволяється законом [6; 14; 17]. Це створює передумови для переходу від переважно документарної моделі контролю до системи управління податковими ризиками на основі даних.

Відповідно, одним із головних пріоритетів цифровізації має стати не максимальне накопичення інформації, а формування інтегрованого та юридично визначеного механізму її використання для прийняття обґрунтованих управлінських рішень.

Такий підхід відповідає загальній тенденції розвитку цифрового урядування у державах Європейського Союзу. Європейська цифрова політика передбачає розвиток сумісних інформаційних систем, безпечного обміну даними та цифрових публічних послуг, а у сфері ідентифікації важливим орієнтиром є європейська рамка цифрової ідентичності [12]. Для податкової сфери це означає поступове формування середовища, у якому інформація може використовуватися між різними адміністративними системами без необхідності багаторазового подання одних і тих самих даних громадянином або підприємством. Для України адаптація до такої моделі має не лише технічний, а й правовий вимір, оскільки потребує визначення повноважень органів, меж доступу до інформації, порядку її використання та відповідальності за порушення встановлених правил [5; 6].

Особливого значення набуває принцип *once-only*, відповідно до якого особа не повинна повторно подавати державі інформацію, якою вона вже законно володіє. У податковій сфері реалізація цього принципу здатна істотно зменшити адміністративні витрати платників та одночасно підвищити якість державних даних. Якщо інформація про юридичну особу, її реєстраційні характеристики, певні майнові або господарські обставини вже міститься у державних інформаційних системах, повторне витребування відповідних документів від платника не відповідає логіці цифрової держави [6; 14; 17]. Водночас практична реалізація такого принципу вимагає чіткого правового визначення того, які саме дані можуть передаватися між органами, у яких випадках та на якій правовій підставі.

Для України це питання має особливу актуальність через значну кількість державних реєстрів та інформаційних систем, які історично формувалися окремими органами влади. Їх функціонування не завжди забезпечує належний рівень сумісності, а відмінності у форматах даних, процедурах доступу та механізмах оновлення інформації можуть створювати ризик виникнення суперечностей. Тому одним із першочергових завдань цифровізації податкової політики слід вважати не просто збільшення кількості електронних сервісів, а забезпечення **інтероперабельності державних інформаційних систем**. Саме здатність різних систем обмінюватися інформацією у стандартизованому та юридично визначеному форматі створює основу для функціонування сучасної цифрової податкової адміністрації [6; 17].

У цьому зв'язку заслуговує на увагу розвиток електронного аудиту. Використання стандартизованих електронних даних бухгалтерського та податкового обліку означає якісну зміну способу взаємодії між платником і контролюючим органом, оскільки податкова адміністрація отримує можливість працювати зі значним масивом облікової інформації, а не лише з окремими документами [2; 17; 18]. У перспективі це може забезпечити більш швидкий аналіз господарських операцій, автоматичне виявлення логічних невідповідностей та формування обґрунтованого переліку ризиків, які потребують додаткової перевірки.

Проте запровадження електронного аудиту потребує обережного правового підходу. Автоматизована обробка бухгалтерської інформації здатна виявляти статистично нетипові або потенційно ризикові операції, однак нетиповість не означає незаконність. Господарська діяльність за своєю природою може містити значну кількість нестандартних операцій, особливо в періоди економічної кризи, війни або структурної перебудови ринку. Тому результати цифрового аналізу повинні розглядатися як інформаційна основа для подальшої юридичної оцінки, а не як самостійний доказ вини платника [1; 5; 39].

Не менш важливим пріоритетом є розвиток ризикоорієнтованого адміністрування. Цифрові технології дозволяють аналізувати значно більший обсяг інформації, ніж це можливо у межах традиційного ручного опрацювання документів. На цій основі держава може визначати характерні моделі ризикової поведінки, встановлювати взаємозв'язки між різними економічними показниками та концентрувати контрольні ресурси на операціях, які мають підвищену ймовірність порушення податкового законодавства [16–18]. Такий підхід відповідає сучасній тенденції переходу від масового контролю до вибіркового контролю на основі об'єктивних критеріїв.

Ризикоорієнтована модель має принципове значення і для захисту прав платників. Чим точніше держава може ідентифікувати реальний ризик, тим менше необхідності здійснювати контроль щодо платників, поведінка яких не свідчить про порушення. Це дозволяє зменшити адміністративні витрати бізнесу, скоротити кількість безрезультатних перевірок та підвищити передбачуваність діяльності контролюючих органів [21]. Водночас така модель повинна бути заснована на чітких критеріях, які відповідають вимогам закону. Використання алгоритмічного аналізу не може створювати необмежену дискрецію податкового органу, оскільки це суперечило б принципу правової визначеності.

Особливої уваги потребує питання прозорості алгоритмічних процедур. Якщо система автоматично визначає платника як ризикового, особа повинна мати можливість отримати інформацію про юридично значущі підстави такого рішення та реалізувати право на його оскарження. Недостатня прозорість алгоритмів може створювати ризик виникнення ситуації, за якої особа фактично не здатна з'ясувати, чому саме її діяльність була визначена як ризикова. Тому подальший розвиток цифрового податкового контролю потребує нормативного закріплення не тільки порядку збору та обробки даних, а й загальних вимог до алгоритмічних процедур, можливості їх перевірки та оскарження результатів автоматизованого аналізу [5; 11; 39; 40].

Іншим стратегічним пріоритетом є подальший розвиток електронної взаємодії з платником. Сучасний електронний кабінет має поступово перетворюватися з технічного каналу подання звітності на комплексне цифрове середовище податкових правовідносин. У ньому платник повинен мати можливість не лише виконувати податкові обов'язки, а й отримувати актуальну інформацію про власний податковий статус, строки виконання обов'язків, результати контрольних процедур, наявність податкового боргу, можливість використання передбачених законом прав та способи оскарження рішень [14; 17; 18]. Така модель відповідає сучасній концепції сервісної держави, у межах якої цифрові технології повинні спрощувати взаємодію людини з публічною адміністрацією.

Сучасні показники використання електронних сервісів свідчать про те, що цифровий формат вже став домінуючим способом взаємодії значної частини платників із податковою адміністрацією. Проте кількісне поширення електронних сервісів повинно супроводжуватися якісним удосконаленням їх функціональності. Важливо, щоб цифровий сервіс не просто дублював паперову процедуру, а скорочував кількість процедур, які необхідно пройти платнику, забезпечував автоматичне отримання необхідної інформації та мінімізував ризик технічних або адміністративних помилок [17–19].

Важливим напрямом є також розвиток проактивного податкового адміністрування. Його сутність полягає у тому, що держава не лише очікує від платника виконання певного обов'язку, а заздалегідь інформує його про відповідні юридичні наслідки, строки та можливі способи виконання вимог законодавства. Такий підхід має потенціал для підвищення добровільного дотримання податкового законодавства. Платник, який своєчасно отримує зрозумілу інформацію про власні обов'язки, має менше підстав для ненавмисного порушення [13–18].

Для України це особливо важливо у період воєнного стану та майбутнього відновлення економіки. Значна частина підприємців функціонує в умовах нестабільного попиту, логістичних труднощів, пошкодження активів, зміни місця здійснення діяльності та інших факторів, які об'єктивно ускладнюють виконання податкових обов'язків. За таких умов податкова адміністрація повинна не тільки виявляти порушення, а й забезпечувати максимально зрозуміле та доступне виконання законних обов'язків. Цифрові інструменти дозволяють реалізувати такий сервісний підхід значно ефективніше, ніж традиційна модель взаємодії [2; 19].

Європейська інтеграція водночас вимагає посилення міжнародної складової цифровізації. Глобалізація економічної діяльності створила ситуацію, за якої інформація, необхідна для визначення податкових зобов'язань резидента, може перебувати в іншій державі. Саме тому сучасна податкова адміністрація повинна бути здатною не лише обробляти внутрішні дані, а й ефективно використовувати міжнародний обмін податковою інформацією [8; 17–20; 27; 30–33; 35–37]. Цифрова сумісність інформаційних систем стає однією з передумов повноцінної участі України у міжнародній системі податкового адміністрування.

Це питання безпосередньо пов'язане з проблемою виведення капіталу та приховування доходів за межами України. У сучасних умовах цифрової економіки переміщення фінансових ресурсів може здійснюватися швидко та через складні корпоративні структури, що істотно ускладнює традиційні форми податкового контролю. Ефективна протидія таким явищам потребує не лише вдосконалення матеріальних норм податкового права, а й створення інформаційної інфраструктури, здатної забезпечувати ідентифікацію пов'язаних осіб, зіставлення інформації про доходи та активи, аналіз транскордонних операцій і використання міжнародних баз даних [20; 30–37].

У цьому контексті важливими є дослідження українських науковців щодо природи та функціонування сучасної податкової системи. Зокрема, у

дослідженні С. С. Пироги обґрунтовується значення принципу джерела у побудові податкової системи, що має безпосередній зв'язок із визначенням юрисдикції, в якій виникає економічний дохід та повинні реалізовуватися відповідні податкові наслідки [27]. У сучасних умовах цифрової економіки ця проблематика набуває додаткового виміру, оскільки визначення джерела доходу дедалі частіше потребує аналізу транскордонних цифрових операцій, мобільних форм капіталу та економічних зв'язків, які не мають очевидної фізичної локалізації [27; 30].

Водночас цифровізація не повинна призводити до автоматичного розширення фіскальних повноважень держави. Розширення доступу до інформації та використання технологій аналізу великих даних має відбуватися на підставі чітких законодавчих положень. Правовий механізм цифрового податкового адміністрування повинен визначати не лише повноваження контролюючого органу щодо отримання інформації, а й межі такого доступу, мету обробки даних, строки їх зберігання, порядок виправлення помилок та відповідальність за неправомірне використання інформації [5; 6; 7].

Окремою проблемою є забезпечення кібербезпеки податкової інформації. В умовах повномасштабної війни державні інформаційні системи стали не лише інструментами адміністрування, а й потенційними об'єктами кібератак. Податкова інформація має значну економічну цінність, а її несанкціоноване розкриття може завдати шкоди як державі, так і конкретним платникам. Тому цифровізація податкової системи повинна супроводжуватися розвитком резервування даних, захисту інформаційних систем, контролю доступу та механізмів відновлення функціонування критичних сервісів у разі технічних або воєнних загроз [5; 7].

Необхідність комплексного підходу до цифрової трансформації податкової служби підтверджується сучасним розвитком міжнародних і національних цифрових рішень. OECD пов'язує цифрову трансформацію податкових

адміністрацій із розвитком цифрової ідентифікації, API, автоматизованого обміну даними, електронного виставлення рахунків, аналітики та використання штучного інтелекту [14–18]. Для України це створює орієнтир не лише щодо окремих технологій, а щодо самої архітектури майбутнього податкового адміністрування.

У перспективі це дозволяє сформулювати принципово нове розуміння цифрової податкової адміністрації. Її головною характеристикою має бути не кількість електронних сервісів, а здатність забезпечувати безперервний, юридично визначений та безпечний рух інформації між платником, контролюючим органом та іншими уповноваженими суб'єктами. У такій системі цифрові технології повинні сприяти одночасному досягненню кількох цілей: збільшенню добровільного виконання податкових обов'язків, зменшенню масштабів ухилення від оподаткування, скороченню адміністративних витрат, підвищенню ефективності податкового контролю та забезпеченню прав платників [17–19; 21].

Таким чином, пріоритети цифровізації податкової політики України в умовах європейської інтеграції доцільно пов'язувати не з окремими технологічними рішеннями, а з формуванням нової моделі податкового адміністрування. Її основними характеристиками мають стати інтегроване управління даними, інтероперабельність державних інформаційних систем, електронний аудит, ризикоорієнтований контроль, міжнародний автоматизований обмін податковою інформацією, розвиток проактивних цифрових сервісів, належний захист інформації та прав платників [2; 6; 17–19]. При цьому цифрова трансформація повинна бути безпосередньо пов'язана із завданнями європейської інтеграції, фінансової стійкості держави, протидії тінізації економіки та створення передумов для повоєнного відновлення.

Зрештою, головним критерієм успішності цифровізації має бути не рівень технологічної складності податкової адміністрації, а якість правового та

економічного результату, якого вона дозволяє досягнути. Якщо цифрові технології сприяють своєчасному та справедливому справлянню податків, зменшують адміністративні витрати, забезпечують рівність платників, підвищують прозорість державного управління та одночасно гарантують належний рівень захисту прав особи, вони стають реальним інструментом модернізації податкової політики. Саме така модель відповідає європейському напряму розвитку України та може забезпечити формування податкової системи, здатної функціонувати в умовах війни, підтримувати процес відновлення економіки і водночас інтегруватися у цифровий простір Європейського Союзу.

### 4.2. Цифрові інструменти податкової політики у забезпеченні функцій соціальної держави

Розгляд цифровізації податкової політики виключно крізь призму підвищення фіскальної ефективності держави є методологічно неповним. Податки забезпечують не лише мобілізацію фінансових ресурсів до бюджетів, а й виконують розподільчу, регулюючу та соціальну функції, через реалізацію яких держава впливає на рівень суспільного добробуту, фінансує соціальні послуги, забезпечує підтримку вразливих категорій населення та створює умови для функціонування систем освіти, охорони здоров'я, соціального захисту і публічної безпеки. У сучасних умовах цифрова трансформація податкового адміністрування повинна тому оцінюватися не лише за критеріями швидкості обробки декларацій або збільшення бюджетних надходжень, а й за її здатністю забезпечувати справедливий розподіл податкового навантаження, доступність передбачених законом соціальних механізмів та належну реалізацію прав платників [24; 25; 34].

Такий підхід відповідає сучасному розумінню держави добробуту, у межах якого податкова система є одним із ключових механізмів перерозподілу суспільного продукту. Саме через податки держава акумулює ресурси, необхідні

для фінансування суспільних благ, а через систему податкових пільг, знижок, звільнень та інших інструментів може впливати на фактичний рівень податкового навантаження різних соціальних та економічних груп. С. С. Пирога, досліджуючи правове регулювання податкової системи, акцентує на взаємозв'язку фіскальної та перерозподільної функцій оподаткування із завданнями соціально орієнтованої держави [34]. Цей висновок має особливе значення для цифрової трансформації, оскільки сучасні інформаційні технології здатні істотно змінити механізми практичного забезпечення зазначених принципів.

У цьому контексті цифрові технології створюють передумови для переходу від переважно універсальної моделі застосування податкових правил до більш диференційованого та адресного механізму реалізації соціальної політики. Якщо держава має можливість оперативно зіставляти інформацію про доходи, майновий стан, зайнятість та інші юридично значущі обставини особи, то з'являється можливість точніше визначати право на передбачені законодавством податкові пільги та інші форми державної підтримки. Водночас саме тут виникає принципова межа: інформаційна спроможність держави повинна використовуватися виключно в межах визначеної законом компетенції. Автоматизоване встановлення соціально значущих обставин не може перетворюватися на неконтрольоване спостереження за приватним життям особи [5; 6].

Особливо важливого значення цифрові інструменти набувають в умовах війни. Повномасштабна збройна агресія Російської Федерації істотно змінила структуру соціальних потреб населення та водночас збільшила навантаження на державні фінанси. Держава змушена одночасно фінансувати оборонні потреби, підтримувати внутрішньо переміщених осіб, забезпечувати соціальні виплати, відновлювати пошкоджену інфраструктуру, підтримувати функціонування системи охорони здоров'я та освіти. За таких умов питання ефективності

податкового адміністрування набуває безпосереднього соціального виміру: кожна гривня, яка не надходить до бюджету внаслідок тінізації або ухилення від оподаткування, потенційно зменшує ресурс держави для виконання відповідних соціальних і безпекових функцій [2; 19].

Проте забезпечення соціальної функції оподаткування не може зводитися до максимізації податкових надходжень. Фіскальна політика, яка ігнорує реальну платоспроможність населення або створює надмірне навантаження на економічно активні групи, здатна породжувати протилежні наслідки: скорочення споживання, зменшення інвестицій, переміщення економічної діяльності в тіньовий сектор та зростання соціальної напруженості. Тому цифровізація має забезпечувати більш точне визначення податкової бази та реального економічного стану платника, що створює можливість для більш обґрунтованого розподілу фіскального навантаження [19; 25; 34].

Одним із найважливіших напрямів у цьому відношенні є автоматизація адміністрування податків на доходи фізичних осіб. Цифрові технології дозволяють поєднувати інформацію, яка надходить від податкових агентів, фінансових установ та інших суб'єктів у межах передбачених законодавством процедур, що потенційно зменшує можливості для приховування доходів. Водночас така інтеграція може спрощувати виконання податкового обов'язку самим громадянином, оскільки частина необхідної інформації може бути доступна в електронному кабінеті або автоматично використовуватися під час формування податкової звітності [14; 17; 18]. Таким чином, цифровізація здатна одночасно посилювати контрольну функцію держави та зменшувати трансакційні витрати платника.

Саме зменшення адміністративного навантаження є одним із найбільш вагомих соціальних ефектів цифровізації. Податковий обов'язок традиційно сприймається як фінансове зобов'язання, однак його реалізація супроводжується певними часовими та організаційними витратами. Платник повинен вести облік,

подавати звітність, отримувати документи, взаємодіяти з контролюючими органами та в окремих випадках підтверджувати обставини, які вже можуть бути відомі державі. Переведення цих процесів у цифрове середовище та інтеграція державних реєстрів дозволяють поступово скорочувати витрати, пов'язані з дотриманням податкового законодавства [6; 14; 17; 18]. Для малого підприємництва та фізичних осіб така економія часу й ресурсів може мати не менше значення, ніж безпосередня величина податкової ставки.

Сервісний характер сучасного податкового адміністрування особливо виразно проявляється в розвитку електронного кабінету платника. Цей інструмент має потенціал перетворитися на основний цифровий простір реалізації не тільки обов'язків, а й прав особи у податковій сфері. Йдеться про отримання інформації про стан розрахунків із бюджетом, подання заяв та декларацій, листування з контролюючими органами, отримання адміністративних послуг, оскарження рішень та доступ до іншої інформації. Розвиток цифрових сервісів та електронної взаємодії є одним із напрямів модернізації податкового адміністрування [14; 17; 18]. Важливо, що цифровий сервіс у такій моделі повинен не просто дублювати паперову процедуру, а змінювати її логіку – робити реалізацію податкових прав швидшою, доступнішою та зрозумілішою.

Особливої актуальності цифрові платформи набули для осіб, які мають обмежені можливості фізичного доступу до державних установ. Для України така проблема набула нового виміру внаслідок переміщення населення, окупації окремих територій, руйнування адміністративної інфраструктури та загальних обмежень, пов'язаних із воєнним станом. Цифрові сервіси дозволяють забезпечувати безперервність податкової взаємодії навіть тоді, коли особа фізично не може відвідати відповідний орган. Водночас цифрова доступність не повинна автоматично означати повну відмову від альтернативних способів реалізації прав: держава повинна враховувати цифрову нерівність, відмінності у

доступі до інтернету, рівень цифрової грамотності та особливі потреби окремих категорій населення [4; 12; 40].

Проблема цифрової нерівності має особливе значення при реалізації соціальної функції податків. Чим більше адміністративних процедур переводиться в електронне середовище, тим більшої уваги потребують особи, які через вік, стан інфраструктури, місце проживання або інші об'єктивні обставини не можуть повною мірою користуватися цифровими сервісами. Тому принцип цифровізації не повинен тлумачитися як обов'язок держави повністю відмовитися від традиційних форм взаємодії. Його зміст має полягати у створенні максимально ефективних цифрових каналів при одночасному забезпеченні реальної доступності податкових прав і процедур для всіх категорій платників [11; 12; 40].

Соціальний потенціал цифровізації проявляється також через можливість більш ефективного адміністрування податкових пільг. Податкова пільга є формою законодавчо встановленого відхилення від загального податкового режиму, обумовленого певною економічною або соціальною метою. Проте фактична реалізація пільги може ускладнюватися необхідністю підтвердження відповідних юридичних обставин. У цифровому середовищі частину інформації, необхідної для встановлення права на пільгу, можна отримувати з державних інформаційних систем, якщо така можливість прямо передбачена законодавством [1; 6]. Це створює передумови для поступового переходу від моделі, за якої особа самостійно доводить державі кожну юридично значущу обставину, до моделі, у якій держава використовує вже наявну інформацію та не перекладає на громадянина зайвий адміністративний тягар.

Водночас автоматизація соціально орієнтованих податкових механізмів потребує особливо високого рівня точності даних. Помилка в інформаційній системі, яка в комерційному адмініструванні може призвести до необхідності додаткового уточнення, у соціальній сфері здатна безпосередньо позначитися на

матеріальному становищі людини. Саме тому для цифрових систем, що використовуються при визначенні податкових пільг або інших соціально значущих наслідків, необхідно встановлювати підвищені вимоги до якості інформації, можливості її оперативного виправлення та обов'язкового людського контролю у випадках, коли автоматизована система формує несприятливе для особи рішення [5; 11; 39; 40].

Цифрові технології можуть бути використані й для підвищення справедливості оподаткування. Однією з фундаментальних проблем податкової політики є нерівномірність фактичного податкового навантаження між суб'єктами, які формально перебувають у схожому правовому становищі. Якщо частина економічних суб'єктів систематично приховує доходи або використовує складні схеми мінімізації податкових зобов'язань, сумлінні платники фактично несуть більшу частину фінансового навантаження. Автоматизований аналіз даних, електронний аудит та міжнародний обмін інформацією можуть сприяти виявленню таких дисбалансів і тим самим реалізовувати не тільки фіскальну, а й соціально-справедливу функцію оподаткування [17–20; 21; 34].

Ця проблема безпосередньо пов'язана з питанням прогресивності та перерозподільної функції податків. Як зазначає С. С. Пирога, ефективне функціонування соціально орієнтованої держави потребує узгодження фіскальної, перерозподільної та стимулюючої функцій оподаткування, а справедливість податкової системи не може бути відокремлена від питання розподілу податкового навантаження між різними групами платників [34]. У цифрову епоху реалізація такого підходу значною мірою залежатиме від спроможності держави отримувати достовірну інформацію про доходи та економічну діяльність, у тому числі транскордонну. Отже, цифровізація не змінює саму природу принципу соціальної справедливості, але створює нові технологічні можливості для його практичного забезпечення [17–20; 34].

Важливе значення має також цифровізація оподаткування нових форм зайнятості. Поширення дистанційної роботи, цифрових платформ та інших нестандартних форм економічної активності породжує питання щодо визначення податкового статусу особи, джерела доходу, податкового агента та порядку сплати податків і соціальних платежів. Загальна тенденція розвитку цифрової економіки об'єктивно вимагає адаптації податкової системи до нових форм створення та отримання доходу [19; 27; 30]. Соціальний вимір цього процесу полягає в необхідності забезпечення належного співвідношення між гнучкістю нових форм зайнятості та гарантіями соціального захисту.

Окремого значення набуває використання цифрових інструментів для боротьби з тіньовою зайнятістю. Неофіційна зайнятість означає не лише недоотримання бюджетом податкових надходжень, а й втрату працівником частини соціальних гарантій, пов'язаних із пенсійним забезпеченням, страхуванням та іншими формами соціального захисту. Інтеграція інформації про трудові відносини, нарахування доходів та сплату відповідних платежів за належного правового регулювання здатна підвищити ефективність виявлення системних порушень. При цьому цифровий контроль повинен бути спрямований передусім на системні моделі ухилення, а не перетворюватися на непропорційне втручання у приватне життя працівників [5; 17; 19].

Значний потенціал має цифровізація адміністрування податкових платежів, пов'язаних із місцевими бюджетами. У системі децентралізації податкові надходження є одним із ключових джерел фінансової спроможності територіальних громад. Чим точніше та оперативніше органи влади володіють інформацією про об'єкти оподаткування, тим ефективніше вони можуть планувати бюджетні видатки та забезпечувати надання соціальних послуг. Інтеграція інформації про нерухомість, землю, господарську діяльність та відповідні податкові зобов'язання створює можливості для зменшення розриву

між фактичним використанням майна та його відображенням у податкових даних [6].

Такий підхід має важливе значення для відновлення територій, постраждалих від війни. Органи місцевого самоврядування повинні мати можливість оперативно оцінювати стан власної податкової бази, прогнозувати надходження та визначати можливості фінансування відновлювальних заходів. Цифрові реєстри та системи аналітики можуть стати інструментом такого планування, однак їх ефективність безпосередньо залежить від достовірності та актуальності даних. Тому цифрова модернізація податкової політики повинна охоплювати не тільки центральний рівень податкового адміністрування, а й інформаційне забезпечення фінансової спроможності територіальних громад [6; 19].

У цьому аспекті цифровізація податкової політики перетинається з ширшою проблемою цифровізації публічних фінансів. Податкові дані можуть бути використані не ізольовано, а як один із компонентів системи управління бюджетними ресурсами. Зіставлення інформації про надходження податків із бюджетним плануванням, соціальними видатками та економічними показниками дозволяє підвищити обґрунтованість державних фінансових рішень. Проте такий інформаційний обмін повинен мати чітке нормативне підґрунтя, оскільки податкова інформація має спеціальний правовий режим, а її використання не може бути довільно розширене за межі встановленої законом мети [1; 5; 6].

Сучасний розвиток цифрового податкового адміністрування також повинен враховувати необхідність забезпечення довіри громадян до держави. Соціальна функція податків реалізується ефективніше тоді, коли платники сприймають податкову систему як справедливу та зрозумілу. Цифрові сервіси здатні сприяти такій довірі, якщо вони забезпечують прозорість процедур, своєчасне інформування та можливість контролювати власні податкові відносини. Проте сама наявність електронного сервісу не гарантує довіри. Якщо

автоматизована система формує незрозумілі рішення, технічні помилки неможливо оперативно виправити, а особа не має ефективного механізму оскарження, цифровізація може, навпаки, посилювати недовіру до держави [11; 17; 21].

Тому центральним принципом цифровізації соціально орієнтованої податкової політики має стати людиноцентричність. Цифрова система повинна бути створена не для зручності самої адміністрації як самоцілі, а для забезпечення належного виконання державою своїх фінансових і соціальних функцій. У практичному вимірі це означає доступність сервісів, зрозумілість інформації, можливість виправлення помилок, реальне право на оскарження, захист персональних даних та недопущення дискримінації за цифровими або соціальними ознаками [5; 11; 12; 40].

У цьому зв'язку особливого значення набуває пропорційність використання автоматизованих систем. Чим серйознішими є юридичні наслідки рішення, тим вищими повинні бути вимоги до його перевірки та можливості втручання уповноваженої посадової особи. Автоматичне формування інформаційного повідомлення про необхідність подати документ і автоматичне визначення податкового зобов'язання, яке породжує безпосередній обов'язок сплати коштів, не можуть розглядатися як юридично тотожні ситуації. В останньому випадку необхідні додаткові гарантії перевірки, пояснення та оскарження [5; 39; 40].

Відповідно, цифровізація податкової політики у сфері соціальної держави повинна розвиватися за принципом диференційованої автоматизації. Технічні та сервісні операції, які не створюють істотного втручання у права особи, можуть бути максимально автоматизовані. Натомість рішення, які безпосередньо впливають на майновий стан людини, її право на податкову пільгу або обсяг податкового зобов'язання, повинні супроводжуватися належним рівнем юридичного контролю [1; 5; 11].

Особливе місце у цьому механізмі повинна посідати якість податкових даних. Цифрова система не може бути справедливішою за інформацію, на якій вона ґрунтується. Якщо державні реєстри містять неповні або суперечливі відомості, автоматизований алгоритм лише відтворюватиме відповідну помилку з більшою швидкістю та у більшому масштабі. Тому одним із базових напрямів цифрової модернізації має бути постійне очищення та актуалізація даних, встановлення механізмів їх верифікації, визначення відповідальності за внесення недостовірної інформації та забезпечення права особи на виправлення даних, що її стосуються [5; 6; 17].

Не менш важливою є проблема інформаційної безпеки. Соціально значущі податкові дані можуть містити відомості про доходи, майно, сімейний стан, місце роботи та інші обставини приватного життя. Концентрація таких даних у цифрових системах підвищує потенційний ризик їх неправомірного використання. Тому принцип цифровізації повинен бути нерозривно пов’язаний із принципом мінімізації даних: держава повинна збирати та використовувати лише ту інформацію, яка є необхідною для визначеної законом мети [5; 7; 11].

Водночас цифрові інструменти створюють можливості для більш ефективної реалізації не тільки податкових пільг, а й ширшого механізму соціальної підтримки через бюджетну систему. Інформаційна сумісність податкових та соціальних реєстрів, якщо вона здійснюється на належній правовій основі, може сприяти виявленню дублювання виплат, швидкому реагуванню на зміни соціального статусу особи та підвищенню адресності державної допомоги. Однак тут особливо важливо не допустити механічного ототожнення податкового та соціального адміністрування. Їхні цілі, правові режими інформації та способи прийняття рішень відрізняються, а тому інтеграція повинна здійснюватися через чітко визначені законодавством канали [5; 6].

Слід також враховувати, що цифровізація може посилювати не тільки перерозподільну, а й стимулюючу функцію податків. Автоматизоване адміністрування спеціальних режимів, інвестиційних стимулів, податкових пільг для інноваційних підприємств або окремих видів економічної діяльності дозволяє зменшувати адміністративні бар'єри для використання таких інструментів. Це особливо актуально для післявоєнного відновлення України, коли податкова політика повинна одночасно забезпечувати бюджетні доходи та стимулювати інвестиційну активність [19; 25]. У такій ситуації цифровий сервіс може стати одним із засобів, за допомогою яких держава робить економічні стимули більш передбачуваними та доступними.

Отже, цифрові інструменти податкової політики мають значний потенціал для забезпечення функцій соціальної держави, але цей потенціал не реалізується автоматично. Для його використання необхідне комплексне правове регулювання, яке одночасно забезпечує фіскальну ефективність, справедливість розподілу податкового навантаження, доступність соціально орієнтованих податкових механізмів та захист прав особи. Цифровізація повинна сприяти виявленню тіньових доходів і забезпечувати рівність платників, але не перетворюватися на інструмент необмеженого контролю; вона має спрощувати реалізацію податкових прав, але не позбавляти особу можливості користуватися традиційними способами захисту; вона повинна підвищувати адресність соціальної політики, але не створювати нові форми цифрової дискримінації [17–19; 24; 34; 40].

Таким чином, у контексті функціонування соціальної держави цифрова модернізація податкової політики повинна базуватися на поєднанні чотирьох взаємопов'язаних начал: *фіскальної спроможності держави, соціальної справедливості, сервісної орієнтації та правової захищеності особи* [19; 24; 34]. Саме їх збалансоване поєднання дозволяє розглядати цифровізацію не як механічну автоматизацію податкових процедур, а як інструмент модернізації

всієї системи публічних фінансів. Для України такий підхід набуває особливого значення в умовах війни й майбутнього відновлення, оскільки ефективність податкової системи безпосередньо визначатиме фінансову спроможність держави забезпечувати соціальні гарантії, підтримувати економічну активність та виконувати конституційно значущі функції.

### 4.3. Зарубіжний досвід цифрового моніторингу та оподаткування вивозу капіталу і великих статків

Цифрова трансформація податкового адміністрування найбільш виразно проявляє своє значення у сфері контролю за транскордонним рухом капіталу, доходами та майновими активами осіб із високою платоспроможністю. Глобалізація фінансових ринків, розвиток цифрових фінансових послуг, поширення дистанційної економічної діяльності та можливість оперативного переміщення коштів між юрисдикціями істотно ускладнили традиційні механізми контролю за податковою базою. Для держави вже недостатньо володіти інформацією лише про доходи та активи, що знаходяться на її території. Ефективне оподаткування дедалі більше залежить від здатності отримувати, зіставляти та юридично використовувати інформацію про активи, доходи і фінансові операції, пов’язані з іншими юрисдикціями [17–20]. Саме тому цифровий моніторинг транскордонних операцій поступово перетворюється на невід’ємну складову сучасної податкової політики.

Для України ця проблематика має особливе значення. В умовах повномасштабної війни та майбутнього масштабного відновлення держава зацікавлена у збереженні внутрішньої податкової бази, недопущенні незаконного виведення коштів за кордон та забезпеченні справедливого розподілу податкового навантаження. Водночас необхідність залучення іноземного капіталу, інтеграції українського бізнесу до європейського економічного простору та розвитку міжнародної економічної діяльності

потребує відмови від надмірно репресивних моделей контролю. Завдання полягає у формуванні такої системи, за якої законна міжнародна економічна діяльність не створює надмірних адміністративних бар'єрів, тоді як штучне переміщення прибутків, приховування активів та агресивне ухилення від оподаткування своєчасно виявляються [19; 30–37].

Сучасна модель міжнародного податкового адміністрування формується передусім під впливом діяльності Організації економічного співробітництва та розвитку. Одним із фундаментальних напрямів цієї роботи стала реалізація міжнародних стандартів податкової прозорості та автоматичного обміну інформацією. Їх значення полягає не тільки у передачі конкретних відомостей про рахунки, доходи чи активи, а у створенні постійної міжнародної інформаційної інфраструктури, яка істотно зменшує можливості використання фінансової непрозорості для приховування доходів [17; 18]. Для України імплементація відповідних механізмів є важливою складовою інтеграції до міжнародного податкового простору.

Автоматичний обмін інформацією сам по собі, однак, не гарантує ефективного оподаткування. Отримані дані повинні бути належним чином структуровані, перевірені та зіставлені з іншими інформаційними масивами. Саме тут цифрові технології набувають самостійного правового та управлінського значення. Якщо податкова адміністрація отримує значні обсяги транскордонної інформації, але не має належних аналітичних інструментів для її опрацювання, міжнародний обмін перетворюється лише на формальну процедуру. Тому наступним етапом після підключення до міжнародних інформаційних систем має бути створення національної спроможності аналізувати великі масиви даних та ідентифікувати невідповідності між задекларованими доходами і фактичними фінансовими можливостями платника [16–19].

Саме в цьому контексті особливого значення набуває концепція *tax gap* – розриву між сумою податкових зобов'язань, яка повинна бути сплачена відповідно до законодавства, і сумою податків, фактично мобілізованою до бюджету. Цифрові технології дозволяють державі точніше визначати причини такого розриву, розмежовуючи випадки ненавмисних помилок, економічних труднощів, використання передбачених законом механізмів оптимізації та свідомого ухилення від оподаткування. Для податкової політики це принципово важливо, оскільки ефективність боротьби з податковим розривом не повинна вимірюватися кількістю перевірок або штрафних санкцій. Її критерієм має бути збільшення добровільного виконання податкових обов'язків та скорочення необґрунтованих втрат бюджету [17–19].

Одним із найбільш важливих напрямів міжнародної податкової політики є протидія розмиванню податкової бази та переміщенню прибутків до низькоподаткових юрисдикцій. Сучасні механізми BEPS спрямовані на забезпечення такого оподаткування прибутку, яке більше відповідає місцю здійснення реальної економічної діяльності та створення економічної вартості [20; 30; 35]. Цифровізація посилює практичні можливості реалізації цих принципів, оскільки сучасні системи можуть автоматизовано аналізувати корпоративні структури, транскордонні платежі, відносини між пов'язаними особами та інші показники, які можуть свідчити про штучне переміщення прибутку.

Для України проблема є особливо актуальною через транскордонну діяльність українського бізнесу та необхідність забезпечення конкурентного середовища для підприємств, які сумлінно виконують податкові обов'язки. Використання складних корпоративних структур або юрисдикцій із пільговим режимом оподаткування не є незаконним саме по собі. Проблема виникає тоді, коли юридична конструкція використовується без реального економічного змісту виключно для отримання необґрунтованої податкової переваги. Тому

цифровий контроль повинен бути спрямований не на сам факт міжнародної діяльності, а на виявлення невідповідності між юридичною формою операції та її економічним змістом [30; 31; 35; 37].

Значний розвиток у цій сфері отримали механізми забезпечення прозорості бенефіціарної власності. Виявлення кінцевого власника юридичної структури має принципове значення для визначення того, хто фактично контролює актив або отримує економічну вигоду від операції. Для податкової системи це особливо важливо у випадках, коли активи формально належать декільком юридичним особам, зареєстрованим у різних юрисдикціях. Цифрові реєстри бенефіціарної власності та механізми обміну відповідною інформацією дозволяють державі перейти від аналізу формального власника до встановлення фактичного контролю [6; 17; 33].

Європейський Союз у цьому напрямі послідовно розвиває правові механізми прозорості та адміністративної співпраці. Система DAC стала одним із центральних інструментів обміну податковою інформацією, а її подальший розвиток охопив нові форми економічної діяльності. Особливого значення набули правила щодо діяльності цифрових платформ, які передбачають збір та автоматичний обмін відповідною інформацією між податковими адміністраціями [8]. Подальше реформування цифрового оподаткування ЄС доповнюється пакетом *VAT in the Digital Age*, спрямованим на посилення цифрового адміністрування ПДВ, електронне виставлення рахунків та розвиток цифрової звітності [9; 10].

Поява нових правил щодо цифрових платформ є особливо показовою для сучасної трансформації податкової політики. Цифрові платформи демонструють, наскільки швидко технологічні зміни можуть створювати нові форми отримання доходів, які складно контролювати традиційними методами. Європейський підхід полягає у тому, щоб поширювати вимоги до податкової прозорості на нові форми фінансової та підприємницької діяльності, не

допускаючи утворення «цифрових зон» поза сферою ефективного податкового контролю [8–10].

Цей досвід має безпосереднє значення для України, яка поступово інтегрує своє законодавство до європейського правового простору. Українська податкова політика повинна враховувати, що цифрова економіка не скасовує принцип територіальної юрисдикції держави, але істотно ускладнює його практичну реалізацію. Якщо дохід створюється, отримується або переміщується через декілька юрисдикцій, визначення держави, яка має право на оподаткування, потребує використання міжнародних стандартів і механізмів інформаційного обміну [27; 30; 32; 37].

Окремий напрям зарубіжного досвіду становить цифровий контроль за великими статками. У багатьох державах високий рівень майнової концентрації супроводжується використанням складних структур володіння, холдингів, фондів та інших юридичних механізмів. Формально кожна окрема операція може відповідати законодавству, однак сукупність таких структур здатна істотно ускладнювати визначення реального власника та загального обсягу активів. Цифровізація дозволяє податковим органам переходити від аналізу окремих об’єктів до аналізу сукупності активів і фінансових зв’язків [17–20; 33; 34].

У цьому аспекті цифрові технології дозволяють формувати комплексний інформаційний профіль платника на основі законно отриманих даних про доходи, нерухомість, фінансові активи, корпоративні права та транскордонні операції. Метою такого аналізу не повинно бути встановлення додаткового податкового обов’язку виключно через розмір майнового стану особи. Його призначення полягає у встановленні відповідності між задекларованими доходами та фактичними економічними можливостями платника. Такий підхід дозволяє виявляти випадки прихованого доходу, використання складних схем переміщення активів або інших обставин, які потребують подальшого правового аналізу [17–19; 34].

Водночас дискусія щодо оподаткування великих статків не може зводитися до механічного запровадження окремого податку на багатство. Міжнародний досвід демонструє різноманітність моделей оподаткування високих доходів і майнових активів, а їх ефективність значною мірою залежить від якості адміністрування, міжнародного обміну інформацією та здатності держави запобігати переміщенню оподатковуваних активів у непрозорі юрисдикції [18–20; 34]. Для України механічне копіювання окремої моделі було б недоцільним без урахування структури національної економіки, рівня тінізації, інвестиційних потреб та особливостей воєнної економіки.

У цьому аспекті цифровізація створює передумови для більш обґрунтованого вирішення питання про податкове навантаження на великі статки. Без достовірної інформації про сукупний майновий стан особи будь-яка модель оподаткування багатства ризикує стати формальною. Якщо значна частина активів перебуває за межами країни, зареєстрована через іноземні компанії або належить особі через складні корпоративні структури, національна база даних не відображатиме реального обсягу майнових ресурсів. Саме тому ефективне оподаткування великих статків неможливе без міжнародного обміну інформацією, цифрової ідентифікації бенефіціарних власників та інтегрованого аналізу активів [17–20; 27; 33; 34].

Також, цифровізація змінює сам характер податкового контролю. Раніше податковий орган переважно перевіряв документи, які перебували у розпорядженні платника або були отримані в межах конкретної перевірки. Сучасна модель дозволяє формувати цифровий профіль платника на основі великої кількості законно отриманих даних. Проте такий профіль не повинен перетворюватися на юридичну презумпцію порушення. Його функція – визначення рівня ризику та необхідності додаткового аналізу. Остаточний висновок про порушення повинен ґрунтуватися на належних доказах і відповідати процедурним гарантіям [5; 11; 39; 40].

Важливою проблемою є також визначення співвідношення між цифровим моніторингом і правом на приватність. Інформація про фінансові активи, доходи та майно належить до даних, які можуть мати особливо чутливий характер. Міжнародний автоматичний обмін інформацією є допустимим лише за умови існування належної правової бази, гарантій конфіденційності та безпеки даних. Тому імплементація міжнародних стандартів податкової прозорості повинна супроводжуватися не тільки технічною інтеграцією інформаційних систем, а й розвитком правових механізмів відповідальності за незаконне використання або розголошення отриманої інформації [5; 7; 11; 17].

Для України ця вимога має особливе значення з огляду на європейський курс розвитку системи захисту персональних даних. Інтеграція до європейського цифрового простору не може відбуватися шляхом одностороннього розширення державного доступу до інформації. Навпаки, необхідно забезпечити баланс між податковою прозорістю та фундаментальними правами людини. Саме такий баланс є одним із ключових критеріїв правової держави в цифрову епоху [5; 11; 40].

Не менш важливою є проблема виведення капіталу через трансфертне ціноутворення. Контроль за операціями між пов’язаними особами традиційно належить до найбільш складних напрямів податкового адміністрування, оскільки вимагає встановлення відповідності ціни принципу «витягнутої руки» та оцінки економічної сутності операції. Використання цифрової аналітики дозволяє порівнювати великі масиви міжнародних операцій, виявляти нетипові відхилення та формувати ризикові профілі платників. У поєднанні з міжнародним обміном інформацією це створює значно ефективнішу систему протидії штучному переміщенню прибутку [17–20; 35; 36].

Важливе місце в сучасній системі міжнародної податкової прозорості посідає також звітування міжнародних груп компаній. Інформація про розподіл доходів, прибутку, податків та економічної активності між юрисдикціями

дозволяє податковим адміністраціям оцінювати, чи відповідає географія отриманого прибутку фактичному розміщенню економічної діяльності [20; 35]. Для України використання таких інструментів особливо важливе в умовах інтеграції національної економіки до європейського ринку.

Разом із тим цифровий моніторинг транскордонних фінансових потоків повинен бути спрямований на законодавчо визначені ризики, а не на загальний контроль усіх операцій. Надмірна кількість автоматизованих перевірок може створювати значні адміністративні витрати для бізнесу та блокувати нормальну міжнародну діяльність. Тому ефективною є модель, у якій цифрова система здійснює первинний аналіз і ранжування ризиків, після чого контрольні ресурси спрямовуються на найбільш обґрунтовані випадки [17–19; 21].

Для української податкової політики це має принципове значення. Після завершення війни країна буде зацікавлена у значному припливі приватних інвестицій, а отже, податкове регулювання транскордонного руху капіталу не може будуватися виключно на обмежувальних механізмах. Інвестор повинен мати можливість швидко та зрозуміло визначити свої податкові обов’язки, а держава –отримувати необхідну інформацію для запобігання незаконному переміщенню прибутку. Цифровізація може забезпечити саме такий баланс, якщо її правова конструкція буде побудована на принципах передбачуваності, пропорційності та міжнародної сумісності [19; 27; 30–37].

Значний потенціал має також застосування штучного інтелекту та машинного навчання для виявлення нетипових фінансових моделей. Такі технології можуть аналізувати взаємозв’язки між великою кількістю економічних показників, які фізично неможливо опрацювати вручну. Проте використання алгоритмів машинного навчання у податковій сфері потребує особливої обережності. Алгоритмічна модель може виявити статистичну закономірність, але не здатна сама по собі визначити юридичну протиправність поведінки. Отже, результати автоматизованої аналітики повинні залишатися

інструментом для професійної діяльності податкового органу, а не замінювати юридичну оцінку [17; 39].

З огляду на це перспективною для України є модель, за якої цифрова система формує ризиковий сигнал, а уповноважений працівник податкового органу здійснює його правову та фактичну перевірку. Такий механізм дозволяє використати переваги штучного інтелекту, одночасно зберігаючи принцип відповідальності публічної адміністрації за прийняте рішення. Він також забезпечує можливість оскарження несправедливого або помилкового результату автоматизованого аналізу [5; 39; 40].

Зарубіжний досвід переконливо демонструє, що цифровий контроль за капіталом не є окремою технологічною функцією податкової адміністрації. Він є частиною глобальної системи фінансової прозорості, яка включає автоматичний обмін інформацією, контроль бенефіціарної власності, трансфертне ціноутворення, протидію розмиванню податкової бази, регулювання цифрових платформ та нових форм фінансової діяльності [8; 17–20; 30–37]. Україна, рухаючись у напрямі членства в Європейському Союзі, повинна розглядати ці елементи як взаємопов’язану систему, а не як сукупність окремих реформ.

При цьому цифровізація не повинна використовуватися як аргумент для запровадження надмірного фіскального втручання. Оподаткування великих статків та контроль за виведенням капіталу є легітимними цілями державної політики лише за умови їх реалізації відповідно до закону. Належна податкова система повинна однаково захищати як публічний інтерес у мобілізації доходів бюджету, так і приватний інтерес у збереженні законно набутого майна та здійсненні економічної діяльності [1; 5; 11; 34].

Отже, зарубіжний досвід цифрового моніторингу свідчить про формування нової моделі міжнародного податкового контролю, основою якої є не фізичне переміщення документів між державами, а автоматизований обмін

структурованими даними. Для України найбільш перспективними напрямами є подальша імплементація міжнародних стандартів автоматичного обміну інформацією, розвиток контролю бенефіціарної власності, удосконалення трансфертного контролю, регулювання доходів від цифрових платформ та розвиток ризикоорієнтованої аналітики [8; 17–20; 30–37].

У сфері оподаткування великих статків принциповим має залишатися не саме встановлення високого рівня майнового забезпечення особи, а забезпечення відповідності між її фактичним економічним становищем і виконанням податкових обов'язків. Саме тут цифрові технології можуть відіграти ключову роль: вони дозволяють поєднувати інформацію про різні категорії активів, транскордонні операції та корпоративні зв'язки, забезпечуючи більш повне уявлення про податкову базу. Проте отримана інформація повинна використовуватися лише в межах закону, з дотриманням гарантій приватності, конфіденційності та права на ефективний захист [5; 11; 17; 34].

Таким чином, для України цифровізація контролю за транскордонним рухом капіталу повинна розглядатися як складова європейської інтеграції та одночасно як інструмент забезпечення фінансової стійкості держави в умовах війни та післявоєнного відновлення. Йдеться не про встановлення тотального цифрового контролю над фінансовою поведінкою громадян і підприємств, а про формування сучасної системи податкової прозорості, в якій законна міжнародна економічна діяльність захищається, а штучне приховування доходів та переміщення оподатковуваної бази своєчасно виявляються [19; 30–37]. Саме такий підхід відповідає сучасній європейській тенденції розвитку податкового права та створює нормативні й технологічні передумови для подальшої модернізації української податкової системи.

### 4.4. Правове регулювання рентних відносин в умовах упровадження цифрових технологій обліку природних ресурсів

Рентні відносини посідають особливе місце у системі публічних фінансів, оскільки безпосередньо пов'язані з використанням природних ресурсів, які мають не лише економічну, а й суспільну та стратегічну цінність. Надра, водні, лісові та інші природні ресурси є об'єктами особливого правового режиму, а їх використання породжує комплекс відносин між державою, територіальними громадами та суб'єктами господарювання. У податково-правовому вимірі ці відносини матеріалізуються, зокрема, через справляння рентної плати, яка є одним із механізмів вилучення до публічних фондів частини економічної вигоди, отриманої внаслідок використання природного ресурсу. У сучасних умовах цифрової трансформації економіки традиційні підходи до обліку природних ресурсів та визначення податкових зобов'язань поступово потребують перегляду, оскільки точність рентного оподаткування дедалі більше залежить від якості інформації про фактичні обсяги, місце, спосіб та економічні результати використання відповідного ресурсу [1].

Податковий кодекс України визначає рентну плату як загальнодержавний податок, що охоплює, зокрема, плату за користування надрами для видобування корисних копалин, плату за користування надрами в цілях, не пов'язаних із видобуванням корисних копалин, рентну плату за спеціальне використання води та лісових ресурсів [1]. Така конструкція свідчить про комплексний характер рентного оподаткування та про те, що цифровізація відповідних відносин не може обмежуватися автоматизацією подання податкової декларації. Йдеться про необхідність створення цілісної інформаційної системи, у якій дані про природний ресурс, право на його використання, фактичний обсяг видобування чи споживання, результати господарської діяльності та податкові зобов'язання можуть бути взаємопов'язані.

Принципове значення має те, що рентне оподаткування ґрунтується на інформації про фізичні та економічні характеристики використання природного ресурсу. Для визначення податкового зобов'язання недостатньо знати лише про

існування спеціального дозволу або факт реєстрації суб'єкта господарювання. Необхідно встановити, який саме ресурс використовується, у якому обсязі, на якій ділянці, протягом якого періоду, за яких технологічних умов та з якою економічною результативністю. У традиційній системі такі відомості можуть формуватися в різних інформаційних масивах, що належать різним органам державної влади. Відсутність їх належної інтеграції створює ризик розбіжностей між даними дозвільної системи, ресурсного обліку та податкової звітності [6].

Саме тому цифровізація обліку природних ресурсів повинна розглядатися як передумова підвищення якості самого податкового регулювання. Якщо держава володіє достовірною цифровою інформацією про фактичне використання природного ресурсу, можливості для заниження податкової бази істотно скорочуються. Водночас цифровий облік дозволяє зменшити залежність контролюючого органу від інформації, яку сам платник надає у звітності. Податкова декларація в такій моделі перестає бути єдиним або основним джерелом інформації про об'єкт оподаткування, а перетворюється на один з елементів ширшої системи цифрової верифікації [6; 17; 18].

Особливого значення це набуває у сфері користування надрами. Розвідка, видобування та первинна переробка корисних копалин є видами діяльності, де розбіжність між фактичним обсягом використання ресурсу та даними, які надходять до держави, може мати істотні бюджетні наслідки. Податковий кодекс передбачає, що платниками рентної плати за користування надрами для видобування корисних копалин є суб'єкти господарювання, які набули право користування відповідною ділянкою надр на підставі спеціального дозволу [1]. Отже, право користування природним ресурсом, його фактична реалізація та виникнення податкового обов'язку є взаємопов'язаними юридичними фактами, інформація про які повинна узгоджуватися в цифровому середовищі.

У сучасних умовах особливого значення набуває цифрове картографування природних ресурсів та просторове позиціонування об'єктів

користування надрами. Геоінформаційні системи дозволяють поєднувати інформацію про межі земельних ділянок, розташування родовищ, спеціальні дозволи, фактичні обсяги видобування та інші характеристики. Такий підхід дозволяє перейти від суто документального контролю до просторово-інформаційного аналізу використання природних ресурсів. Для держави це означає можливість швидше виявляти ситуації, коли фактична діяльність не відповідає даним дозвільної документації, а для платника –більш чітке визначення меж та правового статусу об'єкта користування.

Водночас цифровий облік не повинен створювати ілюзію абсолютної точності. Природні ресурси мають фізичні характеристики, які не завжди можуть бути безпосередньо визначені цифровими засобами. Дані дистанційного зондування, геологічних досліджень, автоматизованого вимірювання або виробничих систем можуть містити похибки. Тому правове регулювання цифрового обліку повинно передбачати методологію визначення достовірності даних, порядок їх верифікації та процедури виправлення помилок. Особливо це важливо тоді, коли цифрова інформація використовується для визначення розміру податкового зобов'язання [1; 5; 6].

Важливим напрямом сучасної трансформації є цифровізація спеціальних дозволів на користування надрами. Перехід від паперової дозвільної документації до електронних реєстрів дозволяє забезпечувати оперативний доступ до інформації про суб'єкта користування, ділянку надр, строк дії дозволу, умови користування та інші юридично значущі характеристики. Це підвищує прозорість використання природних ресурсів і створює передумови для автоматичного зіставлення інформації між дозвільною системою та податковою адміністрацією [6].

Водночас принципова проблема полягає у необхідності забезпечення юридичної сили цифрових даних. Якщо інформація про об'єкт природокористування міститься в декількох державних системах і між ними

виникають розбіжності, законодавство повинно чітко визначати, які дані мають пріоритет, хто відповідає за їх актуальність і яким чином платник може оскаржити неправильну інформацію. В іншому випадку цифровізація може не зменшити, а збільшити кількість спорів між державою та суб'єктами господарювання [5; 6].

Сучасне рентне оподаткування поступово переходить від контролю за декларацією до контролю за **ланцюгом формування податкової бази**. Для надрокористування такий ланцюг може включати право на користування ділянкою надр, фактичний обсяг видобування, характеристики отриманої сировини, її переробку, реалізацію та фінансовий результат. Цифрова інтеграція цих елементів дозволяє виявляти розбіжності на різних етапах руху ресурсу та запобігати заниженню рентних платежів [1; 6; 17].

Особливого значення набуває автоматизація обліку фізичних обсягів видобування. Сучасні технології промислового обліку, дистанційного моніторингу, геоінформаційних систем та автоматизованого вимірювання можуть використовуватися для отримання даних безпосередньо з місця видобування. У перспективі це створює можливість переходу до моделі, коли певна частина інформації про об'єкт рентного оподаткування надходить до державних систем безпосередньо з технологічного середовища підприємства. Проте така модель потребує спеціальних правових вимог до сертифікації обладнання, достовірності показників, захисту каналів передачі інформації та відповідальності за втручання в цифрові системи обліку [5; 7; 17].

Не менш важливим є питання інтеграції податкової інформації з геологічними та екологічними даними. Використання природного ресурсу має не лише фіскальний наслідок, а й екологічний. Обсяг видобування, спосіб використання ресурсу та характер господарської діяльності можуть впливати на стан навколишнього природного середовища. У перспективі інтеграція відповідних інформаційних систем могла б забезпечити комплексніший

контроль за використанням природних ресурсів, у межах якого економічні та екологічні наслідки діяльності оцінювалися б на основі узгоджених даних [6; 41].

Для України ця проблематика набуває особливої актуальності через стратегічне значення мінеральних ресурсів для післявоєнного відновлення та розвитку нових промислових секторів. Критично важливі мінеральні ресурси можуть стати одним із напрямів залучення інвестицій та інтеграції української економіки до європейських виробничих ланцюгів. Проте використання такого потенціалу потребує одночасного забезпечення прозорості надрокористування та справедливого розподілу економічної вигоди від використання природних ресурсів. Цифровий облік може стати одним із механізмів досягнення цього балансу [41].

Дослідження українських авторів щодо критичної сировини підтверджують, що актуалізація геологічної інформації, верифікація запасів та її цифровізація безпосередньо пов’язані з реалізацією Ukraine Facility та європейською інтеграцією України [41]. Саме тому цифровізація ресурсної інформації повинна розглядатися не лише як адміністративна реформа, а як елемент формування інвестиційно привабливого та прозорого середовища для розвитку ресурсного сектору.

Важливим компонентом прозорості є відкритість інформації про видобувні галузі. Україна тривалий час бере участь у міжнародній Ініціативі прозорості видобувних галузей (EITI), яка передбачає розкриття інформації про управління природними ресурсами та доходи від їх використання. Водночас війна створила об’єктивні обмеження для повного розкриття інформації щодо окремих територій. У 2025 році Правління EITI погодило для України адаптоване застосування стандарту щодо територій, тимчасово окупованих Російською Федерацією [42]. Це демонструє необхідність пошуку балансу між принципом прозорості природокористування та вимогами національної безпеки.

У цьому аспекті цифровізація створює подвійний ефект. З одного боку, вона дозволяє підвищувати прозорість шляхом відкритих реєстрів, електронних карт, цифрових дозволів та автоматизованого оприлюднення інформації. З іншого боку, концентрація детальної інформації про розташування родовищ, обсяги видобування та критичну інфраструктуру може створювати додаткові ризики в умовах війни. Тому законодавство повинно передбачати диференційований режим доступу до інформації: дані, що мають суспільне значення, повинні бути максимально відкритими, тоді як інформація, розголошення якої може створювати реальні загрози національній безпеці, повинна захищатися відповідно до закону [5; 7; 42].

Цифровий облік природних ресурсів має значення і для забезпечення належного розподілу рентних доходів між різними рівнями бюджетної системи. Якщо інформація про обсяг використання ресурсу є достовірною та оперативною, відповідні платежі можуть бути точніше прогнозовані, а бюджетне планування – здійснюватися на більш обґрунтованій інформаційній основі. Особливо це важливо для територіальних громад, на території яких здійснюється природокористування. Надходження від використання природних ресурсів можуть бути істотним джерелом фінансової спроможності місцевого самоврядування, а тому цифровий облік має не лише податкове, а й муніципально-фінансове значення [1; 6].

В умовах війни роль рентних платежів набуває додаткового значення. Податкова система повинна забезпечувати мобілізацію доходів, необхідних для фінансування оборони, соціальних видатків та функціонування держави. Водночас природоресурсні платежі мають особливість: вони пов’язані з використанням активів, які не створені самим суб’єктом господарювання, а належать Українському народу та перебувають під особливою охороною держави відповідно до Конституції України. Отже, ефективне рентне

оподаткування є не лише питанням бюджетної техніки, а й механізмом реалізації публічного інтересу щодо справедливого використання природного багатства.

Перспективним напрямом є створення єдиного цифрового інформаційного середовища природокористування, у якому дані про ресурс існували б протягом усього його життєвого циклу – від геологічного дослідження та отримання права користування до видобування, реалізації, переробки та припинення користування. Для податкової системи така модель означала б можливість автоматизованого отримання інформації про податково значущі юридичні та фактичні обставини. Для держави загалом – формування єдиного інформаційного простору управління природним капіталом [6; 17; 41].

Однак створення такої системи потребує чіткого розмежування повноважень між органами державної влади. Дані про надра, землю, водні та лісові ресурси можуть перебувати у віданні різних суб'єктів публічної адміністрації. Цифрова інтеграція не повинна означати механічного об'єднання всіх баз даних в одну систему. Значно важливішим є встановлення стандартизованих протоколів обміну інформацією, визначення юридично значущих наборів даних, відповідальних розпорядників інформації та процедур її актуалізації [6].

Необхідність правового врегулювання особливо проявляється у випадках, коли цифрові дані використовуються як підстава для донарахування рентної плати. Якщо автоматизована система встановлює розбіжність між обсягом видобування та даними декларації, платник повинен мати можливість ознайомитися з інформацією, на якій ґрунтується відповідний висновок, надати пояснення та докази, а також оскаржити рішення контролюючого органу. Отже, цифровий доказ повинен включатися у загальну систему доказування, а не створювати окремий, неконтрольований вид фіскального доказу [1; 5].

У перспективі доцільним є нормативне закріплення принципу *цифрової простежуваності природного ресурсу.* Його зміст може полягати у можливості

встановити за допомогою законно отриманих цифрових даних походження ресурсу, його обсяг, правову підставу використання, переміщення, переробку та реалізацію. Для мінеральної сировини це особливо важливо, оскільки цифрова простежуваність може одночасно використовуватися у податковому, митному, екологічному та інвестиційному регулюванні [6; 41].

Застосування такого підходу може мати значний антикорупційний ефект. Чим більша частина інформації про використання природних ресурсів існує у стандартизованому цифровому форматі, тим менше можливостей для маніпулювання паперовими документами, приховування обсягів або вибіркового доступу до інформації. Проте цифровізація сама собою не усуває корупційних ризиків. Вона лише переносить частину таких ризиків у цифрове середовище, де вони можуть проявлятися через неправомірне редагування даних, несанкціонований доступ, маніпуляції алгоритмами або зловживання повноваженнями адміністратора системи [5; 7].

Важливим є і питання технологічної нейтральності законодавства. Правові норми не повинні надмірно прив’язуватися до конкретної технології, яка через декілька років може стати застарілою. Доцільніше визначати юридичні вимоги до достовірності, цілісності, доступності та простежуваності даних, залишаючи технічні способи їх забезпечення предметом відповідного підзаконного та технічного регулювання. Такий підхід дозволить модернізувати інформаційні системи без постійного внесення змін до базових податкових норм [1; 6].

Особливого значення набуває також питання використання штучного інтелекту для прогнозування обсягів видобування та виявлення аномальних показників. Поєднання даних про історичні обсяги видобутку, виробничі потужності, геологічні характеристики, експорт, ціни та інші показники може дозволити формувати моделі ризику. Проте такі моделі повинні використовуватися лише як інструмент аналітичного відбору. Юридична

відповідальність не може ґрунтуватися виключно на математичному прогнозі без встановлення конкретного факту порушення [17; 39].

Отже, цифровізація рентних відносин передбачає якісну зміну всієї системи державного управління природними ресурсами. Її перспективна модель повинна поєднувати електронний облік прав на природокористування, цифрове картографування ресурсів, автоматизоване отримання даних про фактичне використання, інтеграцію інформації про видобування та реалізацію, електронне декларування, ризикоорієнтований податковий контроль і міжнародні стандарти прозорості [1; 6; 17; 41; 42]. При цьому центральним принципом має залишатися достовірність інформації та можливість її юридичної перевірки.

Для України така модель має стратегічне значення. В умовах війни цифровий облік природних ресурсів повинен забезпечувати не лише збільшення бюджетних надходжень, а й збереження державного контролю над стратегічними ресурсами, прозорість їх використання та стійкість системи управління. У період післявоєнного відновлення цифрова інфраструктура природокористування може стати основою для залучення інвестицій, розвитку критичної сировинної бази та інтеграції української економіки до європейських ланцюгів створення вартості [19; 41].

Відповідно, модернізація рентного оподаткування не повинна обмежуватися зміною ставок або формул розрахунку рентної плати. Її сутність має полягати у створенні інформаційно та юридично узгодженої системи, за якої держава точно знає, *який природний ресурс, ким, на якій правовій підставі, у якому обсязі та з яким економічним результатом використовується.* Лише за такої умови рентний платіж може виконувати не тільки фіскальну, а й регулятивну та ресурсозберігаючу функції [1; 41].

Таким чином, цифрові технології здатні істотно підвищити ефективність правового регулювання рентних відносин, але лише за умови їх поєднання з належними юридичними гарантіями. Цифровий облік природних ресурсів

повинен забезпечувати прозорість і простежуваність їх використання, інтеграцію між дозвільними, ресурсними та податковими системами, підвищення точності визначення податкової бази та зменшення можливостей для тінізації природокористування. Водночас він повинен гарантувати достовірність даних, право платника на їх перевірку та виправлення, належний захист інформації і можливість ефективного оскарження рішень, прийнятих із використанням цифрових даних [5–7].

У цьому полягає принципова відмінність цифрової модернізації від простої електронізації рентної звітності. Електронна декларація лише змінює форму передачі інформації, тоді як цифрова модель змінює **саму архітектуру правовідносин**, переводячи державний контроль від періодичного документального підтвердження до безперервного інформаційного моніторингу використання природного ресурсу. Саме така трансформація є найбільш перспективною для України в контексті європейської інтеграції, цифрової перебудови публічного управління та необхідності забезпечення справедливого використання природного багатства в умовах війни та майбутнього відновлення [2; 19; 41; 42].

### 4.5. Використання цифрових платформ для узгодження законних інтересів суб’єктів податкових правовідносин

Цифрова трансформація податкової сфери України на сучасному етапі виходить далеко за межі технічного переведення окремих адміністративних процедур в електронну форму. Йдеться про поступову перебудову всієї системи взаємодії держави, платників податків та інших учасників податкових правовідносин на основі цифрових технологій, інтегрованих інформаційних систем, автоматизованої обробки даних та електронної комунікації. Така трансформація безпосередньо пов’язана з необхідністю забезпечення балансу

між публічним інтересом держави у стабільному формуванні доходів бюджету та приватним інтересом платника у передбачуваності оподаткування, правовій визначеності, мінімізації адміністративних витрат і належному захисті своїх прав [21; 24]. Саме тому цифрову платформу доцільно розглядати не лише як технічний інструмент податкового адміністрування, а як нове інституційне середовище реалізації та узгодження законних інтересів суб'єктів податкових правовідносин.

Теоретичним підґрунтям такого підходу є розуміння податкової системи як складного правового та економічного механізму, у межах якого фіскальні інтереси держави повинні реалізовуватися з урахуванням прав та законних інтересів платників. У цьому контексті особливого значення набувають дослідження С. С. Пироги та І. С. Пироги, присвячені ефективності податкового контролю, автоматизації адміністрування податку на додану вартість, а також загальним проблемам правового регулювання податкової системи [21–23; 27; 29]. У цих працях простежується підхід, відповідно до якого удосконалення податкового адміністрування повинно поєднувати підвищення результативності державного контролю зі створенням належних правових умов для реалізації інтересів платника. У сучасних умовах зазначений підхід набуває нового змісту через поширення цифрових платформ, автоматизованих систем та електронної взаємодії.

У цьому аспекті цифрова платформа дозволяє подолати одну з традиційних проблем податкового адміністрування – інформаційну асиметрію між державою та платником. Контролюючий орган у сучасній цифровій державі має можливість отримувати та аналізувати інформацію з великої кількості законних джерел, тоді як платник за традиційної моделі взаємодії часто був змушений самостійно формувати значний обсяг документів і неодноразово подавати державі відомості, якими вона вже володіла. Цифрова інтеграція державних інформаційних ресурсів створює передумови для зміни цієї моделі: інформація

може передаватися між інформаційними системами без безпосереднього залучення платника, якщо така передача має законну підставу [6; 14; 17]. Відповідно, цифровізація здатна одночасно підвищувати ефективність податкового контролю та зменшувати адміністративне навантаження на суб'єкта господарювання.

Важливим кроком у цьому напрямі є реалізація Національної стратегії доходів до 2030 року, яка передбачає комплексну модернізацію податкового адміністрування, підвищення його ефективності та прозорості, а також наближення відповідних процедур до європейських стандартів [2]. При цьому цифровізація розглядається не ізольовано, а як складова ширшої трансформації податкової адміністрації, яка охоплює управління ризиками, аудит, адміністрування податкового боргу, обслуговування платників та організацію внутрішніх процесів [17–19].

Сучасний розвиток податкового адміністрування на міжнародному рівні також демонструє поступовий перехід від окремих електронних сервісів до системної цифрової архітектури. OECD пов'язує цифрову трансформацію податкових адміністрацій із розвитком цифрової ідентифікації, електронних рахунків, інтеграції даних, автоматизованого обміну інформацією, аналітики та штучного інтелекту [14–18]. Для України це означає необхідність формування такого цифрового середовища, у якому технологічні рішення не існують відокремлено, а функціонують як взаємопов'язані елементи єдиного механізму податкового адміністрування.

Отже, цифрова платформа поступово набуває ознак своєрідного *правового інтерфейсу* між платником та державою. Через неї особа не тільки передає інформацію контролюючому органу, а й реалізує суб'єктивні права, отримує адміністративні послуги, ознайомлюється зі станом своїх розрахунків, отримує документи та повідомлення, подає пояснення й запити, а в передбачених законом випадках – реалізує право на адміністративне оскарження. Відповідно,

функціональна спроможність цифрової платформи безпосередньо впливає на можливість реалізації податкових прав. Саме тому надійність, безперервність та юридична визначеність роботи цифрових систем повинні розглядатися як складові належного адміністрування.

В українській науковій літературі ідеї автоматизації податкового адміністрування не є принципово новими. У праці С. С. Пироги та І. С. Пироги «Автоматизована система нарахування, сплати і відшкодування ПДВ» обґрунтовувалася необхідність переходу до автоматизованої моделі адміністрування податку на додану вартість, яка мала б мінімізувати можливості зловживань та підвищити ефективність його справляння [22]. Сьогодні ця наукова позиція набуває нового змісту, оскільки сучасні технологічні можливості дозволяють перейти від автоматизації окремої процедури ПДВ до комплексної цифрової взаємодії платника з податковою адміністрацією, що охоплює реєстрацію, звітність, контроль, обмін інформацією та оскарження.

Саме тому ранні наукові напрацювання щодо автоматизації податкового адміністрування доцільно розглядати не як застарілу технологічну модель, а як один із етапів формування сучасної концепції цифрового податкового права. Суттєва відмінність полягає у масштабі технологічних можливостей. Якщо попередні моделі передбачали автоматизацію окремої податкової процедури, то сучасна цифрова платформа може поєднувати реєстраційні, облікові, контрольні, аналітичні та сервісні функції в межах єдиного інформаційного середовища [13–18; 22].

Особливо важливого значення набуває електронний аудит. Використання стандартизованих електронних даних бухгалтерського та податкового обліку дозволяє податковій адміністрації аналізувати значні масиви інформації, здійснювати їх автоматизоване зіставлення та концентрувати контрольні ресурси на операціях із підвищеним рівнем ризику [16–18]. Така технологія змінює саму природу податкового контролю. Контролюючий орган отримує можливість

здійснювати значно глибший аналіз господарської діяльності, водночас у добросовісного платника зменшується потреба у проходженні численних документальних процедур, якщо відповідна інформація вже доступна державі в електронній формі.

Проте підвищення ефективності контролю не повинно означати автоматичного посилення адміністративного тиску. У правовій державі цифрові технології мають використовуватися передусім для підвищення обґрунтованості рішень контролюючих органів. Якщо алгоритмічна система виявляє певну невідповідність або аномалію, це повинно створювати підставу для додаткового аналізу, але не автоматично встановлювати факт правопорушення. Остаточний юридичний висновок має ґрунтуватися на доказах і прийматися уповноваженим суб'єктом у межах передбаченої законом процедури [1; 5; 39; 40].

Це особливо важливо у зв'язку з розвитком ризикоорієнтованого підходу. Автоматизовані системи можуть аналізувати значні масиви інформації та визначати операції, які статистично відрізняються від звичайної поведінки відповідного сегмента платників. Така аналітика здатна суттєво скоротити кількість безрезультатних перевірок та спрямувати ресурси держави на найбільш ризикові сфери [17; 18; 21]. Водночас ризик не може ототожнюватися з порушенням. Між ними існує принципова юридична відмінність: ризик є прогнозною характеристикою, тоді як правопорушення повинно бути доведене у встановленому законом порядку.

Відповідно, однією з основних гарантій цифрового податкового адміністрування має стати *право платника знати юридично значущі підстави негативного для нього рішення.* Якщо цифрова система визначила його операцію ризиковою, платник повинен мати можливість зрозуміти, які саме обставини стали підставою для такого висновку, надати пояснення та документи і, за необхідності, оскаржити відповідне рішення [5; 11; 39; 40]. Такий підхід

відповідає не тільки загальним принципам адміністративного права, а й вимогам правової визначеності та ефективного захисту прав.

У цьому контексті особливої уваги потребує співвідношення автоматизації та дискреції податкового органу. Цифрова система повинна обмежувати необґрунтовану суб'єктивність посадової особи, але не може перетворитися на неконтрольований механізм автоматичного прийняття владних рішень. Найбільш обґрунтованою видається модель, за якої цифровий алгоритм забезпечує збір, систематизацію та аналітичну обробку інформації, а посадова особа несе юридичну відповідальність за кінцеве рішення [17; 39]. Такий підхід дозволяє поєднати технологічну ефективність із принципом персональної відповідальності суб'єкта владних повноважень.

Іншим важливим аспектом є забезпечення принципу **«одноразового подання інформації»**. Якщо держава вже отримала законним шляхом інформацію про особу або господарську операцію, вимога повторно подавати ті самі дані до іншого органу суперечить самій логіці цифрової трансформації. Інтеграція інформаційних систем повинна поступово зменшувати кількість документів, які платник подає державі, та переносити відповідний обов'язок на державні органи в частині обміну даними між ними [6; 14; 17].

Разом із тим інтеграція інформаційних систем не може бути безмежною. Податкова адміністрація володіє значними масивами персональної та фінансової інформації, а тому її обробка повинна здійснюватися виключно на визначених законом підставах і відповідно до конкретної легітимної мети [5; 11]. Технологічна можливість отримати певні дані сама по собі не створює права на їх необмежене використання. Цифрова трансформація повинна супроводжуватися посиленням гарантій захисту персональних даних, інформаційної безпеки та контролю за доступом до інформаційних ресурсів [5; 7].

Особливе значення в умовах України має кібербезпека податкової інформаційної інфраструктури. Повномасштабна війна створила додаткові загрози для безперервності функціонування державних цифрових систем. Пошкодження критичної інфраструктури, кібератаки та інші загрози можуть безпосередньо впливати на можливість платника виконати податковий обов'язок або реалізувати процесуальне право. Тому стійкість цифрової податкової системи повинна розглядатися як елемент не тільки адміністративної, а й фінансової та національної безпеки [7; 19].

Водночас інтерес держави до отримання інформації не може бути необмеженим. Принцип пропорційності передбачає, що обсяг інформації, яка збирається та обробляється, повинен відповідати легітимній меті податкового контролю. Надмірне накопичення даних створює ризик перетворення цифрової податкової системи на інструмент загального фінансового спостереження. Тому одним із напрямів удосконалення законодавства має стати чітке визначення цілей обробки інформації та механізмів контролю за її використанням [5; 11].

Позитивним напрямом розвитку цифрових платформ є розширення сервісних функцій. Платник повинен отримувати не тільки можливість виконати обов'язок, а й інформацію, яка допомагає виконати його правильно. Автоматичні нагадування про строки подання звітності, попередження про можливі технічні помилки, доступ до персоналізованої інформації, електронне листування з контролюючим органом, отримання індивідуалізованих повідомлень та інші сервіси здатні істотно підвищити рівень добровільного виконання податкових обов'язків [13–18].

Такий сервісний підхід відповідає сучасному розумінню *taxpayer compliance*, за якого поведінка платника розглядається не лише крізь призму контролю і санкцій, а й через створення умов для добровільного виконання законодавства. Чим зрозумілішими є правила та простішим є їх виконання, тим

менше стимулів для помилок та ухилення. У цьому сенсі цифрова платформа може виступати інструментом превентивного податкового регулювання [17–19].

Показовим є досвід держав, які активно розвивають цифрові податкові сервіси. Електронне подання звітності, попереднє заповнення податкових декларацій, електронне виставлення рахунків, цифрова ідентифікація та автоматизований обмін даними поступово стають стандартними елементами діяльності сучасних податкових адміністрацій [14–18]. Сукупність цих практик демонструє загальну тенденцію: цифрова податкова адміністрація поступово переходить від моделі «податкова служба як контролер» до моделі «податкова служба як цифровий адміністратор і сервісний партнер», хоча контрольна функція при цьому зберігається.

Український досвід має власну специфіку. Цифрові державні сервіси розвивалися швидкими темпами ще до повномасштабної війни, а після її початку цифрова інфраструктура стала одним із механізмів забезпечення безперервності державного управління. Важливо, щоб цей позитивний досвід поширювався і на податкову сферу. Податкові сервіси повинні бути максимально інтегрованими, зрозумілими та орієнтованими на життєві ситуації платника [2; 17–19].

У цьому контексті перспективним є розвиток концепції **«податкової події»** як основи цифрової взаємодії. Замість того щоб платник самостійно визначав усі юридичні наслідки господарської операції, цифрова система може автоматично ідентифікувати юридично значущу податкову подію та повідомляти особу про відповідні права й обов’язки. Наприклад, набуття певного статусу, здійснення транскордонної операції, придбання майна або початок господарської діяльності можуть автоматично генерувати інформаційне повідомлення про необхідні податкові дії. Такий підхід зменшує ризик ненавмисного порушення законодавства [13; 17].

Однак автоматизація не повинна означати автоматичне покладення нового податкового обов’язку без чіткої законодавчої підстави. Цифрова платформа не

може створювати податкові зобов'язання, яких не передбачає закон. Технологія повинна реалізовувати закон, а не замінювати його. Це є прямим наслідком принципу законності оподаткування [1; 3; 4].

Важливою складовою узгодження інтересів є також прозорість зміни цифрових правил. Оновлення програмного забезпечення, алгоритмів або критеріїв ризику може істотно впливати на поведінку платника. Тому зміна технологічної логіки платформи, якщо вона має юридично значущі наслідки, повинна бути передбачуваною. Платник не може опинятися у ситуації, коли його операція вчора відповідала встановленим правилам, а сьогодні автоматично визнається ризиковою через зміну алгоритму, про яку він не мав можливості дізнатися [1; 5; 39].

У цьому аспекті цифрове податкове адміністрування повинно базуватися на принципі *технологічної передбачуваності.* Його можна розглядати як сучасне продовження загального принципу правової визначеності. Особа повинна мати можливість передбачити не лише норму закону, а й основні юридично значущі наслідки застосування цифрової системи до її поведінки [1; 39; 40].

Цифрові платформи також можуть створювати нові механізми досудового врегулювання податкових спорів. Електронна комунікація, автоматизоване подання пояснень, електронний обмін доказами та відстеження процесу розгляду скарги здатні скоротити строки та адміністративні витрати. У перспективі можливо використовувати технології аналітичної підтримки для попереднього визначення предмета спору та виявлення очевидних помилок у позиціях сторін. Проте остаточне рішення у спорі має залишатися результатом юридичної процедури, а не автоматичного алгоритмічного визначення [1; 5; 39; 40].

Важливим є також забезпечення реальної рівності сторін. Цифрова держава володіє значно більшими інформаційними ресурсами, ніж окремий платник. Податкова адміністрація може отримувати дані з багатьох джерел та здійснювати їх автоматизований аналіз, тоді як платник часто бачить лише

кінцевий результат. Така інформаційна асиметрія може посилити нерівність сторін. Тому цифрова платформа повинна частково компенсувати її шляхом надання платнику доступу до інформації, яка безпосередньо використовується для прийняття рішення щодо нього, настільки, наскільки це сумісно із законом [5; 11; 40].

Саме тут набуває значення принцип *«рівності цифрової інформації».* Він не означає, що держава повинна розкривати всі свої аналітичні моделі або службову інформацію. Йдеться про те, що платник повинен мати доступ до тієї інформації, яка безпосередньо визначила юридичні наслідки щодо нього, настільки, наскільки це сумісно із законом, захистом третіх осіб та публічним інтересом. Такий підхід здатний істотно підвищити довіру до цифрової податкової системи [5; 11; 40].

Важливою є і проблема цифрової ідентичності. Надійна електронна ідентифікація платника є передумовою юридичної значущості електронних дій. У перспективі розвиток цифрової ідентичності дозволить зменшити кількість документів, які подаються для підтвердження особи або статусу суб'єкта. Водночас така ідентичність повинна бути захищена від незаконного використання, а механізми відновлення доступу мають бути достатньо надійними [4; 12].

Таким чином, цифрова платформа у податковій сфері повинна розглядатися як *правовий інтерфейс взаємодії держави та платника,* а не просто як програмний продукт. Через неї реалізуються права, виконуються обов'язки, передаються юридично значущі документи, приймаються адміністративні рішення та формується інформаційна база контролю. Саме тому вимоги до її функціонування повинні визначатися на рівні права, а не лише технічних регламентів [1; 3–6].

Для України найбільш перспективною видається модель цифрової податкової платформи, яка поєднуватиме сервісний, контрольний,

інформаційний та гарантійний компоненти. Сервісний компонент має спрощувати виконання податкових обов'язків; контрольний – забезпечувати виявлення ризиків; інформаційний – інтегрувати законно отримані дані; гарантійний – забезпечувати права платника, прозорість процедур та можливість оскарження [17–19; 21; 24; 40]. Лише одночасний розвиток усіх складових дозволить уникнути однобічної фіскалізації цифровізації.

Важливим напрямом подальшої трансформації є розвиток цифрового оподаткування доходів, отриманих через платформи. Європейський Союз уже сформував правові механізми автоматичного обміну інформацією про доходи продавців через цифрові платформи в межах DAC7 [8]. Для України імплементація відповідних підходів має особливе значення з огляду на розвиток платформної економіки та необхідність забезпечення рівних умов оподаткування для традиційних і цифрових форм підприємницької діяльності. Водночас передача даних про доходи через цифрові платформи повинна поєднуватися з належними гарантіями захисту персональної інформації [5; 8; 11].

Таким чином, цифрові платформи можуть стати одним із найбільш ефективних інструментів узгодження публічних і приватних інтересів у податковій сфері. Для держави вони забезпечують оперативність отримання інформації, автоматизацію контролю, підвищення ефективності адміністрування та протидію тінізації економіки. Для платника – зменшення адміністративних витрат, доступність податкових послуг, швидкість комунікації, можливість дистанційного виконання обов'язків та реалізації процесуальних прав. Проте досягнення такого балансу можливе лише за умови, що цифровізація буде підпорядкована принципам права, а не замінюватиме їх [1; 5; 17; 21; 24].

Особливої ваги ця теза набуває в умовах війни. Україна одночасно повинна забезпечувати фінансування оборони, соціальних видатків і функціонування держави та створювати умови для збереження й відновлення підприємницької

активності. У такій ситуації цифрове податкове адміністрування здатне зменшити адміністративне навантаження на бізнес, прискорити мобілізацію бюджетних ресурсів та підвищити прозорість їх формування. Тому цифровізація податкової системи в умовах війни повинна розглядатися не як другорядна адміністративна реформа, а як складова економічної стійкості держави [2; 19].

Перспективна модель української цифрової податкової системи має базуватися на поєднанні п'яти взаємопов'язаних засад: законності автоматизованих процедур, інформаційної інтеграції державних систем, сервісної орієнтації податкової адміністрації, ризикоорієнтованого контролю та належного захисту прав платника [1; 5; 6; 17; 21]. Лише за такого поєднання цифрова платформа перестає бути виключно інструментом фіскального контролю і перетворюється на інституційний механізм справедливого та ефективного оподаткування.

Отже, цифровізація податкових правовідносин не повинна оцінюватися лише за кількістю електронних сервісів або ступенем автоматизації окремих процедур. Її справжнім критерієм має бути здатність цифрової системи забезпечити *одночасне підвищення ефективності державного адміністрування та рівня правової захищеності платника.* Саме в цьому полягає її потенціал як механізму узгодження законних інтересів суб'єктів податкових правовідносин і як одного з ключових напрямів модернізації української податкової політики в умовах європейської інтеграції.

### *Висновки до Розділу 4*

Проведене дослідження цифрової модернізації правового регулювання податкової політики України в умовах європейської інтеграції дає підстави стверджувати, що цифровізація податкової сфери перестала бути виключно технологічним напрямом реформування державного управління. Вона поступово перетворюється на комплексний чинник трансформації податкового

права, механізмів адміністрування податків, характеру взаємодії платників із державою та принципів реалізації публічної фінансової політики. У сучасних умовах цифрові технології впливають не тільки на форму виконання податкового обов'язку, а й на способи визначення податкових ризиків, здійснення контролю, отримання інформації, комунікації з платниками та захисту їхніх прав [13–18]. Саме тому цифрову модернізацію доцільно розглядати як один із системоутворюючих напрямів розвитку сучасного податкового права України.

Особливого значення цей процес набуває у зв'язку з європейською інтеграцією України. Наближення національного законодавства до права Європейського Союзу передбачає не лише формальне запозичення окремих нормативних положень, а й поступове впровадження європейських стандартів належного врядування, прозорості, пропорційності, правової визначеності, захисту персональних даних та ефективної адміністративної процедури [8–12]. У податковій сфері це означає необхідність формування такої цифрової моделі, у якій підвищення ефективності фіскального контролю не відбувається за рахунок звуження прав платника. Навпаки, цифровізація повинна створювати умови для одночасного підвищення ефективності держави та рівня правової захищеності суб'єкта оподаткування.

В умовах повномасштабної війни цифрова модернізація набуває додаткового значення. Війна зумовила необхідність забезпечення безперервності функціонування державних інституцій, дистанційного доступу до адміністративних послуг, збереження інформаційних ресурсів та стабільного наповнення державного бюджету. Податкова система в цих умовах виконує не лише традиційну фіскальну функцію, а й функцію забезпечення фінансової стійкості держави. Тому розвиток цифрових податкових сервісів, електронного аудиту, автоматизованого аналізу ризиків та міжвідомчого інформаційного обміну повинен розглядатися як елемент загальної політики економічної та інституційної стійкості України [2; 19].

Водночас цифровізація не може бути самоціллю. Її правова цінність визначається не кількістю запроваджених електронних сервісів, а здатністю забезпечити більш справедливу, прозору, передбачувану та ефективну модель податкового адміністрування. З цієї точки зору особливо важливим є розмежування понять автоматизації та цифрової трансформації. Автоматизація передбачає перенесення окремої процедури у цифрове середовище, тоді як цифрова трансформація передбачає комплексну зміну способу організації відповідних правовідносин. Саме останній підхід відповідає сучасним потребам України та узгоджується із загальною тенденцією цифрового розвитку податкових адміністрацій [13–18].

Одним із ключових результатів дослідження є висновок про необхідність переходу від переважно контрольної до *сервісно-контрольної моделі податкового адміністрування*. У такій моделі держава не відмовляється від контролю, але здійснює його більш адресно, на основі аналізу ризиків та цифрових даних, одночасно створюючи для сумлінного платника максимально прості умови виконання податкового обов'язку. Це дозволяє поєднати публічний інтерес у забезпеченні бюджетних надходжень із приватним інтересом у мінімізації адміністративних витрат та передбачуваності правового регулювання [21; 24].

Важливою передумовою такої моделі є розвиток електронного кабінету та інших цифрових сервісів. Електронна взаємодія повинна поступово охоплювати не тільки подання звітності, а й реєстрацію, отримання інформації, електронне листування, подання пояснень, адміністративне оскарження та інші юридично значущі процедури [3; 4; 14; 17]. При цьому цифровий сервіс повинен бути не просто технічно доступним, а юридично передбачуваним. Особа має розуміти, які юридичні наслідки породжує її електронна дія, які строки застосовуються, яким чином можна виправити помилку та яким способом захистити своє право.

Особливого значення набуває проблема автоматизованого прийняття рішень. Використання алгоритмів у податковому контролі має значний потенціал для зменшення суб'єктивізму, корупційних ризиків та необґрунтованих перевірок. Водночас алгоритм не повинен перетворюватися на автономного суб'єкта владних повноважень. Автоматизований аналіз може визначати ризики, систематизувати інформацію та формувати рекомендації, однак юридично значуще рішення, яке обмежує права особи, повинно залишатися результатом встановленої законом процедури та перебувати під належним людським контролем [5; 11; 39; 40].

Звідси випливає необхідність нормативного закріплення принципів *алгоритмічної прозорості, підзвітності та людського контролю* у податковому адмініструванні. Платник повинен мати можливість отримати достатнє пояснення щодо підстав прийняття рішення, надати власні аргументи та докази і скористатися передбаченими законом способами його оскарження. Такий підхід є необхідною умовою забезпечення правової визначеності в цифровому середовищі [5; 11; 39; 40].

Важливим напрямом модернізації є також розвиток електронного аудиту та ризикоорієнтованого податкового контролю. Використання структурованих електронних даних дозволяє державі здійснювати більш глибокий аналіз господарської діяльності та концентрувати контрольні ресурси на операціях із підвищеним ризиком [16–18]. Проте ризик не може автоматично ототожнюватися з правопорушенням. Саме тому автоматизоване визначення ризиковості повинно мати попереджувальний та аналітичний характер, тоді як встановлення юридичної відповідальності повинно здійснюватися виключно на основі доказів та у встановленому законом порядку [1; 21].

Окремої уваги потребує цифровий моніторинг доходів, пов'язаних із транскордонними операціями, переміщенням капіталу та діяльністю цифрових платформ. Розвиток цифрової економіки створює нові форми отримання доходів,

які можуть залишатися поза межами традиційних механізмів податкового контролю. Тому міжнародний автоматичний обмін податковою інформацією, імплементація відповідних стандартів ОЕСР та ЄС, а також регулювання діяльності цифрових платформ стають необхідними елементами сучасної податкової політики [8; 17–20]. Україна, рухаючись до європейської інтеграції, повинна розвивати не тільки нормативну, а й технологічну спроможність брати участь у такому інформаційному обміні.

Водночас ефективне протистояння виведенню капіталу не може здійснюватися лише через посилення контрольних заходів. Необхідно забезпечити комплексне використання цифрової аналітики, правил трансфертного ціноутворення, контролю за контрольованими іноземними компаніями, механізмів протидії тонкій капіталізації та міжнародних інструментів запобігання розмиванню податкової бази [30–37]. Наукові праці С. С. Пироги у цій сфері мають безпосереднє значення для розвитку української доктрини, оскільки дозволяють пов’язати сучасну цифрову трансформацію податкового адміністрування з проблемами глобалізації, транскордонного руху капіталу, КІК, трансфертного ціноутворення та податкової юрисдикції [27; 30–37].

Дослідження підтверджує також особливе значення цифровізації для реалізації соціальної функції податків. Податкова система повинна забезпечувати не тільки достатній рівень доходів бюджетів, а й справедливий розподіл податкового навантаження, доступність соціально орієнтованих механізмів та рівність платників. Цифрові інструменти здатні підвищувати адресність податкових пільг, виявляти тіньові доходи та зменшувати адміністративні витрати платників. Водночас вони повинні застосовуватися таким чином, щоб не створювати нові форми цифрової дискримінації та не обмежувати можливість реалізації прав осіб, які мають об’єктивні труднощі з користуванням цифровими сервісами [24; 25; 34; 40].

Окремим напрямом модернізації є цифровізація рентних відносин. Ефективність справляння рентних платежів безпосередньо залежить від достовірності інформації про фактичне використання природних ресурсів. Тому інтеграція даних про спеціальні дозволи, геологічну інформацію, фактичні обсяги видобування, реалізацію продукції та податкові зобов'язання може істотно підвищити прозорість ресурсного сектору [1; 6]. В умовах післявоєнного відновлення особливого значення набуває цифровий облік критичної сировини та забезпечення сумісності відповідних інформаційних систем із європейськими підходами [41].

Українська специфіка полягає в тому, що цифровізація природоресурсної сфери повинна здійснюватися одночасно з урахуванням вимог національної безпеки. Публічність інформації про природні ресурси та прозорість видобувного сектору є необхідними умовами належного врядування, однак в умовах війни окремі відомості про стратегічні ресурси та критичну інфраструктуру можуть потребувати спеціального режиму доступу. Саме тому адаптоване застосування міжнародного стандарту EITI для України в умовах війни має важливе значення для поєднання принципів прозорості та безпеки [42].

Дослідження дозволяє також сформулювати висновок про необхідність розвитку *цифрового податкового права як комплексного напряму наукового та нормативного осмислення* наслідків цифрової трансформації оподаткування. Йдеться не про створення окремої галузі права, а про системне дослідження правових особливостей електронного адміністрування, цифрових доказів, алгоритмічних рішень, електронної ідентифікації, міжвідомчого інформаційного обміну, кібербезпеки та захисту прав платника у цифровому середовищі [3–7; 11; 39; 40].

У цьому зв'язку важливо враховувати наукову тяглість відповідних досліджень. Раннє дослідження І. С. Пироги та С. С. Пироги щодо автоматизованої системи нарахування, сплати і відшкодування ПДВ свідчить,

що проблема автоматизації податкового адміністрування була предметом української правової науки ще до сучасного етапу цифрової трансформації [22]. Подальший розвиток цієї проблематики у працях авторів щодо податкового контролю, правового регулювання ПДВ, податкової системи та податкової політики демонструє послідовне формування доктринального підґрунтя для сучасної цифрової моделі адміністрування [21–25; 27; 29].

На цій основі доцільно запропонувати низку напрямів подальшого вдосконалення правового регулювання. Насамперед необхідно забезпечити подальшу інтеграцію податкових інформаційних систем із державними реєстрами за принципом законної та цільової обробки даних; нормативно визначити статус результатів автоматизованого ризик-аналізу та алгоритмічних рішень; закріпити гарантії доступу платника до юридично значущої інформації, використаної щодо нього; забезпечити належний людський контроль у випадках прийняття рішень, що істотно впливають на права особи; удосконалити правове регулювання електронного аудиту, цифрових платформ, міжнародного обміну інформацією та цифрового обліку природних ресурсів [1; 5; 6; 8–10; 17; 39; 40].

Важливим напрямом є також розвиток принципу **«once-only»** у податковій сфері. Держава повинна не вимагати від платника повторного надання вже наявної інформації, а забезпечувати належний міжвідомчий обмін даними. Проте реалізація цього принципу повинна супроводжуватися чітким визначенням правових підстав доступу до інформації, відповідальності розпорядників даних та механізмів виправлення помилкових відомостей [5; 6; 14; 17].

Окремого правового оформлення потребує принцип *технологічної передбачуваності,* відповідно до якого зміни алгоритмів та цифрових процедур, що мають юридично значущі наслідки для платника, повинні бути доступними та передбачуваними. Технологічне оновлення не повинно створювати прихованого механізму зміни фактичних умов оподаткування. Будь-яке істотне

обмеження прав особи має випливати із закону, а не з технічного рішення програмного забезпечення [1; 39; 40].

Не менш важливим є забезпечення кіберстійкості цифрової податкової інфраструктури. У воєнних умовах безперервність функціонування податкових інформаційних систем має безпосереднє значення для фінансової стійкості держави. Тому резервування критичних даних, захищені канали передачі, контроль доступу, відновлення після кібератак та інші заходи безпеки повинні розглядатися як обов'язкові елементи цифрового податкового адміністрування [7; 19].

У кінцевому підсумку цифрова модернізація податкової політики України повинна забезпечувати *баланс між фіскальною спроможністю держави, економічною свободою, соціальною справедливістю та правами платника.* Надмірна фіскалізація цифрових технологій може знизити довіру до держави та збільшити адміністративні витрати, тоді як недостатня цифрова спроможність не дозволить ефективно протидіяти тінізації економіки, незаконному виведенню капіталу та приховуванню доходів. Оптимальною є модель, у якій держава використовує цифрові технології для точнішого, адреснішого та доказовішого адміністрування, а платник отримує більш простий, передбачуваний і доступний спосіб виконання обов'язків та захисту своїх прав [17–21].

Таким чином, цифрова модернізація правового регулювання податкової політики України в умовах європейської інтеграції повинна розглядатися як комплексна трансформація, що охоплює податкове адміністрування, міжнародний обмін інформацією, соціальну функцію оподаткування, контроль за транскордонним рухом капіталу, рентні відносини та цифрові платформи. Її успішність визначатиметься не стільки рівнем технологічної складності, скільки здатністю забезпечити законність, прозорість, справедливість, пропорційність та ефективність податкового регулювання. Для України цей процес має додатковий стратегічний вимір, оскільки відбувається одночасно з повномасштабною

війною, необхідністю збереження фінансової стійкості держави, відновленням економіки та наближенням до правового й цифрового простору Європейського Союзу [2; 8–12; 19].

Відповідно, подальша цифрова модернізація податкової системи має бути спрямована на формування *людиноцентричної, ризикоорієнтованої, інформаційно інтегрованої та правово гарантованої моделі податкового адміністрування.* Така модель повинна поєднувати автоматизацію стандартних процедур із людським контролем юридично значущих рішень, міжнародну податкову прозорість із захистом приватності, фіскальну ефективність із соціальною справедливістю, а цифрову відкритість – із вимогами національної безпеки. Саме ця збалансована конструкція, на нашу думку, може стати одним із ключових напрямів формування сучасної податкової системи України у процесі її європейської інтеграції та повоєнної відбудови.

## Список використаних джерел

1. Податковий кодекс України: Кодекс України; Закон України від 02.12.2010 № 2755-VI. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2755-17

2. Про схвалення Національної стратегії доходів до 2030 року: розпорядження Кабінету Міністрів України від 27.12.2023 № 1218-р. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1218-2023-%D1%80

3. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/851-15

4. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2155-19

5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17

6. Про публічні електронні реєстри: Закон України від 18.11.2021 № 1907-IX. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1907-20

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19

8. Council Directive (EU) 2021/514 of 22 March 2021 amending Directive 2011/16/EU on administrative cooperation in the field of taxation. *Official Journal of the European Union*. 2021. L 104. P. 1–26. URL: https://eur-lex.europa.eu/eli/dir/2021/514/oj

9. Council Directive (EU) 2025/516 of 11 March 2025 amending Directive 2006/112/EC as regards VAT rules for the digital age. *Official Journal of the European Union*. 2025. OJ L, 2025/516. URL: https://eur-lex.europa.eu/eli/dir/2025/516/oj

10. Council Regulation (EU) 2025/517 of 11 March 2025 amending Regulation (EU) No 904/2010 as regards the VAT administrative cooperation arrangements needed for the digital age. *Official Journal of the European Union*. 2025. OJ L, 2025/517. URL: https://eur-lex.europa.eu/eli/reg/2025/517/oj

11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

12. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. *Official Journal of the European Union*. 2024. OJ L, 2024/1183. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj

13. OECD. *Tax Administration 3.0: The Digital Transformation of Tax Administration*. Paris: OECD Publishing, 2020. DOI: https://doi.org/10.1787/ca274cc5-en

14. OECD. *Tax Administration 3.0 and the Digital Identification of Taxpayers: Initial Findings*. Paris: OECD Publishing, 2022. 74 p. DOI: https://doi.org/10.1787/3ab1789a-en

15. OECD. *Tax Administration 3.0 and Electronic Invoicing: Initial Findings*. Paris: OECD Publishing, 2022. 56 p. DOI: https://doi.org/10.1787/2ffc88ed-en

16. OECD. *Inventory of Tax Technology Initiatives*. Paris: OECD, 2024. URL: https://www.oecd.org/en/data/datasets/inventory-of-tax-technology-initiatives.html

17. OECD. *Tax Administration Digitalisation and Digital Transformation Initiatives*. Paris: OECD Publishing, 2025. DOI: https://doi.org/10.1787/c076d776-en

18. OECD. *Tax Administration 2025: Comparative Information on OECD and Other Advanced and Emerging Economies*. Paris: OECD Publishing, 2025. 155 p. DOI: https://doi.org/10.1787/cc015ce8-en

19. OECD. *OECD Economic Surveys: Ukraine 2025*. Paris: OECD Publishing, 2025. DOI: https://doi.org/10.1787/940cee85-en

20. OECD. *The Global Minimum Tax Implementation Toolkit*. Paris: OECD Publishing, 2026. 97 p. DOI: https://doi.org/10.1787/0ee66d84-en

21. Пирога С. С., Пирога І. С. Правові засоби забезпечення ефективності податкового контролю. *Науковий вісник Ужгородського національного*

*університету. Серія: Право*. 2022. Вип. 69. С. 311–316. DOI: https://doi.org/10.24144/2307-3322.2021.69.52

22. Пирога С. С., Пирога І. С. Автоматизована система нарахування, сплати і відшкодування ПДВ. *Науковий вісник Ужгородського університету. Серія: Право*. 2011. Вип. 17. С. 154–157. URL: https://dspace.uzhnu.edu.ua/items/13fb6303-7898-4717-8482-367a56205943

23. Pyroha S. S., Pyroha I. S. Legal insignificance of VAT legal regulation in Ukraine. *Law Review of Kyiv University of Law*. 2021. № 4. P. 67–72. DOI: https://doi.org/10.36695/2219-5521.4.2021.12

24. Пирога С. С., Пирога І. С. Юридичні інструменти забезпечення економічних і соціальних прав в Україні. *Український часопис конституційного права*. 2022. № 1. С. 35–45. DOI: https://doi.org/10.30970/jcl.1.2022.3

25. Пирога І. С. Механізм податкового стимулювання соціально-економічного розвитку України: монографія. Ужгород: ДВНЗ «Ужгородський національний університет» ; Херсон: Гельветика, 2019. 279 с. ISBN 978-966-916-936-5.

26. Пирога С. С. Особливості визначення об’єктів оподаткування. *Правничий часопис Донецького національного університету імені Василя Стуса*. 2023. № 2. С. 142–150. DOI: https://doi.org/10.31558/2786-5835.2023.2.16

27. Пирога С. С. Податкова система заснована на принципі джерела. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Т. 1, № 80. С. 530–536. DOI: https://doi.org/10.24144/2307-3322.2023.80.1.81

28. Pyroha S. S. Effective means of legal regulation of foreign trade. *ScienceRise: Juridical Science*. 2023. № 3 (25). P. 64–71. DOI: https://doi.org/10.15587/2523-4153.2023.286749

29. Пирога С. С. Правові проблеми, спричинені недоліками податкового законодавства України. *Вісник Національної академії правових наук України*.

2023. Т. 30, № 4. С. 228–240. DOI: https://doi.org/10.31359/1993-0909-2023-30-4-228

30. Пирога С. С. Вплив глобалізації на податкову систему країн. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 2, № 81. С. 196–202. DOI: https://doi.org/10.24144/2307-3322.2024.81.2.30

31. Пирога С. С. Проблеми правової регламентації тонкої капіталізації в Україні. *Проблеми законності*. 2024. № 164. С. 120–134. DOI: https://doi.org/10.21564/2414-990X.164.296330

32. Пирога С. С. Правова оцінка чинних угод про уникнення подвійного оподаткування. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 2, № 82. С. 238–244. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.38

33. Пирога С. С. Особливості правового регулювання контрольованих іноземних компаній в Україні. *Європейські перспективи*. 2024. № 1. С. 150–157. DOI: https://doi.org/10.32782/ep.2024.1.21

34. Пирога С. С. Правові заходи забезпечення справедливого розподілу доходів для гарантування сталого розвитку України. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 1 (104), ч. 1. С. 124–135. DOI: https://doi.org/10.32631/v.2024.1.11

35. Пирога С. С. Реформи трансфертного ціноутворення в контексті BEPS: проблеми залишаються. *Право і безпека*. 2024. № 1 (92). С. 163–172. DOI: https://doi.org/10.32631/pb.2024.1.15

36. Пирога С. С. Трансфертне ціноутворення нематеріальних активів: проблеми правозастосування. *ScienceRise: Juridical Science*. 2024. № 1 (27). С. 30–35. DOI: https://doi.org/10.15587/2523-4153.2024.301253

37. Пирога С. С., Пирога І. С. Податок на виведений капітал чи амністія тіньових доходів. *Вісник Національної академії правових наук України*. 2024. Т. 31, № 3. С. 85–102. DOI: https://doi.org/10.31359/1993-0909-2024-31-3-85

38. Пирога С. С. *Правове регулювання системи оподаткування України: проблеми теорії і практики:* дис. ... д-ра юрид. наук: 12.00.07. Ужгород, 2025. Державний вищий навчальний заклад «Ужгородський національний університет». URL: https://www.uacademic.info/ua/document/0525U000001

39. Волкова Ю. Ф., Пирога І. С. Право на використання технологій штучного інтелекту: нові виклики та загрози для людини. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 1, № 84. С. 138–143. DOI: https://doi.org/10.24144/2307-3322.2024.84.1.20

40. Колб С. О., Пирога І. С. Інформаційні права людини в цифровому просторі. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 1, № 89. С. 216–221. DOI: https://doi.org/10.24144/2307-3322.2025.89.1.29

41. Vyzhva S., Biliavska O., Babchuk D., Babchuk Y. Critical raw materials in the context of the Ukraine Facility program and European integration. *Visnyk of Taras Shevchenko National University of Kyiv. Geology*. 2025. Vol. 4, No. 111. P. 131–136. DOI: https://doi.org/10.17721/1728-2713.111.15

42. Extractive Industries Transparency Initiative. *The Board approved Ukraine's request for adapted implementation*. 2025. URL: https://eiti.org/board-decision/2025-35

# РОЗДІЛ 5
# ЦИФРОВА ТРАНСФОРМАЦІЯ ОБЛІКОВО-АНАЛІТИЧНОЇ СИСТЕМИ ПІДПРИЄМСТВА: КОНЦЕПЦІЯ, ІНСТРУМЕНТИ, ОЦІНКА ЕФЕКТИВНОСТІ

Автор: **Лисенко Алла Миколаївна,** *кандидат економічних наук, доцент, доцент кафедри аудиту, обліку та оподаткування Центральноукраїнський національний технічний університет*

## 5.1. Теоретичні засади формування обліково-аналітичної системи підприємства

Сучасна обліково-аналітична система підприємства базується на даних бухгалтерського обліку, органічно поєднуючи підсистеми обліку, контролю та економічного аналізу. При цьому функція контролю частково реалізується у процесі ведення обліку, а також на різних етапах проведення аналізу управлінських завдань. В узагальненому форматі обліково-аналітична система являє собою комплексний механізм збору, економіко-аналітичної оцінки, обробки, трансформації різних видів інформації, необхідної для розробки й ухвалення управлінських рішень.

У працях науковців складові обліково-аналітичної системи та їх функціональне призначення різними авторами трактуються з деякими термінологічно-концептуальними відмінностями. Так, на думку Кудренко Н. В. обліково-аналітична система є інтегрованим комплексом відповідних процедур, методів, технологій, спрямованих на збір і обробку, оцінювання й подання інформації для прийняття управлінських рішень, у якому дані бухгалтерського обліку поєднуються з аналітичними модулями, механізмами контролю, планування та прогнозування [3, с. 129-130].

Лень В. С. виокремлює поняття «обліково-аналітична система» та «система обліково-аналітичного забезпечення», зазначаючи, що обліково-аналітична система «… характеризує систему, яка виробляє інформацію для зовнішніх та

внутрішніх користувачів» [5, с. 284], а система обліково-аналітичного забезпечення «… характеризує її підсистему, яка виробляє інформацію (кінцевий продукт) для прийняття управлінських рішень внутрішніми користувачами» [5, с. 284]. На думку науковця, «обліково-аналітична система - це впорядкована внутрішня структура організації, яка накопичує дані господарського обліку та зовнішню позаоблікову інформацію для аналізу та формування звітності для внутрішніх і зовнішніх користувачів у необхідному для них розрізі» [5, с. 286]. Проаналізувавши взаємозв'язок понять «обліково-аналітична система» та «система обліково-аналітичного забезпечення», Лень В. С. стверджує, що на основі використання відповідних методик обліку, аналізу, контролю, планування обліково-аналітична система організації дає можливість сформувати обліково-аналітичне забезпечення в управлінні бізнес-процесами [5, с. 286].

Сьомочкіна Т. І. та Грищук Г. В. досліджують обліково-аналітичне забезпечення як складову інформаційного забезпечення підприємства, як впорядковану систему формування, обробки й подання внутрішнім і зовнішнім користувачам обліково-аналітичної інформації, необхідної для прийняття управлінських рішень. Науковці стверджують, що обліково-аналітичне забезпечення є інформаційною системою другого рівня, а результат функціонування такої системи відповідає характеристикам інформаційного продукту для потреб внутрішніх користувачів та залежить від попиту на конкретну обліково-аналітичну інформацію [8].

Яловега Л. В., Лега О. В., Прийдак Т. Б. зазначили, що обліково-аналітична система - це «система, що формується у результаті збору інформації, джерелами якої є облікові та звітні дані бухгалтерського та інших видів обліку (оперативного й статистичного)» [10, с. 131].

Серед підсистем обліково-аналітичної системи Яловега Л. В., Лега О. В., Прийдак Т. Б. виокремлюють: облікову (управлінський, фінансовий та податковий облік); аналітичну (фінансовий, економічний, стратегічний аналіз); контрольну (внутрішній та зовнішній контроль) [10, с. 134].

На думку Василішина С. І., включення підсистеми аудиту (контролю) до обліково-аналітичного забезпечення залишається досить спірним моментом, однак головним аргументом на його користь є нерозривність функціонування ланцюга «облік-аналіз-контроль» при організації ведення обліку та роботи економічної служби підприємства. Функцію контролю науковець розглядає як окрему функцію в системі менеджменту та як специфічну функцію підсистем обліку та аналізу [1, с. 101].

Яремко І. Й. виокремлює практичний та теоретичний підходи у дослідженні обліково-аналітичного забезпечення. Дослідник стверджує, що система обліково-аналітичного забезпечення з практичної точки зору поєднує процеси формування масиву інформації в різних підсистемах обліку та її подальше опрацювання методами економічного аналізу, відповідними для конкретних цілей управління. З теоретичної ж точки зору вивчаються різні аргументи щодо формування раціональної моделі комплексної консолідованої інформації, необхідної для підсистеми управління різними видами діяльності підприємства [12].

На думку Яремка І. Й., складовими обліково-аналітичної системи є: облікове поле, у рамках якого формується базова інформація бухгалтерських систем (здійснюється ідентифікація, вимірювання і систематизація інформації); звітність як результатна облікова інформація (узагальнена інформація); економічний аналіз, при проведенні якого формується результатна аналітична інформація на основі обробки облікової інформації [12].

При формуванні підприємством обліково-аналітичної системи Кононенко Л. В. та Ніколаєва С. П. рекомендують максимально враховувати єдність підприємства із зовнішнім середовищем, оскільки зовнішнє середовище здійснює значний вплив на результати господарювання, якість ухвалених управлінських рішень та забезпечення стабільності розвитку підприємства [2, с. 72].

Для забезпечення бізнесу надійною базою даних, в обліково-аналітичній системі виконується сукупність послідовних дій:

– здійснюється безперервний збір даних з фіксацією господарських операцій в системі обліку та звітності (виконується облікова функція);

– перевіряється повнота та правильність відображення даних в обліку та звітності, дотримання фінансової дисципліни, здійснюється виявлення ризиків, запобігання втратам (реалізується функція контролю);

– облікова інформація, перевірена на предмет повноти та достовірності, інтерпретується у процесі дослідження факторних впливів, прогнозування розвитку, для оцінки динаміки змін показників, фінансового стану підприємства, виявлення резервів (реалізується аналітична функція).

В цифрову епоху обліково-аналітична система підприємства зазнала суттєвих трансформаційних змін. Відбувся перехід від «паперового» формату до впровадження інтегрованих інформаційних технологій, застосування яких забезпечує автоматизацію збору даних, здійснення контролю та аналізу, прийняття рішень.

З використанням сучасних автоматизованих систем формуються облікові документи. Для здійснення контролю та аналізу даних з використанням спеціалізованого програмного забезпечення формуються звіти в режимі реального часу. Використовуючи аналітичні дані, керівник ухвалює рішення щодо оптимізації витрат, масштабування бізнесу тощо. Отже, сучасні інформаційно-комунікаційні технології дають можливість перетворювати масиви облікових даних на структуровані інсайти для бізнесу.

Водночас, при упровадженні цифровізації виникає ряд викликів, основними серед яких є:

– суттєве зростання обсягу інформації, у т.ч. даних, що надходять у режимі реального часу;

– проблеми з актуальністю інформації, повнотою та зрозумілістю даних, що ускладнює процес аналітики та ухвалення рішень;

– складність поєднання даних з різних інформаційних джерел; обмежений доступ до певної інформації та її швидке «старіння»;

– зростання потреби у використанні відповідних інструментів та спеціальних знаннях [6, с. 294-295].

Враховуючи актуальність використання цифрових інструментів у різних сферах ведення бізнесу, науковці вивчають особливості їх впровадження та вплив на функціонування обліково-аналітичної системи підприємства. Зокрема, проблематику трансформації обліку та інструментів контролю в умовах цифровізації, обґрунтування ролі кіберзахисту в облікових процесах дослідили Лега О. В., Канцедал Н. А., Прийдак Т. Б. [4]. Взаємопов'язані групи цифрових інструментів в обліку та сфері аудиту, які забезпечують можливість здійснення глибинної обробки даних, моделювання розвитку подій та прийняття обґрунтованих рішень виокремила Скрипник С. В. [7]. Вплив на організацію облікових процесів ERP-рішень, технологій AI, хмарних платформ та машинного навчання вивчала Янковська К. [11].

Незважаючи на значну кількість досліджень у сфері цифровізації окремих аспектів бухгалтерського обліку, внутрішнього контролю, економічного аналізу переважна більшість науковців досліджує особливості упровадження окремих технологій (AI, ERP, Blockchain, Big Data тощо). Натомість цілісна концепція цифрової трансформації обліково-аналітичної системи підприємства, яка б інтегрувала бухгалтерський облік, внутрішній контроль та аудит, податкове планування та прогнозування, підтримку управлінських рішень у рамках єдиного цифрового середовища на даний час перебуває на стадії свого формування.

Недостатньо розробленою науковцями є й методологія оцінювання ефективності цифрової трансформації обліково-аналітичної системи підприємства з урахуванням формування індикаторів цифрової зрілості, впливу на якість прийняття рішень та забезпечення економічного ефекту для підприємства. Не досліджені належним чином і комплексні моделі цифрової обліково-аналітичної системи, які б враховували інтеграцію виробничих і

технологічних аспектів при впровадженні цифровізації, недостатньо вивчені науковцями й особливості інтеграції сучасних цифрових технологій у єдину обліково-аналітичну платформу.

### 5.2. Цифрові технології та інструменти функціонування сучасної обліково-аналітичної системи

Пропонуємо розглядати цифрову обліково-аналітичну систему підприємства як інтегроване утворення, до складу якого входить п’ять компонентів (рис. 1).

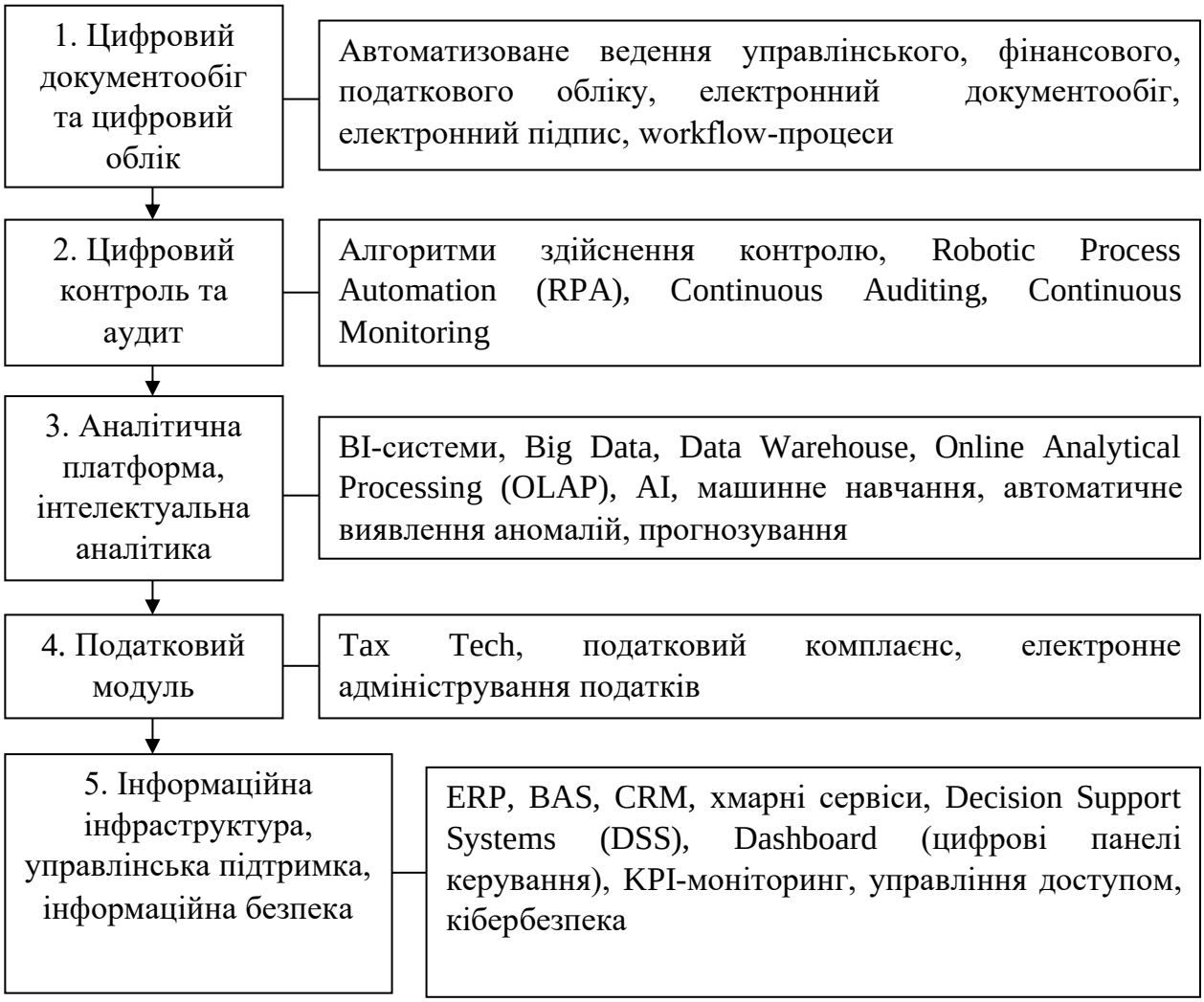



Рис. 1. Основні компоненти цифрової обліково-аналітичної системи підприємства

*Джерело: сформовано автором на підставі [1; 3; 5; 10]*

Таким чином, сучасна цифрова обліково-аналітична система підприємства не обмежується бухгалтерським обліком, контролем та аналізом, інтегруючи паралельно функції прогнозування та підтримки управлінських рішень.

Серед основних цифрових технологій, які забезпечують функціонування сучасних обліково-аналітичних систем, можна виокремити наступні:

1. ERP-системи (Enterprise Resource Planning). Це програмне забезпечення, яке дає можливість комплексно управляти бізнес-процесами підприємства, об'єднуючи кадри, логістику, виробництво та продаж продукції, фінанси у єдину інформаційну базу, забезпечуючи злагоджену роботу структурних підрозділів у режимі реального часу та усуваючи можливість дублювання інформації. У рамках ERP-системи поєднується сукупність модулів, кожен з яких, працюючи з єдиним джерелом даних, відповідає за певний напрям ведення бізнесу:

– бухгалтерія та фінанси (облік витрат, доходів, фінансових результатів, формування звітності);

– логістика, управління складським господарством (контроль залишків запасів, оптимізація ланцюгів постачання);

– HR та зарплата (облік та дослідження руху персоналу, нарахування заробітної плати);

– виробництво (управління ресурсами, планування випуску та контроль якості продукції);

– CRM (Customer Relationship Management) та продажі (взаємодія з клієнтами, управління ціноутворенням та замовленнями).

Підприємства можуть обирати між локальними ERP-системами, які встановлюються на власних серверах, або ж хмарними, представленими у вигляді рішень для різних масштабів ведення бізнесу. Впровадження ERP-систем забезпечує прозорість, оскільки менеджери у єдиному інтерфейсі бачать об'єктивний стан справ на підприємстві, що знижує імовірності допущення помилок та впливу «людського фактора», забезпечує економію часу за рахунок

автоматизації рутинних завдань, пришвидшення процесу ухвалення рішень на основі використання єдиної інформаційної бази та можливості швидкого аналізу даних;

2. Хмарні технології (Cloud Computing). Вони являють собою модель віддаленого доступу до програмного забезпечення, обчислювальних ресурсів та сховищ даних через Інтернет. При цьому користувачі не придбавають фізичні сервери, а орендують у провайдерів IT-потужності та сплачують виключно за фактично використаний об'єм таких потужностей. Основними типами хмарних послуг є IaaS (інфраструктура як послуга), PaaS (платформа як послуга) та SaaS (програмне забезпечення як послуга).

Хмарні технології мають ряд особливостей та переваг, а саме:

– гнучкість, масштабованість, мобільність (їх потужності можна змінювати з урахуванням поточних потреб бізнесу, а доступ до баз даних, файлів, додатків забезпечується через Інтернет з будь-якої точки світу та будь-якого пристрою);

– відсутність потреби в інвестиціях для закупівлі спеціального обладнання та будівництва власних дата-центрів;

3. Big Data (великі дані) – масиви інформації, обсяги яких та швидкість обробки суттєво перевищують можливості традиційних баз даних. Їх використовують з метою прийняття більш обґрунтованих рішень в бізнесі, для виявлення трендів (закономірностей).

Концепція формування Big Data базується на урахуванні наступних ознак:

– volume (обсяг) – фізичний обсяг даних у тера-, пета- та екзабайтах;

– velocity (швидкість) – швидке надходження інформації для її обробки в режимі реального часу;

– variety (розмаїття) – спроможність поєднувати різні типи даних.

Використовуючи Big Data можна перетворити початкову інформацію на конкурентну перевагу, персоналізуючи пропозиції у сфері маркетингу та ритейлу, оцінюючи вибір оптимальної локації бізнесу на основі оцінки потоку

клієнтів, стрімко виявляючи шахрайські схеми у сфері банкінгу. З цією метою в системі Big Data застосовують спеціальні технології, зокрема, розподілені обчислення (спеціальні програми, які роблять можливим виокремлення дрібних частин завдання та їх одночасну обробку на різних серверах), Data Lakes (сховища для зберігання оригінального формату необробленого масиву даних), машинне навчання (алгоритми AI, які здійснюють пошук прихованих взаємозвязків у масивах даних);

4. Business Intelligence (BI) – поєднання інструментів, технологій та методів збору, обробки, аналізу даних. Платформи Power BI, Tableau і т.п. дають можливість отримати на основі використання сирих даних інтерактивні візуалізації (дашборди, звіти) для обгрунтування рішень в управлінні бізнесом. З використанням BI-платформ існує можливість збору даних на основі підкючення до різних джерел їх отримання (ERP-систем, бази Excel, CRM, SQL-бази, хмарних сховищ), їх візуалізації шляхом створення діаграм, графіків, інтерактивних панелей для подальшого відслідковування KPI, проведення аналізу в режимі реального часу.

Слід зазначити, що ключові BI-платформи мають деякі відмінності. Так, Microsoft Power BI є глибоко інтегрованою з екосистемою Microsoft, володіє значними можливостями щодо моделювання даних, здійснення складних обчислень на основі використання мови виразів DAX. В свою чергу, платформа Tableau має інтуїтивний інтерфейс та надає широкий вибір використання різних вбудованих інструментів для створення інтерактивних візуалізацій, не потребуючи наявності у користувача глибоких технічних знань;

5. Artificial Intelligence (AI) – здатність комп’ютерних систем виконувати такі завдання, які потребують використання людського інтелекту (міркування, навчання, розпізнавання мови, прийняття рішень). AI (ChatGPT, Siri, Google Assistant) орієнтований на значні обсяги даних та функціонує завдяки таким технологіям, як машинне навчання (алгоритми, завдяки яким комп’ютери

навчаються на основі даних) та нейронні мережі (системи, які у масивах інформації виявляють складні зв'язки та створюються за принципом дії людського мозку);

6. Machine Learning (ML) є складовою AI, яка замість виконання жорстких інструкцій вивчає алгоритми, спроможні виявляти закономірності, навчатися на даних, ухвалювати рішення без програмування дій. Системи ML на основі отриманого досвіду з часом покращують свою точність. При цьому алгоритм самостійно аналізує дані та розробляє математичну модель для прогнозування або класифікації раніше невідомих даних. Основними типами машинного навчання є навчання з учителем (Supervised Learning), без учителя (Unsupervised Learning), з підкріпленням (Reinforcement Learning);

7. Robotic Process Automation (RPA) є технологією автоматизації бізнес-процесів, основаною на використанні ботів (віртуальних роботів), які взаємодіють з інтерфейсами різних програм, виконуючи механічні повторювані завдання з метою імітації дій людини. Використання RPA дає можливість перекласти рутинні завдання на ПЗ для того, щоб працівники мали змогу зосередитися на важливіших завданнях, зменшити кількість помилок (адже боти виконують поставлені завдання, мінімізуючи вплив людського фактору, за заданим алгоритмом дій), швидко працювати, не потребуючи істотних змін в IT-системах;

8. Blockchain – розподілена цифрова база даних, у рамках якої інформація зберігається у форматі ланцюжка блоків, кожен з яких містить дані про криптографічний підпис та транзакції, що робить систему захищеною від підробок «заднім числом», прозорою та децентралізованою. Дану технологію покладено в основу відстеження ланцюжків постачання товарів, захисту прав інтелектуальної власності, проведення децентралізованих платежів, формування криптовалют тощо;

9. Internet of Things (IoT) – концепція, що поєднує у єдину мережу ПЗ, датчики, фізичні пристрої, які без участі людини передають дані через Інтернет. У процесі збору даних «розумні пристрої» збирають інформацію про свій стан та середовище, відправляють дані до серверів або хмарних платформ через Bluetooth, Wi-Fi, інші спеціальні мережі. На основі аналізу даних система автоматично виконує необхідну дію (наприклад, оптимізує маршрут руху техніки, здійснює моніторинг стану верстатів, трекінг транспорту тощо);

10. Process Mining (інтелектуальний аналіз бізнес-процесів, або процесний майнінг) – технологія, з використанням якої автоматично відновлюються бізнес-процеси, проводиться їх фактичний аналіз. Дана технологія основана на використанні цифрових слідів з IT-систем та реальних даних, щоб показати реальну роботу певних процесів з використанням таких етапів:

– discovery (виявлення) – на основі зібраних даних автоматично формується візуальна модель;

– conformance (відповідність) – порівняння фактичного виконання процесу з регламентом з метою виявлення порушень або відхилень;

– enhancement (покращення) – оптимізація процесів на основі виявлення неефективних дій, «вузьких місць», зайвих етапів;

11. Digital Twins (цифрові двійники) – віртуальні високоточні копії фізичних процесів, об’єктів, систем, які функціонують в умовах реального часу та через мережу датчиків (IoT) синхронізуються з оригіналом для аналізу й прогнозування результатів, моделювання поведінки системи без ризику для реального світу. Дана технологія слугує основою індустрії 4.0, дозволяючи бізнесу оптимізувати процеси, тестувати гіпотези, уникаючи аварій;

12. API-інтеграція поєднує програмні додатки через прикладний програмний інтерфейс (API), що дозволяє програмам автоматично й безпечно здійснювати обмін даними без потреби ручного введення інформації. Коли певна програма потребує даних від іншої програми, вона здійснює відправлення стандартизованого запиту, отримує відповідь, виконує задану дію. Прикладами

такої інтеграції у сфері електронної комерції є підключення платіжної системи з метою миттєвої обробки оплат, у сфері логістики – інтеграція сайту з Новою поштою (для створення експрес-накладних та розрахунку вартості доставки), у сфері маркетингу – автоматичне передавання до CRM-системи даних конкретного клієнта з форми на сайті.

Безперечними перевагами API-інтеграції є раціональне використання часу за рахунок автоматизації рутинних завдань, мінімізація впливу «людського фактора» у процесі копіювання інформації, можливість швидкого додавання нових функцій;

13. Електронний документообіг – це управління створенням документа (документ формується в системі обліку), його підписанням (відправник накладає свій КЕП, гарантуючи автентичність інформації та її цілісність), обміном (файл передається контрагенту миттєво через захищені канали зв'язку), затвердженням (отримувач перевіряє документ, підписує його своїм КЕП), зберіганням (архівуванням) документів у цифровому форматі в електронному архіві. При цьому пошук документів здійснюється за лічені секунди, відсутні витрати на формування паперової документації, забезпечується доступність документів з різних пристроїв;

14. Таксономія UA XBRL (Extensible Business Reporting Language) – міжнародний відкритий стандарт з формування електронної фінансової звітності за МСФЗ, розроблений для забезпечення структуризації машино зчитуваних файлів за допомогою тегів (спеціальних міток), швидкої перевірки та аналізу інформації, зручного обміну даними між суб'єктами господарювання, інвесторами, державними регуляторами. При цьому забезпечуються:

– універсальність підходу (кожен показник звіту отримує цифровий код (тег) у відповідності з єдиним довідником (таксономією));

– можливість миттєвого зчитування інформації, здійснення перевірки цифрових даних та їх аналізу;

– зменшення кількості помилок (в системі забезпечується автоматичний контроль взаємозв'язку між різними показниками та формами звітності).

Важливими складовими технології XBRL є словник термінів та показників, які описують правила формування звітності за МСФЗ, файл з числовими даними, розміченими тегами, а також формат, який робить звіт зручним для сприйняття користувачем;

15. Predictive Analytics – метод аналізу даних, оснований на поєднанні економічної інформації, статистичних алгоритмів, машинного навчання. Він забезпечує отримання ймовірної оцінки майбутнього на основі передбачення майбутніх подій, ринкових трендів, людської поведінки шляхом збору даних з різних джерел, пошуку закономірностей та прихованих взаємозв'язків, створення математичних прогнозних моделей.

Predictive Analytics застосовується у сфері логістики (обслуговування техніки, планування запасів), маркетингу (забезпечує прогнозування відтоку клієнтів, обсягів продажу, попиту), фінансово-банківській сфері (при виявленні шахрайства, оцінці ризиків кредитування).

Концептуальні принципи побудови цифрової обліково-аналітичної системи підприємства узагальнені на рис. 2.

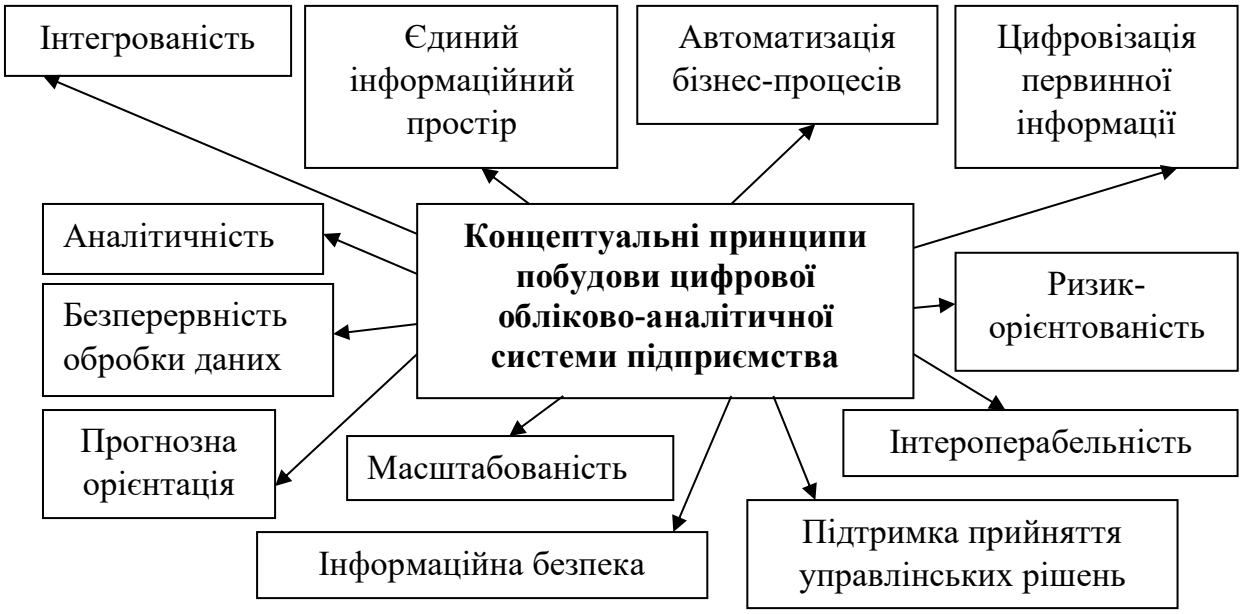


Рис. 2. Концептуальні принципи побудови цифрової обліково-аналітичної системи підприємства

*Джерело: сформовано автором на підставі [4; 6; 7; 11]*

Інтегрованість обліково-аналітичної системи проявляється у поєднанні управлінського, фінансового обліку, аналізу, контролю в єдину інформаційну систему, функціонування якої забезпечує швидкий збір, обробку даних, їх передавання для прийняття обґрунтованих бізнес-рішень без дублювання завдань за підрозділами підприємства. При інтегрованому підході формується єдине середовище, у рамках якого здійснюється автоматичне оновлення інформації та перетворення її на аналітичні звіти, зникає потреба ручного перенесення цифр з однієї програми в іншу, а бухгалтерські дані відразу стають основою для управлінського планування та фінансового аналізу. Усі структурні підрозділи підприємства працюють на основі використання інформації, актуальної в режимі реального часу.

Єдиний інформаційний простір у межах обліково-аналітичної системи формує цілісна сукупність програмних технологій, баз даних, інформаційних потоків, стандартів, що забезпечує швидкий збір, надійне зберігання даних, їх надання для прийняття рішень на всіх рівнях управління. Основними компонентами такого простору є централізована база даних (єдине сховище первинної та звітно-облікової інформації без її дублювання), сучасне програмне забезпечення (ERP-системи, аналітичні інструменти, хмарні сервіси), уніфіковані правила (спільні класифікатори, стандарти документообігу, методи оцінки показників), а також керівники різних рівнів та зовнішні зацікавлені користувачі. При цьому забезпечується можливість усунення інформаційних бар’єрів між підрозділами підприємства, зменшується ризик помилок завдяки автоматичному введенню даних та їх перевірці, пришвидшується процес формування звітності, підвищується якість аналітичних прогнозів.

Автоматизація бізнес-процесів забезпечує раціональне функціонування обліково-аналітичної системи на основі оперативного збору даних, їх перетворення на єдиний цифровий потік, обробки та аналізу. При цьому поєднуються ERP, CRM, BI-платформи, суттєво зменшується кількість помилок та зникає ручна рутина, а керівник отримує точні дані для оперативного прийняття рішень у режимі реального часу. Автоматизація орієнтована на опис завдань та пошук слабких ланок перед перенесенням даних у програму, автоматичне внесення даних з накладних, банківських рахунків, виписок за допомогою роботизовано автоматизації (RPA) або спеціальних модулів, поєднання у єдину базу даних інформації про складські операції, виробництво та продаж, налаштування BI-систем з метою побудови інтерактивних графіків, оцінки ключових показників (KPI), прогнозування ризиків та ключових аспектів розвитку бізнесу.

Для підприємства головними перевагами автоматизації бізнес-процесів є:

– швидкість (звіти формуються за лічені секунди замість днів або тижнів ручної роботи);

– точність (при перенесенні цифрових даних зменшується вплив людського чинника та пов’язані з цим помилки);

– прозорість (керівник у будь-який момент бачить загальну картину щодо наявності фінансів, обсягу складських залишків, а також щодо ефективності функціонування команди загалом);

– прогнозованість (побудована система дає можливість моделювати доходи та витрати на майбутні проміжки часу на основі урахування тенденцій їх змін за минулі періоди).

Популярними інструментами для забезпечення автоматизації бізнес-процесів підприємства є програми гнучкої автоматизації та комплексного управління, зокрема, Odoo Cloud, локальні рішення по типу систем класу BAS для ведення обліку, аналітичні BI-платформи (Power BI, Tableau), які

перетворюють цифрові дані на зручні формати для їх розуміння власниками бізнесу, інструменти роботизації (RPA), які забезпечують виконання однотипних операцій та звірок.

Цифровізація первинної інформації являє собою переведення паперових первинних документів під час введення у систему в зручний цифровий формат. У такий спосіб пришвидшується збір даних, мінімізується виникнення помилок в інтегрованій обліково-аналітичній системі, формується надійна основа для проведення подальшого аналізу та ухвалення рішень. Важливими етапами цифровізації первинних даних є їх збір та введення, розпізнавання, верифікація та зберігання.

При зборі даних використовується інформація з електронних накладних, інтеграція даних з банківськими виписками, здійснюється сканування штрих-кодів, RFID-міток. У процесі розпізнавання даних застосовують технології штучного інтелекту та оптичного розпізнавання символів (OCR) для автоматичного зчитування реквізитів із документів. Верифікація передбачає автоматичну перевірку даних на предмет їх достовірності, логічної повноти, відсутності дублікатів. Для забезпечення зберігання інформації здійснюється її розміщення у захищених хмарних сховищах, а для гарантування незмінності записів використовуються технології blockchain.

Цифровізація первинної інформації забезпечує її миттєве надходження зі складу, виробництва та іншого місця події до загальної бази даних, зниження ймовірності виникнення помилок через ручне введення даних та зменшення впливу людського фактора, побудову звітів у режимі реального часу з використанням BI-систем, швидку обробку великих масивів даних (Big Data), повний контроль керівництвом усіх господарських операцій.

Прояв принципу аналітичності у рамках функціонування обліково-аналітичних систем здійснюється через здатність системи збирати, накопичувати, деталізувати й структурувати первинні дані, перетворювати їх на

якісну інформаційну базу для проведення факторного аналізу, розробки прогнозів та ухвалення ефективних рішень. При аналітичному підході звичайний обліковий масив даних трансформується в дієвий інструмент управління суб'єктом господарювання, забезпечується перехід від простої констатації минулих подій до пошуку резервів.

У процесі аналізу здійснюється деталізація даних на основі розкладання результативних показників на елементи (за видами продукції, центрами відповідальності, ринковими сегментами тощо), їх інтерпретація та синтез через поєднання інформаційних потоків з метою виявлення трендів та закономірностей, налаштування облікових регістрів та бухгалтерських рахунків під особливі інформаційні потреби системи менеджменту. При цьому в рамках облікової підсистеми формується первинна база даних з виокремленням ознак за відповідними рівнями аналітичності (коди витрат, субконто, сегменти), у межах аналітичної підсистеми задля обробки підготовлених даних застосовуються відповідні методи управлінського та фінансового аналізу, а в рамках контрольної підсистеми забезпечується оперативне виявлення відхилень фактично отриманих показників від нормативних або очікуваних. Такий підхід забезпечує зниження ризиків на різних етапах прийняття рішень внаслідок використання достовірних деталізованих розрахунків, оперативність доступу менеджерів різних рівнів до зрізів інформації з урахуванням критеріїв ефективності, можливість моделювання сценаріїв розвитку бізнесу в майбутньому на основі використання ретроспективних даних.

Одним із базових принципів побудови обліково-аналітичної системи є забезпечення безперервності обробки даних, що охоплює повний життєвий цикл інформації (від моменту її первинного введення до формування звітності), усуває інформаційні розриви, передбачає вчасну реєстрацію підприємством господарських операцій, їх накопичення та аналіз в режимі реального часу, гарантуючи актуальність даних для подальшого прийняття рішень. Інформація

потрапляє до системи не періодично, а по мірі здійснення відповідних господарських фактів, пов'язуючи оперативний, управлінський, фінансовий облік у єдину мережу, мінімізуючи час між моментом безпосередньої фіксації події та її відображенням в управлінських звітах.

Важливими технічними та логічними вимогами для забезпечення безперервності обробки даних є їх автоматизоване введення на основі використання RFID, штрих-кодування, API-інтеграцій з CRM-системами, постійний моніторинг системи через її здатність автоматично запускати тригери чи аналітичні алгоритми при зміні показників, цілісність та єдність інформації, оскільки на етапах її передачі між модулями системи забезпечується запобігання дублюванню інформації або її втраті.

При забезпеченні безперервності обробки даних керівники різних ланок отримують актуальну інформацію про стан справ на поточний момент часу, мають можливість будувати тренди і прогнози, швидко виявляти помилки, відхилення, фінансові загрози до моменту настання критичності їхнього прояву.

Прогнозна орієнтація, як важливий принцип побудови обліково-аналітичної системи, передбачає генерацію інформації випереджувального характеру для обґрунтування стратегічних рішень та запобігання ризикам, спрямовує систему на забезпечення переходу від простої констатації минулих подій до розробки моделі майбутнього стану підприємства. При реалізації цього принципу проявляється здатність системи використовувати прогнозні моделі, оперативно реагувати на зміни кон'юнктури ринку, відбувається поєднання бухгалтерського обліку, управлінського аналізу, бюджетування та трансформація обліку на інструмент передбачення, здійснюється оцінка ймовірних втрат до моменту їхнього виникнення, узгодження фактичних даних з майбутніми цільовими орієнтирами бізнесу. Ефектом від застосування цього принципу є вчасне коригування бізнес-процесів з урахуванням зміни зовнішніх умов, підвищення

дієвості контролю за використанням ресурсів, суттєве зниження рівня невизначеності у процесі прийняття рішень.

Масштабованість як принцип формування обліково-аналітичної системи підприємства означає її здатність швидко адаптуватися до зміни обсягів ведення бізнесу, до збільшення потоку даних без втрати точності й швидкості їх обробки для забезпечення якості управлінських рішень. При упровадженні даного принципу забезпечується здатність системи повною мірою охоплювати діяльність новостворених структурних підрозділів, можливість додавати нові розрізи аналітики без кардинальної перебудови бази даних, а інформаційна структура підприємства гарантовано не стає «вузьким місцем» під час масштабування бізнесу, що дає йому можливість без перешкод нарощувати виробничі потужності, оптимізувати IT-інфраструктуру та витрати на модернізацію програмного забезпечення.

Організаційний аспект принципу масштабованості в елементах обліково-аналітичної системи проявляється через раціональний розподіл повноважень та доступу до даних, розширення кола користувачів інформації без зниження загальної продуктивності функціонування системи. Методологічний аспект принципу масштабованості в елементах системи проявляється через застосування універсальних обліково-аналітичних стандартів, які можна без проблем екстраполювати на нові продукти або види діяльності підприємства, через побудову більш складних аналітичних моделей з переходом до стратегічного контролінгу. Програмно-технологічний аспект принципу масштабованості в елементах обліково-аналітичної системи проявляється через інтеграцію сучасних ERP-систем та баз даних з урахуванням зростаючих потреб бізнесу, через спроможність програмного забезпечення обробляти все більші обсяги транзакцій без затримки процесу формування звітності.

Одним із принципів формування обліково-аналітичної системи є ризик-орієнтованість, що означає орієнтацію процесу збору даних, їх обробки,

інтерпретації та аналізу на виявлення інформаційних, господарських, фінансових ризиків, їх оцінку та мінімізацію. При такому підході обліково-аналітична система перетворюється з пасивного реєстратора подій із минулого на дієвий чинник обґрунтування рішень та попередження загроз в умовах невизначеності, забезпечується своєчасне виявлення ризиків, а контрольні та аналітичні дії спрямовуються на найбільш ризикові бізнес-процеси.

При ризик-орієнтованому підході в обліковому блоці здійснюється налаштування регістрів та рахунків на виокремлення операцій з високим рівнем ризику. У межах аналітичного блоку використовуються методи економічного моделювання, експертні оцінки, стрес-тестування для оцінки ймовірності настання негативних подій, розрахунок величини їхнього впливу на результати діяльності підприємства. Контрольний блок забезпечує інтеграцію внутрішнього контролю у контури руху облікових даних з метою запобігання порушенням нормативно-законодавчих вимог, виникненню помилок, недопущенню шахрайства.

Перевагами впровадження принципу ризик-орієнтованості є підвищення аналітичності звітності та достовірності вихідних даних для їх використання внутрішніми та зовнішніми користувачами, покращення здатності підприємства швидко реагувати на зміни в ринковій кон’юнктурі та операційній діяльності, підвищення якості управління ризиками на різних організаційних рівнях.

Інтероперабельність як один із принципів формування обліково-аналітичної системи означає здатність її програмних модулів та компонентів безперебійно працювати, оперативно здійснюючи обмін даними та забезпечуючи їх єдиний інформаційний потік. При цьому різні бази даних поєднуються в єдине ціле, забезпечується швидка передача інформації між структурними підрозділами підприємства та легке додавання нових програм чи модулів. Дані зберігаються таким чином, щоб їх «розуміли» різні програми, а керівники мають змогу бачити повну картину розвитку бізнесу в режимі реального часу.

Важливим принципом формування обліково-аналітичної системи підприємства є інформаційна безпека, яка гарантує захищеність даних від витоку, втрати чи спотворення, забезпечує цілісність, конфіденційність, доступність інформації, необхідної керівникам для збереження активів та ухвалення ефективних рішень. У рамках кожного етапу роботи з даними, від моменту їх збору до аналізу для розробки рішень, має забезпечуватися запобігання навмисній або випадковій зміні облікової інформації, стабільна робота хмарних сховищ, баз даних, бухгалтерських програм, надійний захист від несанкціонованого доступу шляхом обмеження прав користувачів на перегляд звітів та їх зміну, а також регулярне створення копій з метою швидкого відновлення інформації у випадках збою.

Ключовими завданнями забезпечення інформаційної безпеки в обліково-аналітичній системі є дотримання вимог законодавства у сфері захисту персональних даних, збереження комерційної таємниці, своєчасне виявлення махінацій, помилок та спроб зламу системи, забезпечення безперебійної роботи бізнесу завдяки здійсненню постійного контролю за рухом інформаційних потоків.

Важливим принципом побудови обліково-аналітичної системи підприємства є підтримка прийняття управлінських рішень. Цей принцип гарантує орієнтованість процесу збору, обробки та видачі виробничо-фінансових даних не на пасивну реєстрацію подій, які вже відбулися, а на надання системі менеджменту достовірної та актуальної інформації для прогнозування діяльності та ефективного управління підприємством. При реалізації зазначеного принципу обліково-аналітична інформація перетворюється на дієвий інструмент управління, оскільки в системі не лише фіксуються витрати, доходи, інші важливі показники фінансово-господарської діяльності, а й здійснюється побудова аналітичних моделей, забезпечується перехід від ретроспектив до прогнозування, релевантність даних, оперативне надходження необхідної

інформації саме у той момент, коли у системі менеджменту розробляються відповідні тактичні та стратегічні кроки.

Для забезпечення якісної підтримки прийняття управлінських рішень структура обліково-аналітичної системи повинна відповідати наступним основним критеріям:

– адаптивність, що передбачає можливість швидкої зміни набору показників з урахуванням потреб керівництва на конкретний момент часу;

– достатня деталізація, при якій забезпечується можливість розгортання даних у розрізі продуктів, контрагентів, центрів відповідальності тощо;

– інтеграція управлінського, фінансового обліку, контролю та бізнес-аналізу.

Загальна концепція формування цифрової обліково-аналітичної системи являє собою багаторівневу модель, у рамках якої поєднуються джерела надходження даних, цифровий облік, інтеграція даних, аналітика, інтелектуалізація даних та ухвалення рішень (рис. 3).

Використання даних обліково-аналітичної системи у процесі розв’язання управлінських завдань проходить наступні етапи:

1. Ідентифікація проблеми, постановка цілей;

2. Формування альтернативних рішень та варіантів дій, оцінка ризиків з урахуванням даних аналітики;

3. Вибір оптимального варіанта рішення;

4. Контроль виконання ухваленого рішення, аналітична оцінка відхилень фактичного результату від очікуваного.

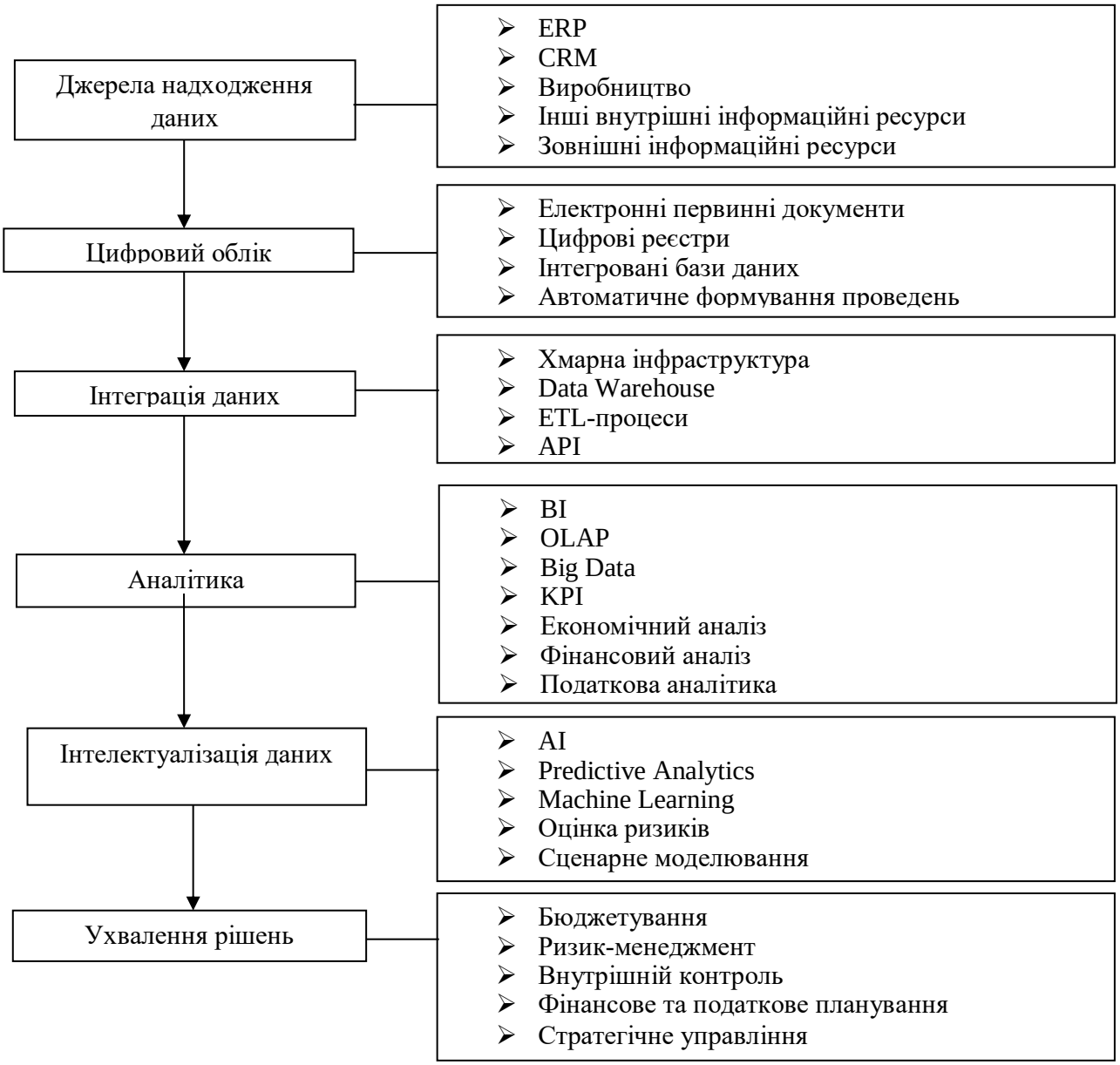



Рис. 3. Загальна концепція формування цифрової обліково-аналітичної системи підприємства

*Джерело: сформовано автором на підставі [4; 6; 7; 11]*

Загалом концепцію побудови цифрової обліково-аналітичної системи підприємства доцільно розглядати як процес формування інтегрованої інтелектуальної платформи на основі хмарних сервісів, технологій AI, Big Data, у рамках якої поєднуються цифровий облік, внутрішній контроль, податкове

адміністрування, прогнозування, бізнес-аналітика, підтримка прийняття управлінських рішень.

В сучасних умовах цифровізація обліку, контролю та аналізу є глобальним трендом, спрямованим на забезпечення автоматизованого збору, перевірки, обробки даних про фінансово-господарську діяльність. Вона забезпечує поступовий перехід від використання паперових та локальних електронних носіїв інформації до інтегрованих обліково-аналітичних платформ, систем електронного документообігу, хмарних сервісів.

### 5.3. Функціональна модель та інструментарій цифрової трансформації обліково-аналітичної системи

Цифрову трансформацію обліково-аналітичної системи підприємства необхідно розглядати не лише як автоматизацію ведення обліку, а з точки зору необхідності комплексної перебудови процесів формування, зберігання, передавання, аналізу та використання інформації для розробки та ухвалення управлінських рішень. Виходячи з цього, її інструментарій повинен широко охоплювати технологічні, організаційні, інформаційні, аналітичні, управлінські аспекти.

Інструменти цифрової трансформації обліково-аналітичної системи підприємства можна структурувати за наступними функціональними групами (табл. 1):

Таблиця 1. Структуризація інструментів цифрової трансформації обліково-аналітичної системи підприємства

| **Функціональна група інструментів** | **Ключові інструменти** | **Основне призначення** |
|---|---|---|
| Автоматизація облікових процесів | ERP, бухгалтерські онлайн-платформи BookKeeper, Dilovod, iFin, SmartFin, Taxer, системні локальні та хмарні пакети BAS, спеціалізовані торговельні й складські програми Торгсофт, Huge Profit | Автоматизація збору та обробки облікових даних |
| Інтеграція інформаційних систем | API, ESB, EDI, IPaaS | Об'єднання обліку з іншими функціональними підсистемами |
| Хмарні технології та цифрова інфраструктура | Cloud ERP, SaaS, IaaS, PaaS, хмарні сховища | Забезпечення доступу, безперервності роботи, масштабованості |
| Цифровий документообіг | ЕДО, КЕП, OCR, e-invoising | Перехід від паперових документів до електронних |
| Big Data та управління даними | Data Lake, Data Warehouse, Master Data Management, ETL/ELT | Якісне управління великими масивами інформації |
| Аналітика та Business Intelligence | BI, Data Mining, OLAP | Перетворення даних на аналітичну інформацію |
| Прогнозування та інтелектуальна автоматизація | AI, RPA, ML | Виявлення закономірностей, прогнозування, підтримка рішень |
| Цифрова безпека та контроль | IAM, Blockchain, MFA, Audit Trail | Захист інформації, контроль за здійсненням цифрових операцій |

*Джерело: сформовано автором на підставі [2-4; 6; 7; 11]*

Розглянуті функціональні групи інструментів цифрової трансформації обліково-аналітичної системи підприємства можна поєднати за наступними рівнями: цифровізація даних; автоматизація процесів; інтеграція інформації; інтелектуалізація аналітики та процесу управління.

Сучасний ринок облікових систем поєднує рішення різного рівня:

1) глобальні корпоративні ERP-системи (Enterprise Resource Planning) – платформи для великих підприємств та міжнародних корпорацій, які поєднують у єдиному просторі виробництво, логістику, ланцюги постачання, кадри, фінанси та потребують значного інвестування коштів на їх впровадження й адаптацію;

2) локальні бухгалтерські та хмарні пакети BAS (Business Automation Software) – сучасні програмні продукти, призначені для автоматизації бізнесу та ведення обліку, які мають десктопні (локальні) та хмарні варіанти й вимагають належного програмного супроводу;

3) бухгалтерські онлайн-платформи:

– BookKeeper – хмарний сервіс для малого та середнього бізнесу з досить простим інтерфейсом;

– Dilovod – українська хмарна система, у якій поєднуються управлінський, фінансовий, оперативний облік, подача електронної звітності. Система створена як альтернатива програмам 1С та BAS, підходить для малого та середнього бізнесу;

– iFin – зручний український онлайн-сервіс, призначений для ведення бухгалтерського обліку, формування та подання електронної звітності для ФОП і ТОВ. Забезпечується можливість роботи через інтернет з податковими органами, Пенсійним фондом, Держстатом;

– SmartFin – хмарна програма, призначена для ФОП, власників малого бізнесу з найманими працівниками, бухгалтерів-аутсорсерів, компаній, які надають бухгалтерські послуги. Основними можливостями даного сервісу є розрахунок зарплати, ведення кадрового обліку, формування та подання регламентованої податкової звітності;

– Taxer – онлайн-сервіс для ведення ФОП та формування податкової звітності, який дає можливість підприємцям вести облік доходів без найму

бухгалтера, здійснювати автоматичний розрахунок податкових платежів, формувати та надсилати за допомогою КЕП декларації до податкової служби;

4) спеціалізовані торговельні й складські програми:

– Торгсофт – програма для автоматизації складського обліку, роздрібної та гуртової торгівлі, мереж магазинів;

– Huge Profit – хмарний сервіс, призначений для контролю залишків, роботи з ТТН у рамках управління інтернет-магазинами, маркетплейсами, товарним бізнесом.

Відмовившись від російських програмних продуктів, український бізнес адаптується до нових реалій, забезпечуючи цифровізацію документообігу, інтеграцію з банківськими установами, сервісами ДПС, міжнародними партнерами. Зокрема, ТОВ «Центр бухгалтерського аутсорсингу», що спеціалізується на повному супроводі комплексного ведення бухгалтерського й податкового обліку, рекомендує підприємствам України використовувати у процесі ведення обліку такі надійні та функціональні програми (табл. 2):

Таблиця 2. Програми бухгалтерського обліку, найбільш рекомендовані до використання на підприємствах України

| **Програма** | **Опис** | **Тип та основне призначення** |
|---|---|---|
| MASTER: Бухгалтерія https://masterbuh.com/ | ERP-платформа для ведення бухгалтерського й податкового обліку, яка підтримує електронний документообіг, інтегрується з API банків та ДПС, має модульну структуру, підходить для суб'єктів державного сектору, підприємств середнього та великого бізнесу, включає галузеві версії (агросектор, медицина, ЖКГ, бюджет) | Тип: десктоп + хмара<br><br>Основне призначення: ERP, бухгалтерія, галузеві рішення |
| Bimp https://bimpsoft.com/ | Сучасна хмарна програма, призначена для спрощення рутинних операцій, ведення документообігу, обліку складу, товарів, взаєморозрахунків, закупівель, фінансів, автоматичного | Тип: хмара<br><br>Основне призначення: склад, |

| **Програма** | **Опис** | **Тип та основне призначення** |
|---|---|---|
| | формування актів, рахунків, звітів. Хмарна архітектура забезпечує можливість роботи з будь-якого пристрою. Дане рішення орієнтоване більшою мірою на управлінський облік та автоматизацію, на малий і середній бізнес (у т.ч. виробництво, рітейл, e-commerce) | облік товарів, взаєморозрахунки |
| Finmap https://finmap.online/ | Простий хмарний сервіс для ведення управлінського й фінансового обліку, який не подає звітність до податкової, однак часто використовується фрилансерами, стартапами, власниками малого бізнесу, інтегрується з банками, сервісами CRM | Тип: хмара<br><br>Основне призначення: управлінський облік, Cashflow |
| iFin https://www.ifin.ua/ | Один з найбільш популярних сервісів для подачі електронної звітності до ДПС, ДССЗІ, який орієнтований на малі підприємства та ФОП, підтримує КЕП, автоматично оновлює платформи, дає можливість формувати електронні документи, здійснювати реєстрацію ПН, забезпечує ведення обліку на базовому рівні (без складного функціоналу) | Тип: хмара<br><br>Основне призначення: податкова звітність (ТОВ, ФОП) |
| СОТА https://sota-buh.com.ua/ | Дає можливість вести облік, підписувати документи за допомогою КЕП, працювати з ПН, подавати звітність, підтримує обмін з банками, клієнтами, органами контролю. Система максимально адаптована під українське законодавство | Тип: хмара<br><br>Основне призначення: документообіг, звітність, ПН |
| BookKeeper https://bookkeeper.kiev.ua/ | Підтримує в одній базі необмежену кількість компаній, дає можливість вести оперативний облік складу, торгівлі, зарплати, каси, необоротних активів, ПН, ЗЕД, підходить для малого та середнього бізнесу | Тип: хмара<br><br>Основне призначення: каса, склад, зарплата, ПН, ЗЕД |

| **Програма** | **Опис** | **Тип та основне призначення** |
|---|---|---|
| Облік Софт https://obliksoft.com.ua/ | Проста програма, орієнтована на ФОП і малий бізнес, яка встановлюється на комп'ютер, має простий інтерфейс, працює без інтернету, призначена для ведення обліку операцій, друку податкових документів, формування звітності | Тип: десктоп<br><br>Основне призначення: простий облік для ФОП |
| SmartFin https://smartfin.ua/ | Призначена для ведення обліку в сфері малого бізнесу, підтримує облік витрат, доходів, зарплати, друк первинних документів, кадровий облік, формує електронну звітність. Сервіс має мобільну версію та постійно оновлюється з урахуванням змін у законодавстві | Тип: хмара<br><br>Основне призначення: витрати, доходи, зарплата, ПН |
| Dilovod https://dilovod.ua/ | Сервіс для ведення обліку складу, продажів, CRM, який автоматично резервує дані у хмарі, забезпечує технічну підтримку, інтеграцію з ПРРО, банками. Не потребує глибоких знань з бухгалтерського обліку, дозволяє контролювати бізнес онлайн, вести облік та формувати електронну звітність для різних систем оподаткування | Тип: хмара<br><br>Основне призначення: універсальна облікова система, CRM, ПРРО |
| Дебет Плюс https://debet.com.ua/ | Українська ERP-платформа, призначена для автоматизованого ведення обліку в організаціях різного масштабу. Має модульну структуру, що забезпечує можливість ведення обліку в агросфері, торгівлі, ЖКГ, медичних закладах, бюджетних установах тощо. Підходить для організацій із гнучкою адаптацією під галузеві процеси | Тип: десктоп + SaaS<br><br>Основне призначення: ERP, агросфера, бюджет, ЖКГ, медицина |
| Клієнт-банк облік (Monobank, Приват24, ПУМБ) | Вбудована міні-система для ведення обліку в онлайн-кабінетах, яка підходить для малого бізнесу, ФОП 3 групи. Так, через Приват24 доступні облік ПН, надсилання звітів, | Тип: інтегроване рішення<br><br>Основне призначення: |

| Програма | Опис | Тип та основне призначення |
|---|---|---|
| | інтеграція з сервісами ДПС, через Monobank - автоматичне генерування рахунків, подання податкової звітності тощо | автоформування актів, рахунків (ФОП) |
| Арт-Звіт Pro https://art-zvit.com.ua/ | Програма для ведення документообігу із функціями КЕП, роботи з ПН, ТТН, формування електронної звітності. Забезпечується інтеграція з ERP-системами, PPO Art Zvit Pro | Тип: десктоп + хмара<br><br>Основне призначення: документообіг, подання електронної звітності |

*Джерело: узагальнено автором на підставі [9]*

Доцільно зазначити, що одним з ключових інструментів цифрової трансформації є ERP-системи, оскільки їх використання забезпечує інтегроване управління обліком, фінансами, логістикою, закупівлями, запасами, продажами, виробництвом, персоналом, основними засобами, податками. При цьому інформація вводиться одноразово, а використовується різними підсистемами багаторазово, що автоматично забезпечує перехід від моделі «господарська операція - документ - звітність» до моделі «господарська операція - автоматичне формування даних - інтегрована база даних - аналітика - формування управлінських рішень».

Вибір інструментів автоматизації облікових процесів залежить від масштабів діяльності підприємства та специфіки виконуваних ним завдань.

Цифрова трансформація передбачає не тільки здійснення автоматизації окремих господарських операцій, а й інтеграцію інформаційних потоків за принципом «CRM - ERP - бухгалтерський облік - склад - банк - податковий облік - BI».

Ключовими технологіями та інструментами, які забезпечують обмін даних, зв'язок між бізнес-системами та різними комп’ютерними програмами є API

(Application Programming Interface), ESB (Enterprise Service Bus), EDI (Electronic Data Interchange), IPaaS (Integration Platform as a Service).

API (Application Programming Interface) забезпечує здійснення автоматизованого обміну даними між програмними системами, є набором готових команд та правил, з використанням яких різні програми можуть контактувати між собою. API бере запит від певної програми, передає його іншій програмі та повертає назад результат, забезпечує швидкий взаємозв'язок у режимі реального часу.

ESB (Enterprise Service Bus) – це централізована програмна архітектура, призначена для обміну повідомленнями між різними внутрішніми системами підприємства. Вона діє всередині крупного підприємства по принципу транспортної мережі, допомагаючи здійснити маршрутизацію даних, переформатувати їх у потрібний формат та забезпечуючи неможливість прямого підключення систем.

EDI (Electronic Data Interchange) забезпечує електронний обмін типовими (стандартизованими) бізнес-документами (накладними, рахунками тощо) між різними підприємствами, який працює за чіткими міжнародними стандартами та передається через спеціальних провайдерів. Досить часто EDI використовується у сфері логістики, виробництва, ритейлу, забезпечує зв'язок постачальників з мережами супермаркетів.

IPaaS (Integration Platform as a Service) – хмарні платформи, які мають зручні візуальні інтерфейси для налаштування взаємозв'язку між сервісами (ERP, CRM, пошта), забезпечують поєднання хмарних і локальних застосунків без написання коду. Прикладами таких платформ є Zapier, Dell Boomi, Make.

Хмарна інфраструктура забезпечує переведення обліково-аналітичної системи із локального у цифрове середовище, яке є доступним через мережу. Хмарні технології розглядають як набір послуг, які надають через інтернет програми, комп'ютерні ресурси, сховища без необхідності придбавати власні

сервери. До їх переліку належать моделі SaaS, IaaS, PaaS, спеціалізовані рішення, такі як Cloud ERP, хмарні сховища.

Основними хмарними моделями, які найбільш часто використовуються у сфері бізнесу, є SaaS (програмне забезпечення як сервіс), IaaS (інфраструктура як сервіс), PaaS (платформа як сервіс). Їх перевагами є забезпечення віддаленого доступу до інформації, її централізоване зберігання, масштабованість, швидке оновлення програм, можливість здійснення резервного копіювання даних та роботи декількох підрозділів підприємства у єдиній системі (що особливо є актуальним для підприємств з територіально відокремленими підрозділами).

При використанні SaaS готові програми працюють у браузері, користувач нічого додатково не налаштовує, а використовує їх як готовий софт. Прикладом SaaS є Microsoft 365, Gmail.

У межах IaaS забезпечується оренда мереж, пам'яті, віртуальних серверів, а користувач повністю керує програмами та операційною системою. Прикладом IaaS є GigaCloud, Amazon Web Services.

PaaS забезпечує готове середовище для розробників (інструменти запуску кодів, бази даних). При цьому користувач створює програми, а провайдер відслідковує роботу серверів. Прикладом PaaS є Microsoft Azure, Google App Engine.

Хмарна система планування ресурсів підприємства Cloud ERP (SAP, NetSuite) є різновидом SaaS для бізнесу, у якому поєднуються програми для управління складом, продажами, кадрами, фінансами.

Хмарні сховища (Google Диск, Dropbox) являють собою сервіси для зберігання файлів, їх резервного копіювання та для обміну файлами в інтернеті. Доступ до цих файлів забезпечується із будь-якого пристрою.

Важливою складовою сучасного цифрового офісу є ЕДО (електронний документообіг), що забезпечує створення електронного документа, його погодження, підписання, передачу, реєстрацію, зберігання, пошук, контроль статусу. У такий спосіб значно пришвидшується робота підприємства,

забезпечується можливість здійснити заміну паперових документів на цифрові файли, які зберігаються в електронних архівах. Захист файлів від підробки забезпечується шляхом використання КЕП – кваліфікованого електронного підпису, який є цифровим аналогом звичайного підпису та печатки (ідентифікує підписанта), що надає електронному документу юридичної сили, гарантує цілісність даних.

З використанням OCR (Optical Character Recognition) здійснюється оптичне розпізнавання інформації з первинних документів, накладних, актів, рахунків, договорів. При цьому скани перетворюються на редагований текст, що дає можливість автоматично зчитати дані з паперових чеків або рахунків. Загалом процес трансформації даних відбувається в такий спосіб: «скан документа - OCR - структуризація даних - ERP - бухгалтерські записи», що суттєво скорочує обсяги ручної роботи.

Виставлення рахунків та їх передача у спеціальних цифрових форматах здійснюється через e-invoising. При цьому дані з рахунку потрапляють автоматично в бухгалтерську програму (без ручного введення), пришвидшується оплата товарів або послуг, зменшується кількість помилок.

Електронні архіви є захищеним сховищем для забезпечення довготермінового зберігання цифрових документів, а також їх конфіденційності за допомогою прав доступу, у рамках якого здійснюється швидкий пошук документів за датами, тегами, контрагентами.

Для якісного управління великими масивами інформації застосовують Data Lake (озеро даних, де зберігаються необроблені дані), Data Warehouse (сховище даних, де зберігаються чисті дані для звітів), Master Data Management (у рамках якого підтримується правильність ключових бізнес-записів), ETL/ELT (де дані змінюються та переміщуються):

– Data Lake забезпечує зберігання структурованих та неструктурованих (необроблених, неформованих) даних у будь-якому форматі (тексти, журнали, відео), є дешевим в експлуатації та відмінно підходить для машинного навчання.

При цьому можуть поєднуватися бухгалтерські записи, документи, Excel-файли, GPS-дані, показники датчиків, супутникові дані, зображення, текстова інформація тощо;

– Data Warehouse забезпечує зберігання чистих, формованих даних, створених для швидкої підготовки бізнес-звітів та SQL-запитів. Сховище даних консолідує інформацію з системи обліку, ERP, CRM, виробничих систем, систем управління персоналом та зовнішніх джерел, формуючи у такий спосіб єдине інформаційне середовище для аналітики;

– Master Data Management створює єдине надійне джерело ключових складників бізнесу в такий спосіб, щоб усі програми використовували однакові дані. MDM забезпечує формування єдиних довідників номенклатури, центрів відповідальності, рахунків, контрагентів, що зменшує дублювання інформації та кількість помилок;

– ETL/ELT забезпечують вилучення даних, їх трансформацію та завантаження у єдине інформаційне середовище: ETL (вилучення, перетворення, завантаження) витягує дані, здійснює їх очистку перед збереженням, а потім зберігає їх у сховищі; ELT (вилучення, завантаження, перетворення) витягує дані, здійснює їх зберігання у необробленому вигляді, а потім, за потреби, очищує їх у хмарному середовищі.

Інтеграція даних дозволяє уникнути повторного введення інформації, дублювання даних, розбіжностей між системами, затримки процесу формування звітності.

Бізнес-аналітика (BI), Data Mining (інтелектуальний аналіз даних), OLAP (онлайн-аналітична обробка), інформаційні панелі та KPI (ключові показники ефективності) формують взаємопов’язану систему, у якій збираються, обробляються, аналізуються, візуально відображаються необроблені корпоративні дані з метою відстеження бізнес-цілей та прийняття обґрунтованих рішень.

Для візуального відображення важливих бізнес-фактів у режимі реального часу використовують інформаційні панелі (dashboards), формують ключові показники ефективності (KPI), які являють собою чіткі числа або цілі, що характеризують досягнення підприємством поставлених цілей.

Бізнес-аналітика поєднує широку систему методів та інструментів, які застосовуються для збору, очищення, вивчення бізнес-даних. BI є одним з ключових інструментів для забезпечення переходу від облікової до аналітичної інформації. При цьому поєднуються інтерактивні dashboards, drill-down, KPI-панелі, OLAP-аналіз, аналіз відхилень, сценарний аналіз, що змінює саму природу облікової інформації, забезпечуючи перехід від статичного звіту до інтерактивного управлінського інструменту.

В сукупності інструментів Data Analytics виокремлюють наступні рівні:

– Descriptive Analytics (дає можливість отримати відповідь на питання «що відбулося», передбачає використання форм звітності, dashboards, KPI);

– Diagnostic Analytics (дає можливість отримати відповідь на питання «чому це відбулося», передбачає використання способів детермінованого та стохастичного факторного аналізу, drill-down);

– Predictive Analytics (дає можливість отримати відповідь на питання «що може відбутися», передбачає використання статистичних моделей, інструментів прогнозування, ML);

– Prescriptive Analytics (дає можливість отримати відповідь на питання «що потрібно зробити», передбачає використання сценарного аналізу, оптимізаційних моделей, AI).

Predictive Analytics у поєднанні з Prescriptive Analytics забезпечують перехід від традиційних підходів у формуванні обліково-аналітичного забезпечення до системи інтелектуальної підтримки процесу прийняття управлінських рішень.

Data Mining, або інтелектуальний аналіз даних, є процесом пошуку закономірностей, правил, прихованих тенденцій у великих наборах даних з використанням інтелектуальної математики або AI.

OLAP (онлайн-аналітична обробка) – швидкий спосіб розгляду під різним кутом зору (час, продукт, регіон) багатошарових бізнес-даних.

При цьому в системи BI формуються необроблені дані. У процесі інтелектуального аналізу даних передбачаються майбутні потреби, а OLAP дає можливість менеджерам миттєво фільтрувати дані у необхідному розрізі. На основі цього формуються ключові показники ефективності (KPI), які відображаються на інтерактивних інформаційних панелях, таких як Power BI. На основі отриманої фактичної інформації менеджери відповідних рівнів приймають управлінські рішення.

Сучасними технологіями для оптимізації роботи та виконання завдань за допомогою комп'ютерної техніки є AI (Artificial intelligence), RPA (Robotic Process Automation), ML (Machine Learning). Так, AI імітує людське мислення, ML є частиною AI, призначеною для самостійного навчання на даних, а RPA на основі дотримання чітких правил автоматизує рутинні дії.

Штучний інтелект (AI, Artificial intelligence) розпізнає мову та зображення, замінює або доповнює думку людини при вирішенні нею складних завдань, робить висновки на основі узагальнення інформації. В обліково-аналітичній системі AI може використовуватися для здійснення автоматичної класифікації операцій, прогнозування доходів, витрат, грошових потоків, обсягів заборгованості, податкових платежів, виявлення нетипових операцій та аномалій, оцінювання ризиків, аналізу текстових документів. Система може автоматично визначати статичне відхилення певної операції від типових операцій підприємства, що може слугувати основою для внутрішнього контролю та аудиту, протидії шахрайству, управління ризиками. Водночас слід ретельно перевіряти отриману інформацію, враховувати можливість «галюціонування» інструментів AI.

Роботизована автоматизація процесів (RPA, Robotic Process Automation) – це програмні боти для виконання рутинних, повторюваних робіт, які імітують кліки миші та дії людини у програмах, працюють за чіткими інструкціями та

правилами. RPA дозволяє програмним роботам виконувати ряд повторюваних операцій: отримання виписки банку; перевірка правильності її формування; зіставлення платежів; формування бухгалтерських проведень; оновлення реєстру операцій; формування звіту.

Особливо доцільним використання RPA є для обробки первинних документів, перенесення даних, контролю реквізитів, звірки інформації, формування управлінських звітів.

Машинне навчання (ML, Machine Learning) дозволяє комп'ютерам навчатися на великих масивах інформації, покращує з часом отримані результати без використання додаткового програмування.

Ключовими технологіями й концепціями у сфері управління даними та кібербезпеки, які забезпечують незмінність історії дій у цифрових системах, контроль доступу користувачів, надійний захист інформації є IAM (Identity and Access Management), Blockchain, MFA (Multi-Factor Authentication), Audit Trail.

IAM (Identity and Access Management) – це управління ідентифікацією й доступом до інформації та програм підприємства. Його ключовими функціями є створення облікових записів, надання прав доступу, перевірка особи користувача.

Blockchain являє собою ланцюжок блоків, з'єднаних із записами даних, призначений для забезпечення зберігання інформації у децентралізованому вигляді. Його ключовими функціями є захист записів від змін та видалення, враховуючи, що кожна нова операція одночасно копіюється на багато комп'ютерів. Потенційно Blockchain може використовуватися для забезпечення прозорості транзакцій, автоматизації контрактів, відстеження ланцюгів постачання, підтвердження незмінності інформації. Наприклад, цифровим ланцюгом підтвердження інформації можуть бути поєднані виробник, переробне підприємство, логістична компанія та покупець.

Чим вищим є рівень цифровізації облікової системи, тим вищими стають вимоги до захисту інформації. До інструментарію, який використовується для

забезпечення захисту даних, відносять: IAM (управління ідентифікацією та доступом), MFA (багатофакторну автентифікацію), SIEM, DLP, резервне копіювання, шифрування інформації, антивірусний захист, забезпечення контролю доступу, ведення журналу подій, сегментування мережі. При цьому доступ до інформації повинен відповідати функціональним повноваженням працівника.

MFA (Multi-Factor Authentication) – це багатофакторна аутентифікація, що забезпечує додатковий захист при вході в систему, вимагаючи здійснення підтвердження особи двома й більше способами (пароль та код з СМС тощо).

Цифрова трансформація суттєво змінює й систему внутрішнього контролю. При безперервному аудиті контроль здійснюється у режимі постійного моніторингу показників та господарських операцій.

Audit Trail (слід подій, журнал аудиту, аудиторський слід, контрольний журнал) являє собою хронологічний запис усіх дій та подій в системі. При цьому фіксується історія створення, змін чи видалення даних (хто створив операцію, хто вніс у неї зміни та які саме зміни було внесено, коли це було зроблено, хто погодив документ), визначається причина збою в системі, перевіряється законність операцій, виявляються конкретні порушники.

Зазвичай Audit Trail фіксує наступну інформацію для кожного кроку:

– Хто? (визначається унікальний ідентифікатор користувача чи системи (логін, ID));

– Що? (визначається тип дії: перегляд, створення, видалення, редагування інформації);

– Коли? (визначається точна дата та час події);

– З чим? (визначається значення даних «до» та «після» (початкове та оновлене значення)).

Таким чином, Audit Trail дає можливість швидко виявити витік даних чи несанкціонований доступ, встановити злам системи, не дозволяє працівникам та

адміністраторам змінювати фінансово-господарські операції та важливі документи «заднім числом».

Сучасним методом перевірки комп'ютерних програм на предмет постійного й регулярного автоматичного контролю операцій та фінансових даних у режимі реального часу є безперервний аудит (Continuous Auditing). При його впровадженні здійснюється автоматичне збирання та аналіз даних під час здійснення бізнес-процесів, забезпечується швидке виявлення помилок, відхилень, підозрілих операцій, формуються миттєві сповіщення про ймовірні ризики.

Ключовими перевагами Continuous Auditing є зменшення ризиків шахрайства, контроль за надійністю фінансових звітів, забезпечення можливості щодо покращення внутрішніх правил на підприємстві, раціональне використання часу фахівців та їх можливість зосередити увагу на складних проблемах.

Узагальнено модель цифрової обліково-аналітичної системи підприємства можна представити наступним чином (рис. 4):

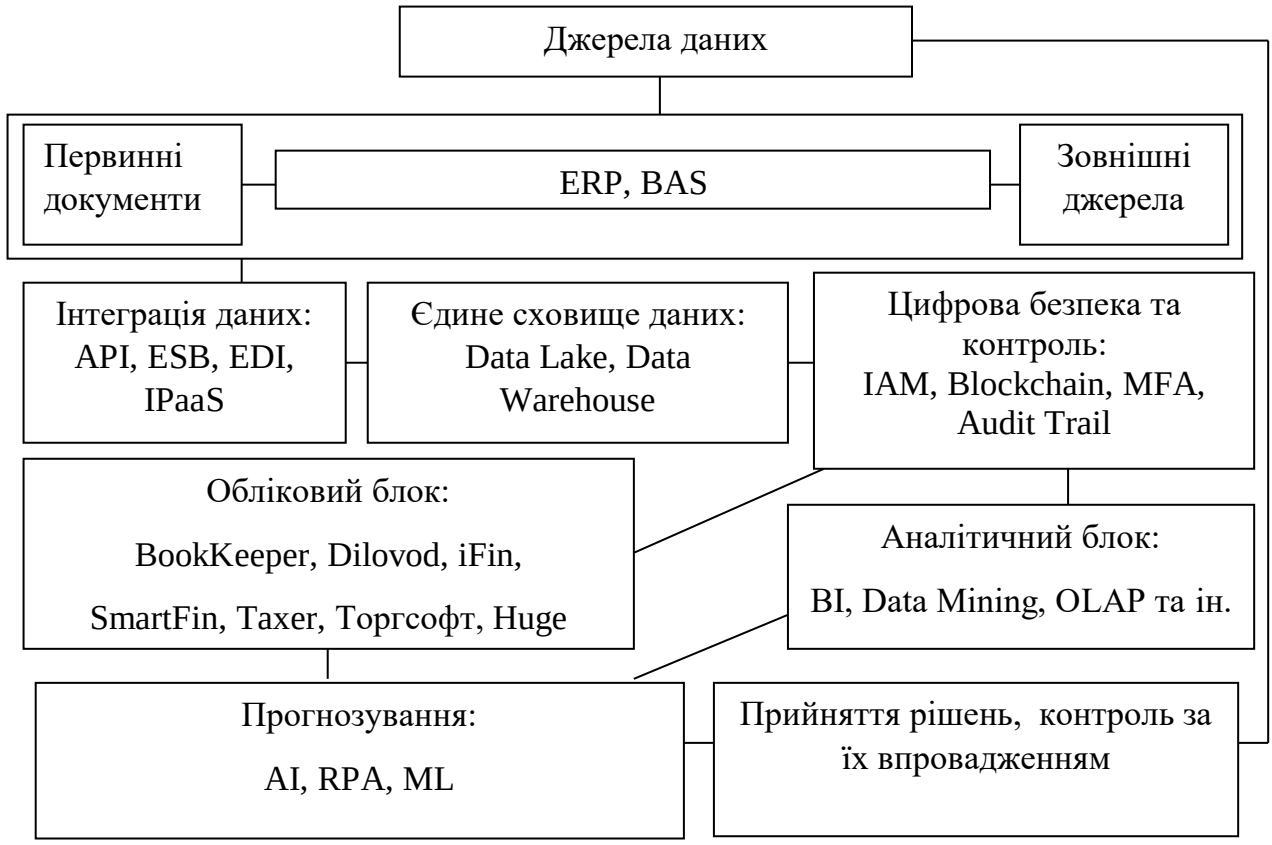


Рис. 4. Узагальнена модель цифрової обліково-аналітичної системи підприємства

*Джерело: сформовано автором*

Слід зазначити, що інструменти цифрової трансформації обліково-аналітичної системи підприємства доречно розглядати не як звичайний перелік технологій, а як ієрархічну систему (рис. 5).

Отже, у рамках цифрової трансформації обліково-аналітичної системи поєднуються: цифровізація даних; автоматизація процесів; інтеграція систем; аналітика та інтелектуалізація; цифровий контроль; управлінська адаптивність.

## 5.4. Система індикаторів ефективності цифрової трансформації обліково-аналітичної системи підприємства

Слід зазначити, що на сьогоднішній день не розроблено методику оцінювання цифрової трансформації обліково-аналітичної системи підприємства. Водночас, у науковій літературі можна побачити загальні підходи до оцінювання цифрової зрілості підприємства на основі використання моделей цифрової зрілості (Digital Maturity Models), рівня цифровізації інформаційних систем та бізнес-процесів.

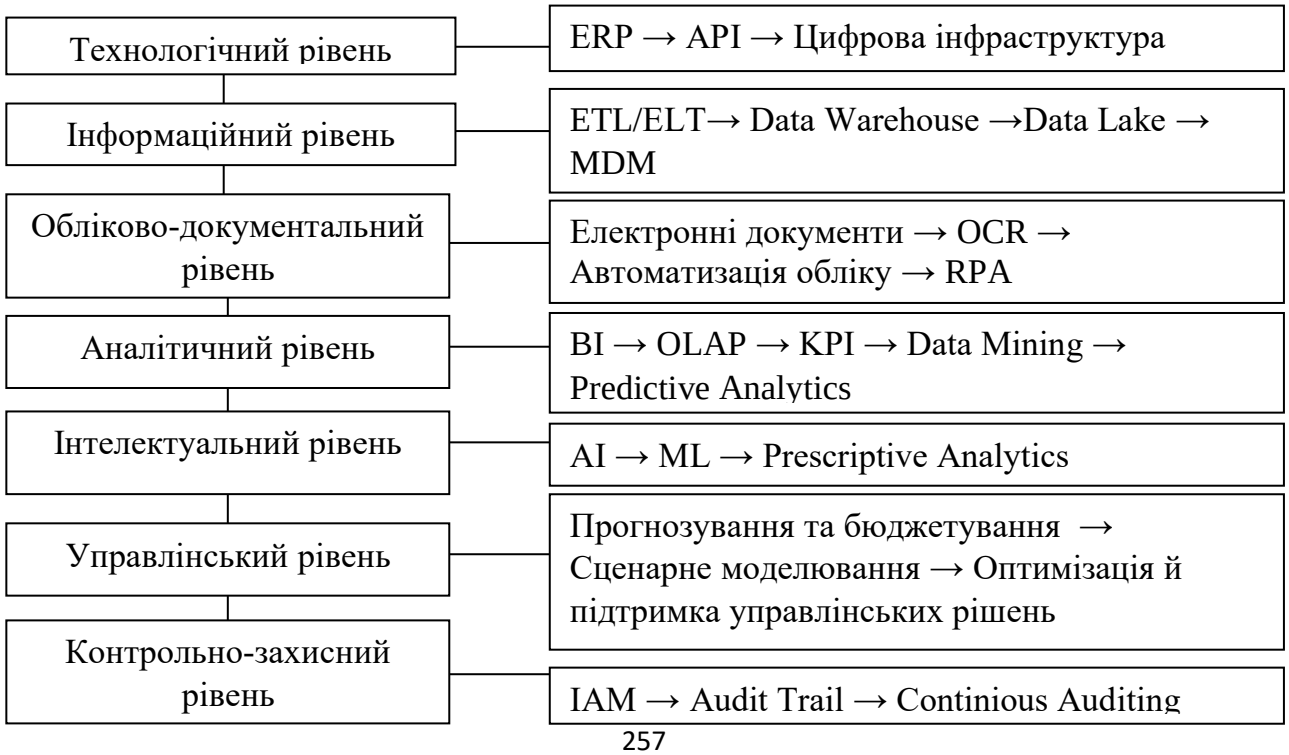


Рис. 5. Інструменти цифрової трансформації обліково-аналітичної системи підприємства як ієрархічна система

*Джерело: сформовано автором на підставі [3; 6; 7; 10; 11]*

Моделі цифрової зрілості (Digital Maturity Models) являють собою спеціальні структуровані рамки й інструменти, з використанням яких підприємство може оцінити рівень розвитку цифрових технологій та процесів, сформувати план подальшої цифрової трансформації [13].

Digital Maturity Models дають можливість оцінити підприємство за наступними важливими напрямами:

– стратегія (наскільки є інтегрованими цифрові цілі);

– культура (враховується готовність керівництва та персоналу до змін та впровадження інновацій);

– технології (рівень використання AI, сучасних IT-систем, хмарних рішень);

– операційні процеси (рівень їх гнучкості та автоматизації);

– дані (враховується якість збору інформації, її аналізу та використання при ухваленні рішень) [13].

У рамках Digital Maturity Models виокремлюють п’ять рівнів зрілості: від базового до «просунутого». Так, на початковому рівні (Traditional/Initial) переважають паперові та ручні процеси, а технології використовуються хаотично. На епізодичному рівні (Emerging) у різних підрозділах підприємства з’являються окремі цифрові інструменти, проте єдиної системи не налагоджено. На визначеному рівні (Defined) розробляється загальна стратегія цифровізації, впроваджуються базові платформи. На керованому рівні (Managed) процеси оптимізуються, а технології починають приносити вигоду. На досконалому рівні (Optimized/Digital Native) постійне оновлення та інновації закладені в основу розвитку підприємства [13].

Використання Digital Maturity Models дає можливість підприємству знайти слабкі місця у впровадженні технологій, створити поетапну «дорожню карту» розвитку та оцінити власний рівень цифрової зрілості на тлі конкурентів.

Для оцінювання цифрової трансформації обліково-аналітичної системи підприємства необхідно використовувати систему індикаторів, у рамках якої інтегруються показники, які відображають рівень цифровізації інформаційних технологій, бухгалтерського обліку, внутрішнього контролю та аудиту, процесу оподаткування, економічного аналізу, управління. При цьому пропонуємо виокремлювати наступні взаємопов'язані групи індикаторів з урахуванням їх основного призначення (рис. 6):

З метою оцінки ефективності процесу цифрової трансформації обліково-аналітичної системи підприємства доцільно використовувати наступні індикатори:

1. Інформаційна інтеграція (оцінка взаємодії інформаційних систем):

– кількість інтегрованих інформаційних систем;
– частка централізованих баз даних;
– ступінь інтеграції ERP, CRM;
– рівень використання хмарних технологій;
– рівень інтеграції з системами електронного документообігу, державними цифровими сервісами;




Рис. 6. Групи індикаторів оцінки ефективності процесу цифрової трансформації обліково-аналітичної системи підприємства та їх основне призначення

*Джерело: сформовано автором*

2. Інформаційна безпека (оцінка рівня захищеності інформації):

– частота оновлення системи безпеки;

– рівень кіберзахисту та шифрування даних;

– відповідність інформаційної безпеки підприємства вимогам міжнародних стандартів;

– контроль доступу до інформації, використання багатофакторної автентифікації;

– частота оновлення систем безпеки;

– забезпечення резервного копіювання;

– прояв інцидентів щодо інформаційної безпеки;

3. Організаційна цифрова зрілість (оцінка кадрового та організаційного забезпечення):

– наявність цифрової стратегії підприємства;

– рівень використання цифрових сервісів та підтримки цифрової трансформації керівництвом підприємства;

– рівень цифрової культури та цифрових компетентностей персоналу;

– частка працівників, які пройшли цифрове навчання;

4. Цифровізація облікових процесів (оцінка рівня автоматизації обліку):

– рівень використання ERP, BAS, SAP;

– частка інтегрованих бізнес-процесів;

– частка автоматизованих бухгалтерських операцій;

– рівень автоматизації первинного обліку та середній час обробки первинного документа;

5. Цифровізація внутрішнього контролю та аудиту (оцінка автоматизації контрольно-аудиторських процедур):

– загальний рівень цифровізації внутрішнього контролю, внутрішнього аудиту;

– частка виконаних автоматизовано процедур контролю, аудиторських процедур;

– автоматизоване виявлення аномалій;

– використання Continious Auditing, Continious Monitoring, RPA;

6. Цифровізація процесу оподаткування (оцінка цифрового податкового планування та прогнозування):

– використання електронного кабінету платника, інтеграція з електронними сервісами фіскальних органів;

– рівень автоматизації процесу податкового прогнозування та планування, оцінки податкових ризиків;

– використання TaxTech-рішень;

7. Аналітичний потенціал (оцінка можливостей проведення аналізу та підтримки системи прийняття рішень):

– використання BI-систем, Big Data, Data Warehouse, AI, прогнозної аналітики;

– кількість автоматично сформованих аналітичних звітів;

– частота оновлення Dashboards;

– кількість KPI, розрахованих автоматично;

8. Економічна ефективність цифрової трансформації (оцінка отриманих економічних результатів діяльності та наслідків рішень):

– скорочення часу на ведення обліку та формування звітності;

– підвищення рівня продуктивності праці бухгалтерів;

– скорочення часу на прийняття управлінських рішень;

– рівень окупності цифрових інвестицій (ROI).

Запропоновані індикатори оцінки ефективності процесу цифрової трансформації обліково-аналітичної системи підприємства можна згрупувати за наступними напрямами оцінювання:

1. Організаційний (цифрова культура, цифрові компетентності);

2. Технологічний (цифрові платформи, хмарні технології, ERP, AI);

3. Функціональний (цифровізація бухгалтерського обліку, внутрішнього контролю та аудиту, податкового адміністрування, аналізу);

4. Результативний (якість інформації, економічний ефект, оперативність прийняття управлінських рішень).

Представлена сукупність індикаторів оцінки ефективності процесу цифрової трансформації обліково-аналітичної системи підприємства має ряд переваг, оскільки вона є орієнтованою передусім на обліково-аналітичну

систему, а не на підприємство загалом. У ній інтегруються ключові функціональні складові (бухгалтерський облік, внутрішній контроль та аудит, податкове адміністрування, економічний аналіз), поєднуються організаційні, технологічні, функціональні й результативні характеристики, що дає змогу комплексно оцінити рівень цифрової трансформації, формуючи основу для здійснення інтегральної оцінки процесу цифрової трансформації обліково-аналітичної системи підприємства. Такий підхід забезпечує можливість його використання при здійсненні моніторингу динаміки процесу цифровізації й обґрунтування ефективних рішень стосовно подальшого розвитку цифрової інфраструктури.

***Висновки до Розділу 5***

Узагальнення теоретичних підходів до сутності обліково-аналітичної системи підприємства дозволяє розглядати її як комплексний механізм формування інформаційного забезпечення управління, що поєднує облік, контроль та економічний аналіз. Її функціонування передбачає послідовний збір і систематизацію даних, перевірку їх повноти та достовірності, подальшу аналітичну обробку й використання отриманої інформації для обґрунтування управлінських рішень. В умовах цифровізації традиційна модель такої системи поступово трансформується у складне інтегроване інформаційне середовище, здатне забезпечувати не лише реєстрацію господарських операцій, а й прогнозування, контроль, оцінювання ризиків та підтримку управлінських рішень.

Встановлено, що цифрову обліково-аналітичну систему підприємства доцільно розглядати як інтегровану інтелектуальну платформу, у межах якої взаємопов’язані: цифровий документообіг та цифровий облік; цифровий контроль та аудит; аналітична платформа, інтелектуальна аналітика; податковий модуль; інформаційна інфраструктура, управлінська підтримка, інформаційна безпека. Її формування ґрунтується на принципах інтегрованості, єдності

інформаційного простору, автоматизації бізнес-процесів, цифровізації первинної інформації, аналітичності, безперервності обробки даних, прогнозної орієнтації, масштабованості, ризик-орієнтованості, інтероперабельності, інформаційної безпеки та управлінської спрямованості.

Обґрунтовано, що функціонування сучасної цифрової обліково-аналітичної системи забезпечується комплексним використанням ERP-систем, хмарних технологій, Big Data, Business Intelligence, Artificial Intelligence, Machine Learning, RPA, Blockchain, IoT, Process Mining, Digital Twins, API-інтеграції, електронного документообігу, XBRL та прогнозної аналітики. Застосування зазначених інструментів створює технологічну основу для переходу від розрізненого опрацювання інформації до безперервного цифрового циклу її формування, інтеграції, аналізу, контролю та використання у процесі управління підприємством.

Цифрова трансформація обліково-аналітичної системи не може бути зведена виключно до автоматизації окремих бухгалтерських операцій. Її зміст полягає у комплексній перебудові процесів формування, зберігання, передавання, обробки та використання інформації. Відповідно, інструментарій такої трансформації охоплює автоматизацію облікових процесів, інтеграцію інформаційних систем, розвиток хмарної інфраструктури, електронний документообіг, управління великими масивами даних, бізнес-аналітику, інтелектуальну автоматизацію, цифровий контроль та забезпечення інформаційної безпеки.

Важливим результатом цифрової трансформації є формування єдиного інформаційного середовища підприємства, у межах якого інформаційні потоки інтегруються за принципом взаємозв’язку CRM, ERP, бухгалтерського і податкового обліку, складських систем, банківських сервісів та BI-платформ. Така інтеграція усуває дублювання інформації, скорочує обсяги ручного введення даних, підвищує оперативність їх обробки та створює умови для

переходу від традиційної моделі «господарська операція – документ – звітність» до моделі, орієнтованої на автоматичне формування даних, їх накопичення в інтегрованій базі, аналітичну обробку та безпосередню підтримку управлінських рішень.

Встановлено, що цифровізація суттєво змінює аналітичну та контрольну складові обліково-аналітичної системи. Використання BI, Data Mining, OLAP, Predictive та Prescriptive Analytics забезпечує перехід від статичної звітності до інтерактивної аналітики, прогнозування та моделювання варіантів розвитку підприємства. Одночасно впровадження IAM, MFA, Audit Trail, Blockchain, Continuous Auditing та інших інструментів цифрового контролю посилює можливості щодо захисту інформації, фіксації дій користувачів, своєчасного виявлення помилок, аномалій, шахрайських операцій та інших ризиків.

Доведено необхідність оцінювання цифрової трансформації обліково-аналітичної системи не лише за фактом упровадження окремих технологічних рішень, а на основі системи взаємопов’язаних індикаторів. Запропонований підхід охоплює інформаційну інтеграцію, інформаційну безпеку, організаційну цифрову зрілість, цифровізацію облікових процесів, внутрішнього контролю та аудиту, процесу оподаткування, аналітичний потенціал і економічну ефективність цифрової трансформації. Таке структурування забезпечує комплексне оцінювання організаційних, технологічних, функціональних та результативних характеристик цифровізації.

Таким чином, цифрова трансформація обліково-аналітичної системи підприємства є комплексним процесом переходу від переважно реєстраційно-облікової моделі до інтегрованої, автоматизованої та інтелектуалізованої системи інформаційного забезпечення управління. Її результативність визначається не кількістю впроваджених цифрових технологій, а рівнем їх інтеграції в єдину систему, здатну забезпечувати достовірність і безперервність інформаційних потоків, підвищувати якість аналітики та контролю,

підтримувати прогнозування й оперативне прийняття управлінських рішень. Запропонована система індикаторів створює основу для комплексного моніторингу цього процесу та оцінювання його впливу на ефективність функціонування обліково-аналітичної системи підприємства.

## Список використаних джерел

1. Василішин С. І. Обліково-аналітичне забезпечення в системі ризиків та загроз економічної безпеки аграрних підприємств України : монографія. Харків. нац. аграр. ун-т ім. В.В. Докучаєва. Харків : ТОВ «Друкарня Мадрид», 2020. 419 с. URL: https://repo.btu.kharkov.ua//handle/123456789/9849

2. Кононенко Л. В., Ніколаєва С. П. Трансформація системи обліково-аналітичного забезпечення як складова управління підприємством в умовах сталого розвитку та діджиталізації суспільства. *Економічний простір*. 2022. № 177. С. 69-75. URL: https://doi.org/10.32782/2224-6282/177-12

3. Кудренко Н. В. Обліково-аналітична система як інструмент забезпечення комплаєнсу підприємств. *Науковий вісник Ужгородського університету. Серія «Економіка»*. 2026. № 1(67). С. 128-135. URL: https://doi.org/10.24144/2409-6857.2026.1(67).128-135

4. Лега О. В., Канцедал Н. А., Прийдак Т. Б. Цифровізація обліку і податкового адміністрування : трансформація ризиків та інструментів контролю в умовах євроінтеграції. *Економіка та суспільство*. 2026. Вип. 86. URL: https://doi.org/10.32782/2524-0072/D2026-86-237

5. Лень В. С. Обліково-аналітична система підприємства: обґрунтування визначення, модель. *Проблеми і перспективи економіки та управління*. 2016. № 1(5). С. 281-290. URL: https://ppeu.stu.cn.ua/article/view/79179/74937

6. Лисенко А. М. Цифровізація обліково-аналітичних процесів як основа раціонального управління підприємством. Цифрова еволюція сучасного бізнесу : виклики, тенденції та перспективи в умовах цифрової економіки

України : кол. моногр. / за ред. А. В. Череп, І. М. Дашко, Ю. О. Огренич, О. Г. Череп. Рига : Baltija Publishing, 2025. Розд. 3.3. С. 291-340. URL: https://dspace.kntu.kr.ua/handle/123456789/16961

7. Скрипник С. В. Цифрові інструменти обліку та аудиту : нові можливості для сучасного підприємства. *Таврійський науковий вісник. Серія : Економіка*. 2026. Вип. 27. С. 94-104. URL: https://doi.org/10.32782/2708-0366/2026.27.10

8. Сьомочкіна Т. І., Грищук Г. В. Особливості обліково-аналітичного забезпечення управління економічним потенціалом підприємств. Економіка та суспільство. 2025. Вип. 81. URL: https://doi.org/10.32782/2524-0072/2025-81-158

9. Якіменко Л. Найкращі програми бухгалтерського обліку України у 2025 році. Центр бухгалтерського аутсорсингу. URL: https://cba.net.ua/najkraschi-prohramy-bukhhalterskoho-obliku-ukrajiny-u-2025-rotsi/.

10. Яловега Л. В., Лега О. В., Прийдак Т. Б. Обліково-аналітична система суб'єктів господарювання : теоретичні аспекти, складові та методологічне забезпечення. *Причорноморські економічні студії*. 2022. Вип. 78. С. 130-135. DOI: https://doi.org/10.32782/bses.78-20

11. Янковська К. Цифрова трансформація обліку та аудиту на основі сучасних інформаційних систем. *Вісник Львівського національного екологічного університету. Серія «Економіка АІК»*. 2025. № 32. С. 50-54. URL: https://doi.org/10.31734/economics2025.32.050

12. Яремко І. Й. Обліково-аналітичне забезпечення як інструментарій управління економічним розвитком підприємства. *Проблеми сучасних трансформацій. Серія : економіка та управління*. 2022. № 6. URL: https://doi.org/10.54929/2786-5738-2022-6-09-02

13. Digital Maturity Models Explained (2025). BMC Helix. Available at: https://blogs.helixops.ai/digital-maturity-models/

# РОЗДІЛ 6
# ЦИФРОВІЗАЦІЯ ДЕРЖАВНОГО УПРАВЛІННЯ ЯК МЕХАНІЗМ ЗАПОБІГАННЯ ВИДАННЮ ТА ВИКОНАННЮ ЗЛОЧИННИХ НАКАЗІВ

Автор: **Ланкевич Андрій Зіновійович,** *голова Львівського окружного адміністративного суду, кандидат юридичних наук, доцент, докторант кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет, https://orcid.org/0009-0005-4443-5684*

## 6.1. Владний наказ у цифровому середовищі як форма публічно-владного волевиявлення

Цифрова трансформація державного управління поступово змінює не лише технічні засоби діяльності органів публічної влади, а й саму організацію процесу формування владного рішення. Електронний документообіг, цифрова ідентифікація, міжвідомча інформаційна взаємодія, автоматизована реєстрація управлінських операцій і використання електронних реєстрів створюють можливість перевести значну частину життєвого циклу владного рішення у цифрове середовище. Внаслідок цього технологічного значення набуває вже не лише кінцевий документ, а й інформація про те, ким, коли, на якій правовій підставі та після проходження яких процедур він був сформований.

Для проблематики злочинних наказів такий напрям цифровізації має самостійне значення. Конституційна заборона виконання явно злочинних наказів і розпоряджень визначає матеріальну межу обов'язковості владної волі. Однак ефективність відповідної конституційної гарантії залежить також від того, наскільки можливо встановити походження конкретного владного рішення, відтворити процедуру його формування, визначити осіб, причетних до підготовки й погодження, та перевірити, чи не був його зміст змінений у процесі доведення до виконавця. У цій площині проблема переміщується від питання про

правову кваліфікацію наказу до питання про належну організацію процедури його формування та обігу [1].

Саме для позначення такого аспекту доцільно використовувати поняття «цифровий супровід владного наказу». Під ним пропонується розуміти організаційно-правове забезпечення основних етапів підготовки, погодження, видання, доведення, зміни та завершення реалізації владного наказу за допомогою цифрових засобів, які дають змогу встановити суб'єкта відповідної дії, її час, правову підставу, зміст та місце у загальній послідовності управлінського процесу. Втім, запропоноване поняття не зводиться до електронного документообігу. Електронний документ є лише одним із його елементів. Цифровий супровід охоплює також відомості про підготовку проєкту рішення, визначення його правової підстави, проходження погоджень, використані інформаційні ресурси, зміни тексту, доведення наказу до адресата, застосування виняткової процедури та інші юридично значущі операції. Йдеться, таким чином, не стільки про переведення паперового наказу в електронну форму, скільки про формування цифрового середовища, у якому весь юридично значущий шлях владного рішення набуває визначеності та доступності для належної перевірки. У такому розумінні цифровізація виконує превентивну функцію ще до виникнення питання про відповідальність за протиправний наказ.

Правове підґрунтя для розвитку відповідної моделі в Україні вже частково сформоване. Закон України «Про електронні документи та електронний документообіг» визначає електронний документообіг як сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів із забезпеченням перевірки їх цілісності та, за необхідності, підтвердження факту одержання [2]. До того ж, законодавство у сфері електронної ідентифікації та електронних довірчих послуг забезпечує правові передумови для достовірного встановлення підписувача та перевірки цілісності електронного документа [3].

Істотне значення має також постанова Кабінету Міністрів України від 17 січня 2018 року № 55, якою врегульовано документування управлінської діяльності в електронній формі та організацію електронного міжвідомчого обміну. Вона демонструє поступовий перехід від розуміння електронного документа як аналога паперового до побудови цілісного електронного процесу роботи з управлінською інформацією [4].

Водночас для запобігання протиправному використанню владного наказу недостатньо самого факту існування електронного документа. Електронна форма не робить рішення правомірним. Цифровий підпис посвідчує визначені юридично значущі характеристики документа, однак не підтверджує законності його змісту. Так само електронна реєстрація не виключає можливості перевищення повноважень, обходу процедури або використання недостовірних даних. Тому превентивний потенціал цифровізації виникає лише тоді, коли цифрове середовище відображає не одну кінцеву дію – підписання наказу, – а дозволяє встановити його походження.

У межах цього дослідження під цифровим походженням владного наказу пропонується розуміти встановлювану послідовність юридично значущих дій і відомостей, на основі яких сформовано остаточне владне рішення. Йдеться про можливість відповісти не лише на питання «хто підписав наказ?», а й на питання: хто його ініціював; яка норма права була зазначена як підстава; які фактичні дані використовувалися; хто готував проєкт; які погодження були обов’язковими; хто і коли їх надав; чи змінювався текст після погодження; хто вніс відповідні зміни; якою була остаточна версія, направлена адресатові. Саме відсутність такого зв’язку між окремими етапами формування рішення створює можливість для розмивання відповідальності. Формально наказ може бути підписаний однією посадовою особою, тоді як його фактичний зміст сформований іншими суб’єктами. І навпаки, особа, яка брала участь лише у технічному опрацюванні

документа, не повинна автоматично ототожнюватися з особою, яка визначала його зміст. Цифровий супровід дозволяє диференціювати ці ролі.

У цьому аспекті доцільно запровадити поняття «цифрового паспорта владного наказу», що являє собою структурований набір метаданих, який автоматично формується інформаційною системою протягом усього проходження управлінського рішення. Такий цифровий паспорт може містити відомості про ініціатора рішення; орган і структурний підрозділ, у межах якого воно формується; вид владного акта; зазначену нормативну підставу; автора проєкту; учасників обов'язкового погодження; дату і час відповідних дій; версії документа; суб'єктів внесення змін; факт остаточного підписання; адресата; дату та спосіб доведення; використання спеціальної або виняткової процедури; завершення чи припинення дії наказу. Принципове значення має те, що цифровий паспорт не повинен містити оцінки «законний», «незаконний» чи «злочинний». Його функція є іншою – сформувати достатню інформаційну основу, яка уможливлює подальшу юридичну оцінку.

Запропонований механізм дозволяє уникнути небезпечної підміни права технологією, позаяк інформаційна система не вирішує питання про юридичну кваліфікацію владного рішення, а забезпечує збереження даних, без яких така кваліфікація може бути ускладненою або неможливою.

Відповідно, першою самостійною функцією цифрового супроводу наказу є *функція відтворюваності управлінського рішення*. Після завершення відповідної процедури уповноважений контрольний суб'єкт повинен мати можливість відтворити основні етапи формування наказу без необхідності покладатися винятково на пам'ять, пояснення або добросовісність його учасників.

Другою функцією є *збереження цілісності управлінської історії*. Зміна тексту наказу, його правової підстави або інших юридично значущих параметрів повинна залишати окремий інформаційний слід. Технічно допустиме

редагування документа не повинно означати можливості непомітного переписування попередньої версії.

Третьою є *функція процедурної дисципліни*. Усвідомлення того, що пропуск обов'язкової стадії, зміна документа після погодження або використання виняткового порядку залишаться зафіксованими, об'єктивно ускладнює прихований обхід установленої процедури.

Четвертою є *контрольна функція*, оскільки належно сформовані цифрові дані можуть використовуватися під час внутрішнього, адміністративного, парламентського, судового або іншого передбаченого законом контролю.

Водночас цифровий супровід не повинен перетворюватися на тотальне документування кожної внутрішньої управлінської комунікації. Така модель була б непропорційною, створювала б надмірне навантаження на державний апарат, збільшувала обсяг інформації з обмеженим доступом і могла б перешкоджати оперативності управління.

Отже, визначальною має бути не максимальна кількість цифрових відомостей, а їх юридична значущість. Фіксувати доцільно ті операції, які можуть впливати на зміст, правову підставу, авторство, процедуру прийняття або подальшу перевірку владного рішення. Останнє дозволяє сформулювати основний принцип цифрового супроводу владного наказу, за якого, чим істотнішими можуть бути юридичні наслідки рішення, тим вищими мають бути вимоги до фіксації його походження та проходження процедури.

Відповідний принцип створює також основу для диференційованої цифровізації державного управління. Рутинне внутрішньоорганізаційне доручення не потребує такого самого рівня фіксації, як рішення про застосування примусових заходів, обмеження прав, використання значних публічних ресурсів чи реалізацію повноважень у сфері безпеки. У цьому аспекті цифровізація перестає бути самоціллю. Її завданням стає не максимальне переведення владної діяльності у цифровий формат, а створення пропорційної системи процедурних

гарантій, здатної зменшувати можливість прихованого формування та реалізації протиправного владного рішення.

### 6.2. Механізми фіксації походження, руху та зміни владного наказу

Владний наказ слід розглядати не як ізольований документ, що виникає у момент його підписання, а як результат певної послідовності управлінських дій. До остаточного формування рішення можуть передувати ініціювання питання, збір інформації, підготовка проєкту, правова експертиза, міжвідомче погодження, перевірка фінансових або безпекових наслідків та інші процедури. Разом із тим, з правової точки зору значення має не кожна технічна операція, а ті дії, які здатні вплинути на зміст рішення або засвідчують проходження обов'язкової стадії його прийняття.

У паперовому середовищі зв'язок між такими етапами нерідко має фрагментарний характер. Частина документів може зберігатися в різних структурних підрозділах, окремі погодження оформлюватися на різних носіях, а зміст проміжних версій документа – не мати самостійної фіксації. Цифрова система здатна об'єднати такі відомості у єдиний логічний ланцюг. Важливо, щоб цей ланцюг не залежав від ручного створення додаткових звітів після завершення процедури. Чим більша частина інформації формується автоматично в момент відповідної дії, тим нижчим є ризик її наступного спотворення.

До прикладу, факт подання проєкту наказу на погодження має автоматично пов'язуватися з конкретною версією документа. Якщо після отримання погодження до тексту внесено зміни, система повинна відображати, чи стосувалося попереднє погодження остаточної редакції. В іншому разі формальна наявність електронної позначки про погодження може створювати хибне враження дотримання процедури.

Саме контроль версій є однією з ключових переваг цифрового середовища. Він дозволяє встановити не лише факт зміни документа, а й момент її внесення та суб'єкта відповідної дії. Для правової оцінки владного наказу це може мати

принципове значення, якщо юридично проблемне положення з'явилося вже після проходження правової експертизи або погодження. Не менш значущою є достовірна ідентифікація учасників. Законодавство про електронні документи та електронну ідентифікацію створює нормативне підґрунтя для встановлення особи, яка підписала документ або виконала іншу юридично значущу дію [2; 3]. Водночас належна ідентифікація повинна охоплювати не лише кінцеве підписання.

Так, для складних управлінських процесів важливо розрізняти принаймні ініціювання, підготовку, погодження, санкціонування, доведення та виконання рішення. Автоматичне віднесення всієї відповідальності до особи, електронний підпис якої стоїть під остаточним документом, так само спрощує реальну картину, як і посилання на абстрактну «колективність» рішення.

Цифрова система має забезпечувати не колективізацію, а розмежування функціональної участі. Особливе значення у цьому процесі мають публічні електронні реєстри. Закон України «Про публічні електронні реєстри» формує загальні правові та організаційні засади створення, функціонування та використання відповідних інформаційних ресурсів. Їх використання у процесі формування владного наказу дозволяє, з одного боку, отримувати необхідні відомості без повторного витребування документів, а з іншого – точніше встановлювати інформаційну основу прийнятого рішення [5].

У перспективі до цифрового паспорта наказу доцільно включати не самі масиви даних, отримані з інших державних ресурсів, а відомості про те, яке джерело було використане та в який момент, що дозволятиме перевірити, на якій інформаційній основі діяла посадова особа, не створюючи при цьому надмірного дублювання персональних або інших захищених даних.

Важливою інфраструктурою міжвідомчої взаємодії є система «Трембіта», нормативне регулювання якої передбачає організацію електронної інформаційної взаємодії між відповідними ресурсами [6]. Значення такого

механізму для цифрового супроводу владних рішень полягає не лише у швидкості передавання інформації. Принципово важливим є те, що юридично значуща взаємодія між інформаційними ресурсами може відбуватися у формалізованому та контрольованому цифровому середовищі.

Водночас інтеграція реєстрів створює новий ризик, де владне рішення може формуватися на підставі значної кількості відомостей, походження яких без спеціальної фіксації буде складно відтворити. Тому у складних процедурах доцільно забезпечувати можливість встановити не лише результат інформаційного запиту, а й ресурс, до якого він був спрямований, юридичну підставу відповідної взаємодії та час отримання даних. Засвідчений підхід не означає, що всі відомості про інформаційну взаємодію повинні бути доступними кожному користувачеві. Режим доступу має визначатися характером інформації та повноваженнями відповідного суб'єкта. Однак наявність обмежень доступу не повинна означати відсутність можливості подальшої перевірки уповноваженим органом.

В той же час, окремою проблемою являється зміна вже сформованого наказу. Управлінська діяльність об'єктивно потребує можливості виправлення помилок, уточнення формулювань або адаптації рішення до нових обставин. Тому технічна неможливість будь-якого редагування була б недоцільною. Натомість доцільним є принцип видимості юридично значущої зміни. Якщо після певного етапу процедури змінюється положення, здатне вплинути на права, обов'язки, адресата, спосіб виконання, обсяг повноважень або інші істотні характеристики наказу, система повинна забезпечувати можливість встановити факт такої зміни, її автора та час. Звісно, не кожне виправлення технічної помилки потребує повторного проходження всієї процедури. Але система повинна розрізняти суто технічне редагування та зміну юридично значущого змісту. Критерії такого розмежування мають визначатися нормативно або організаційно залежно від виду владних актів.

Звідси випливає ще один перспективний напрям – зв'язування погодження з версією документа. Електронне погодження повинно підтверджувати конкретний текст, а не абстрактну назву документа. Якщо після погодження юридично значущі положення змінюються, попередня позначка не повинна автоматично переноситися на нову редакцію. Подібна вимога здатна запобігти ситуації, коли особа формально посилається на погодження юридичної служби, хоча остаточний зміст наказу істотно відрізняється від того, який перевірявся. Саме у цьому проявляється принципова відмінність цифрового супроводу від звичайного електронного архівування. Архів зберігає результат. Цифровий супровід зберігає зв'язки між юридично значущими діями.

Для систем із підвищеним рівнем ризику доцільним є забезпечення захисту такого ланцюга від прихованої модифікації. Конкретна технологія може відрізнятися залежно від інформаційної системи. Використання блокчейну чи іншої конкретної технології не є обов'язковою умовою. Юридично важливим є функціональний результат, за якого зміна або видалення критично важливого запису не повинні відбуватися без формування нового контрольованого запису про відповідну операцію.

Необхідно також розмежовувати право формувати владне рішення та право адмініструвати інформаційну систему, в якій зберігається історія такого рішення. Якщо посадова особа або підрозділ, зацікавлені у приховуванні певної управлінської дії, можуть одноосібно видалити або змінити відповідні журнали подій, превентивне значення цифровізації істотно зменшується. Тому для критично важливих систем доцільно застосовувати принцип функціонального розмежування, де суб'єкти, які формують, погоджують і виконують владне рішення, не повинні мати неконтрольованої можливості змінювати історію системи.

Водночас захищеність цифрового сліду повинна поєднуватися з вимогами інформаційної безпеки та приватності. Накопичення значного обсягу службової

інформації само по собі створює ризики. Законодавство України про захист інформації в інформаційно-комунікаційних системах та персональних даних вимагає належного режиму доступу, визначеності мети обробки та забезпечення захисту відповідних відомостей [7; 8].

Отже, повнота цифрового супроводу не повинна ототожнюватися з необмеженим накопиченням даних. Належним є такий обсяг інформації, який дозволяє встановити юридично значущі обставини формування рішення, але не створює надмірного цифрового спостереження за діяльністю посадових осіб. У цьому контексті доцільно сформулювати принцип необхідної достатності цифрового сліду. Він означає, що обсяг зафіксованої інформації повинен бути достатнім для відтворення юридично значущих етапів рішення, але не перевищувати того, що об'єктивно необхідно для забезпечення законності, контролю та підзвітності.

### 6.3. Цифрові процедурні запобіжники під час формування владного наказу

Необхідно зауважити, що цифровий супровід владного наказу не повинен обмежуватися фіксацією того, що вже відбулося. Значно більший превентивний потенціал має використання цифрового середовища для недопущення очевидних процедурних дефектів ще на стадії підготовки рішення. При цьому принциповим є розмежування оцінки змістовної правомірності наказу і перевірки дотримання встановленої процедури. Питання про те, чи є конкретне розпорядження злочинним, може вимагати складної оцінки фактичних обставин, норм права, характеру наслідків та інших факторів. Цифрова система не повинна перебирати на себе таку юридичну кваліфікацію. Натомість багато процедурних параметрів можуть бути достатньо чітко формалізовані. Саме на них доцільно зосередити цифрові запобіжники.

Перший напрям – перевірка повноваження на здійснення конкретної управлінської дії. Інформаційна система може співвідносити роль користувача з

типом документа або процедурною дією, яку він намагається здійснити. Йдеться не про встановлення законності рішення в цілому, а про недопущення елементарної ситуації, коли користувач намагається виконати дію, якою його службова роль очевидно не охоплюється. Відповідний механізм уже широко використовується на технічному рівні у вигляді розмежування прав доступу. Однак у правовій площині він може бути розвинений у напрямі зв'язку між цифровою роллю користувача і нормативно визначеною компетенцією. Інформаційна система не повинна самостійно формувати компетенцію органу або посадової особи. Навпаки, цифрові налаштування мають відображати повноваження, визначені законом та іншими належними правовими актами. Зміна таких налаштувань також повинна бути контрольованою і документованою.

Другий напрям – контроль обов'язкових елементів процедури. Якщо нормативно встановлено, що певний вид рішення потребує правового висновку, погодження, мотивування, зазначення строку або іншої обов'язкової передумови, система може не дозволяти завершити стандартну процедуру без фіксації відповідного елемента. Важливо, що такий цифровий бар'єр не визначає зміст правового висновку і не гарантує його правильність. Він лише не дозволяє непомітно пропустити передбачену процедуру.

Третій напрям – зв'язок рішення з нормативною підставою. Для категорій владних актів, здатних істотно впливати на права особи або публічні інтереси, електронна форма може вимагати зазначення норми чи іншої належної юридичної підстави прийняття рішення. Сам факт зазначення норми, безумовно, не робить наказ законним. Однак така вимога дисциплінує процес формування рішення і значно полегшує наступну перевірку того, чи відповідає зазначена підстава реальному змісту владного повноваження.

Четвертий напрям – контроль послідовності юридично значущих дій. Якщо погодження має передувати підписанню, система не повинна дозволяти

створювати видимість дотримання процедури шляхом внесення погодження вже після прийняття рішення. Відомості про час відповідних операцій мають зберігатися автоматично.

П’ятий напрям – контроль актуальності погоджень після зміни документа. Якщо до рішення після правової або іншої обов’язкової перевірки внесено істотні зміни, система має сигналізувати про необхідність повторного погодження у тих випадках, коли це передбачено процедурою.

Такі цифрові механізми можна визначити як процедурні запобіжники. Їх мета полягає не в автоматичному підтвердженні законності наказу, а в зменшенні можливості прихованого обходу формалізованих вимог до його прийняття. Особливо важливо не створити зворотної презумпції, за якою успішне проходження цифрової перевірки сприйматиметься як підтвердження правомірності рішення. Зелена позначка інформаційної системи може означати лише те, що виконано передбачені нею формальні умови. Тому будь-яка цифрова система державного управління повинна чітко розмежовувати технічну допустимість операції та юридичну правомірність рішення.

Технічна можливість підписати документ не означає наявності у посадової особи належної компетенції, якщо цифрові права доступу налаштовані помилково. Так само технічне блокування операції не повинно автоматично означати її юридичну забороненість. Ця відмінність має принципове значення, оскільки цифровізація здатна створювати ілюзію об’єктивності, користувач може сприймати результат роботи системи як більш авторитетний лише через його технологічну форму Саме тому процедурні запобіжники повинні бути правово пояснюваними. Якщо система блокує стандартне завершення певної дії, користувач повинен бачити, яка саме процедурна вимога не виконана. Формулювання на кшталт «операція неможлива» без зазначення зрозумілої причини є недостатнім у сфері публічного управління.

Так, Закон України «Про адміністративну процедуру» має важливе значення для загального розуміння цифровізації владних процедур, оскільки передбачає можливість автоматизованого розгляду відповідних справ у встановлених законом випадках, водночас зберігаючи відповідальність за результат за адміністративним органом [9]. Це підтверджує ширший принцип, за якого використання цифрової системи не трансформує технологію у самостійного носія публічної компетенції.

Для розроблення цифрових процедурних запобіжників доцільним є ризик-орієнтований підхід. Не всі накази потребують однакового рівня цифрового контролю. Рутинні внутрішньоорганізаційні рішення можуть проходити мінімальний набір перевірок, як-от: належність користувача до відповідного органу, його повноваження на підписання конкретного виду документа та наявність обов'язкових реквізитів. Для рішень, які можуть істотно впливати на права людини, передбачати примусові заходи, використання значних бюджетних ресурсів або інші суттєві юридичні наслідки, доцільним може бути розширений набір процедурних вимог, де зосереджуються обов'язкове зазначення правової підстави, підтвердження проходження визначених погоджень, збереження джерел істотних вихідних даних та фіксація використання спеціальної процедури.

Таке розмежування відповідає загальній логіці сучасного цифрового регулювання, за якої інтенсивність гарантій пов'язується з рівнем потенційного ризику. Подібний підхід простежується і в Регламенті Європейського Союзу 2024/1689 про штучний інтелект, який для високоризикових систем встановлює підвищені вимоги до документування та ведення журналів подій [10]. Рамкова конвенція Ради Європи про штучний інтелект також пов'язує використання відповідних технологій із вимогами прозорості, підзвітності, належного документування та управління ризиками [11].

Для цифрового супроводу наказу ці підходи важливі не через необхідність обов'язкового використання штучного інтелекту. Навпаки, значна частина запропонованих запобіжників може бути реалізована звичайними інформаційними системами на основі чітко визначених процедурних правил. І це є принциповою перевагою запропонованої моделі. Для запобігання процедурному обходу не потрібно створювати алгоритм, який «розуміє» зміст наказу. Достатньо, щоб цифрове середовище коректно відтворювало передбачену законом процедуру і не дозволяло приховати відхилення від неї.

У цьому контексті доцільним є принцип вбудованої процедурної законності у цифровий процес. Він означає, що юридично обов'язкові стадії повинні враховуватися ще під час проєктування інформаційної системи, а не перевірятися виключно після прийняття рішення. Водночас цей принцип не повинен трансформувати право у жорсткий програмний код. Нормативне регулювання містить оціночні поняття, винятки, дискреційні повноваження та процедури, застосування яких залежить від конкретних обставин. Цифрова система повинна відображати цю складність, а не штучно її усувати. Саме тому особливого значення набуває проблема винятків із стандартної цифрової процедури.

### 6.4. Контрольований виняток, цифровий аудит та гарантії належного функціонування системи

Державне управління не може функціонувати виключно за стандартними сценаріями. Законодавство нерідко передбачає можливість невідкладного рішення, скороченого порядку, спеціальної процедури або відступу від загальної послідовності дій у разі настання визначених обставин. Особливого значення це набуває в умовах воєнного або надзвичайного стану, ліквідації наслідків надзвичайних ситуацій, забезпечення безпеки чи необхідності негайного захисту життя і здоров'я людей.

Якщо цифрова система технічно допускає лише стандартний маршрут, вона може сама стати перешкодою для законної діяльності органу влади. Тому належна цифровізація не повинна ототожнюватися з абсолютною технічною забороною будь-якого відступу від стандартної процедури. Водночас можливість обходу цифрових запобіжників без будь-якої фіксації фактично нівелювала б їх превентивне значення. Для вирішення цієї суперечності пропонується використовувати механізм контрольованого винятку. Його сутність полягає у тому, що коли закон або інший належний нормативний акт допускає відступ від стандартної процедури, інформаційна система повинна дозволяти його здійснення, але окремо фіксувати факт використання такого винятку. До відповідного запису доцільно включати суб'єкта, який ініціював відступ; нормативну підставу; зазначену фактичну причину; час; перелік процедурних етапів, які не були пройдені у звичайному порядку; та, за необхідності, інформацію про подальшу перевірку. Таким чином, виняткова процедура не блокується, але перестає бути невидимою.

Висловлене особливо важливе для запобігання систематичному використанню надзвичайного порядку як способу уникнення стандартних правових гарантій. Якщо інформаційна система накопичує структуровані відомості про випадки використання винятків, контрольний орган може встановити, наприклад, що певний підрозділ або посадова особа непропорційно часто застосовує спрощений порядок. Сам по собі такий факт не доводить протиправності поведінки. Однак він може бути підставою для перевірки того, чи не перетворилася виняткова процедура на фактичне правило. У цьому проявляється ще одна функція цифровізації – можливість переходу від перевірки окремого наказу до аналізу системних управлінських практик.

Якщо традиційний контроль часто починається після виникнення конкретної негативної події, цифрові дані можуть дозволити виявляти повторювані процедурні відхилення до настання особливо тяжких наслідків.

Наприклад, предметом внутрішнього аудиту може бути регулярне внесення істотних змін після юридичного погодження; систематичне використання невідкладної процедури; надмірно часте ручне скасування стандартних цифрових перевірок; повторювані випадки відсутності обов'язкової нормативної підстави; незвична концентрація певних управлінських операцій у одного користувача. Зазначені ознаки не є доказами злочинної поведінки. Їх значення полягає у виявленні організаційної аномалії, що потребує додаткового правового аналізу. Саме тому цифровий аудит не повинен автоматично трансформувати статистичне відхилення у юридичне звинувачення. Такий підхід суперечив би призначенню контрольної системи та створював ризик необґрунтованого втручання у права посадових осіб.

Цифровий аудит, насамперед доцільно розглядати як інструмент перевірки процедури, а не автоматичного встановлення вини. Предметом такого аудиту можуть бути повнота фіксації юридично значущих операцій; дотримання правил доступу; цілісність журналів подій; відповідність цифрових ролей нормативно визначеним повноваженням; коректність застосування процедурних запобіжників; обґрунтованість використання контрольованих винятків; можливість відтворення історії документа.

Окремої уваги потребує незалежність цифрового аудиту. Система контролю втрачає значну частину свого значення, якщо особа, діяльність якої перевіряється, має неконтрольований доступ до механізмів редагування або видалення відповідної інформації. Тому адміністрування критично важливих журналів подій має бути організаційно відокремлене від прийняття управлінських рішень. Для найбільш чутливих систем можуть застосовуватися додаткові процедури доступу, подвійного підтвердження адміністративних операцій або незалежної перевірки цілісності записів.

До того ж, підхід до зберігання цифрового сліду має бути диференційованим. Безстрокове збереження всіх даних не є виправданим.

Строки повинні визначатися характером рішення, можливими юридичними наслідками, законодавчими вимогами до архівного зберігання та необхідністю захисту персональних даних. Так само різним має бути режим доступу. Безпосередній учасник процедури, внутрішній контрольний підрозділ, суд, орган аудиту чи інший уповноважений суб'єкт можуть потребувати різного обсягу інформації. Відповідно, належна система цифрового супроводу повинна поєднувати дві на перший погляд протилежні вимоги: достатність інформації для контролю та обмеження надмірного доступу до неї.

Останнє особливо важливо для наказів і розпоряджень, які містять державну таємницю, службову або іншу інформацію з обмеженим доступом. У таких випадках цифрова фіксація не повинна означати розширення кола осіб, які можуть ознайомитися зі змістом рішення. Водночас режим секретності не повинен виключати саму можливість встановлення того, що юридично значуща дія відбулася. Технічна архітектура може передбачати розмежування між змістом документа та службовими метаданими про його рух, з відповідними окремими режимами доступу.

Особливого значення набуває кібербезпека. У цифровій системі підроблення облікових даних, компрометація засобу автентифікації або незаконний доступ адміністратора здатні створити хибний цифровий слід. Тому правова довіра до електронної фіксації можлива лише за умови належного захисту інформаційної системи [8].

Отже, цифровий запис не повинен сприйматися як абсолютна істина. Як і будь-який інший доказовий матеріал, він потребує оцінки його походження, цілісності та способу формування. Це має особливе значення у спорах, де одна зі сторін заперечує авторство управлінської дії або стверджує про несанкціоноване використання її облікових даних. У таких випадках цифровий паспорт наказу та журнали системи повинні розглядатися у сукупності з інформацією про автентифікацію, безпекові події, права доступу та інші релевантні відомості.

Іншими словами, цифровізація не скасовує традиційних принципів доказування. Вона лише створює нове джерело структурованих відомостей про управлінський процес.

Дослідження автоматизованого адміністративного прийняття рішень у зарубіжній доктрині також демонструють, що технологічна ефективність повинна узгоджуватися з вимогами верховенства права, підзвітності та справедливості. У. Рель та М. Б. Гансен звертають увагу на складне співвідношення між автоматизацією та принципами належного врядування [12]. Х. Хірвонен наголошує на значенні чітких структур відповідальності під час використання автоматизованих систем у публічному секторі [13].

Для запропонованої моделі ці висновки важливі насамперед у частині організаційної відповідальності за функціонування самої цифрової системи. Необхідно розрізняти відповідальність за зміст владного рішення та відповідальність за належне функціонування цифрового середовища, через яке воно проходить. Помилка програмного забезпечення, некоректне налаштування прав доступу або неналежне адміністрування системи можуть впливати на процедуру формування наказу, хоча особа, яка приймає остаточне рішення, безпосередньо не контролює відповідну технічну інфраструктуру. Тому система цифрового супроводу потребує визначення принаймні трьох організаційних ролей: суб’єкта владного рішення; суб’єкта, відповідального за функціонування інформаційної системи; суб’єкта, уповноваженого здійснювати незалежну перевірку її належного функціонування. Наведене розмежування є важливим запобіжником проти ситуації, коли орган, що приймає владні рішення, одночасно одноосібно визначає цифрові правила їх проходження, адмініструє журнали подій і самостійно оцінює належність власних дій.

Цифровий супровід повинен також передбачати періодичний перегляд процедурних правил, закладених в інформаційну систему. Законодавство змінюється, компетенція органів трансформується, окремі погодження

скасовуються або вводяться нові. Якщо цифровий процес своєчасно не актуалізувати, система може почати відтворювати застаріле правове регулювання. У цьому контексті перспективним є запровадження правового аудиту цифрової процедури. Його предметом повинна бути не якість програмного коду як така, а відповідність закладеної в систему послідовності дій чинному законодавству. Такий аудит має перевіряти, чи правильно відображено компетенцію користувачів; чи відповідають обов'язкові поля нормативним вимогам; чи не допускає система обходу необхідних погоджень; чи коректно працюють виняткові процедури; чи не зберігаються застарілі цифрові обмеження після зміни законодавства.

Правовий аудит доцільно проводити не лише після виникнення проблеми, а й під час істотної модернізації інформаційної системи або зміни нормативної бази. Таким чином, контроль має поширюватися не тільки на поведінку посадової особи, а й на саме цифрове середовище здійснення владних повноважень. Останнє дозволяє сформулювати важливий висновок: цифровізація здатна запобігати протиправному владному наказу не тому, що технологія сама відрізняє правомірне рішення від злочинного, а тому, що належно організований цифровий процес зменшує кількість непрозорих зон, у яких може бути приховано порушено процедуру формування владної волі. Чим складніше непомітно змінити документ після погодження, приховати автора істотної правки, оформити відсутнє погодження заднім числом, використати виняткову процедуру без сліду або видалити журнал управлінської операції, тим меншими є організаційні можливості для прихованої реалізації протиправного рішення.

### *Висновки до Розділу 6*

Проведене дослідження дозволяє розглядати цифровізацію державного управління як самостійний організаційно-правовий чинник запобігання протиправному використанню владних наказів. Її превентивний потенціал

пов’язаний не з переданням технологічній системі функції юридичної оцінки наказу, а зі зміною самого середовища формування владної волі. Цифрові засоби здатні зробити юридично значущі етапи підготовки, погодження, видання, зміни та доведення наказу більш встановлюваними, а прихований обхід відповідних процедур – складнішим.

Запропоновано використовувати поняття «цифровий супровід владного наказу», під яким розуміється організаційно-правове забезпечення основних етапів його формування та реалізації за допомогою цифрових засобів, що дозволяють встановити суб’єкта, час, правову підставу, зміст і місце відповідної операції у загальній послідовності управлінського процесу, що переносить акцент із цифровізації кінцевого документа на цифрове забезпечення всього юридично значущого шляху владного рішення.

Обґрунтовано доцільність формування цифрового паспорта владного наказу як структурованого набору метаданих про його походження та проходження процедури. До таких відомостей можуть належати ініціатор рішення, зазначена нормативна підстава, автор проєкту, учасники обов’язкового погодження, час відповідних дій, версії документа, автори істотних змін, факт остаточного санкціонування, адресат, спосіб доведення та використання виняткової процедури. Цифровий паспорт не повинен містити автоматичної оцінки правомірності або злочинності наказу; його призначення полягає у створенні достовірної інформаційної основи для наступного правового контролю.

Встановлено, що одним із ключових елементів цифрового супроводу має бути зв’язок юридично значущої дії з конкретною версією владного рішення. Погодження, правова експертиза чи інша процедурна дія не повинні автоматично поширюватися на істотно змінений після їх здійснення текст. Зміна юридично значущого положення має залишати окремий цифровий слід із зазначенням суб’єкта та часу відповідної операції.

Запропоновано розвивати цифрові процедурні запобіжники, спрямовані на перевірку формалізованих умов прийняття владного рішення: належності відповідної дії до цифрової ролі суб'єкта, проходження обов'язкових погоджень, зазначення передбаченої процедурою правової підстави, дотримання послідовності юридично значущих етапів та актуальності погоджень після зміни документа. Такі запобіжники не повинні розглядатися як автоматичне підтвердження законності рішення. Їх функцією є недопущення непомітного обходу формалізованих вимог до процедури.

Обґрунтовано необхідність чіткого розмежування технічної допустимості операції та юридичної правомірності владного рішення. Можливість або неможливість здійснення певної дії в інформаційній системі сама по собі не створює і не припиняє владне повноваження. Цифрові налаштування мають відображати нормативне регулювання, а не підміняти його.

Для випадків, коли закон допускає відступ від стандартної процедури, запропоновано механізм контрольованого винятку. Його сутність полягає в тому, що цифрова система не блокує законно передбачений відступ, але окремо фіксує суб'єкта, нормативну і фактичну підстави, час та зміст відповідного процедурного відхилення. Це дозволяє поєднати необхідну управлінську оперативність із можливістю наступного контролю та зменшує ризик перетворення виняткової процедури на постійний спосіб обходу правових гарантій.

Доведено, що цифрові відомості про формування владного наказу повинні використовуватися не лише для перевірки окремих рішень, а й для виявлення системних процедурних відхилень. Повторюване використання виняткових процедур, внесення істотних змін після погодження, систематичний обхід передбачених цифрових перевірок або інші нетипові моделі можуть бути підставою для правового аудиту, але не повинні автоматично кваліфікуватися як доказ протиправної поведінки.

Запропоновано розвивати правовий аудит цифрової процедури, предметом якого є відповідність закладеної в інформаційну систему моделі управлінського процесу чинному законодавству. Такий аудит має охоплювати коректність цифрового відображення компетенції, обов'язкових процедур, винятків, правил доступу та механізмів фіксації юридично значущих операцій.

Визначено, що ефективність цифрового супроводу залежить від захищеності цифрового сліду. Особа, яка формує владне рішення, не повинна мати неконтрольованої можливості змінити або видалити історію його проходження. Водночас обсяг фіксації має відповідати принципу необхідної достатності: цифровізація не може перетворюватися на необмежене накопичення службової та персональної інформації.

Таким чином, цифровізація може виконувати превентивну функцію у сфері владних наказів за умови, що її основним орієнтиром є не максимальна автоматизація, а прозорість походження владного рішення, цілісність його управлінської історії та контрольованість процедурних відхилень. Така модель створює середовище, у якому протиправне рішення складніше сформувати шляхом прихованого обходу процедури, непомітно змінити після погодження або позбавити відомостей про осіб, причетних до його підготовки та реалізації.

**Список використаних джерел:**

1. Конституція України від 28.06.1996 р. № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

2. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 року № 851-IV. *Відомості Верховної Ради України*. 2003 р. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

3. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 5 жовтня 2017 року № 2155-VIII. *Відомості Верховної Ради України.* 2017 р. № 45. Ст. 400. URL: https://zakon.rada.gov.ua/laws/show/2155-19

4. Деякі питання документування управлінської діяльності: Постанова Кабінету Міністрів України від 17 січня 2018 року № 55. *Офіційний вісник України.* 2018 р. № 23. Ст. 770. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text

5. Про публічні електронні реєстри: Закон України від 18 листопада 2021 року № 1907-IX. *Відомості Верховної Ради України*. 2023. № 11. Ст. 27. URL: https://zakon.rada.gov.ua/laws/show/1907-IX

6. Деякі питання електронної взаємодії електронних інформаційних ресурсів: постанова Кабінету Міністрів України від 8 вересня 2016 року № 606. *Офіційний вісник України*. 2016. № 73. Ст. 2455. URL: https://zakon.rada.gov.ua/laws/show/606-2016-%D0%BF#Text

7. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

8. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

9. Про адміністративну процедуру: Закон України від 17 лютого 2022 року № 2073-IX. *Відомості Верховної Ради України*. 2023. № 15. Ст. 50. URL: https://zakon.rada.gov.ua/laws/show/2073-20#Text

10. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

11. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225) (2025). URL: https://book.coe.int/en/texts-of-council-of-europe-treaties/12226-pdf-council-of-europe-framework-convention-on-artificial-intelligence-and-human-rights-democracy-and-the-rule-of-law-cets-no-225.html

12. Roehl U. B. U., Hansen M. B. Automated, Administrative Decision-Making and Good Governance: Synergies, Trade-Offs, and Limits. *Public Administration Review.* 2024. Vol. 84. No. 6. P. 1184-1199. DOI: https://doi.org/10.1111/puar.13799

13. Hirvonen H. Just Accountability Structures – A Way to Promote the Safe Use of Automated Decision-Making in the Public Sector. AI & Society. 2024. Vol. 39. P. 155–167. URL: https://link.springer.com/article/10.1007/s00146-023-01731-z

# РОЗДІЛ 7
# ГРОМАДСЬКЕ ЗДОРОВ'Я НАЦІЇ ТА ПРОБЛЕМИ ЗАХИСТУ РЕПРОДУКТИВНИХ ПРАВ НАСЕЛЕННЯ В УКРАЇНІ

Автор: **Галайко Арета Михайлівна,** *аспірантка кафедри теорії права і конституціоналізму, Національного університету «Львівська політехніка» https://orcid.org/0009-0007-9636-2469*

## 7.1. Громадське здоров'я як соціально-правова проблема сучасності

Громадське здоров'я є широкою соціальною, правовою та медичною категорією, що потребує особливої доктринальної уваги на сучасному етапі розвитку державності. Проблеми санітарно-епідеміологічного, профілактичного, постмандемічного та військово-екуологічного характеру створюють додаткові вагомі загрози добробуту нації та його основній нематеріальній цінності – здоров'ю.

Питання забезпечення належного стану здоров'я народу та нації лежить у двох площинках, з одного боку це проблема особистісного характеру та тісно пов'язана з охороною та захистом прав людини на охорону здоров'я, а з іншого боку проблематика також належить сфері державно-публічної політики.

Питання громадського здоров'я у всіх країнах світу перебуває на особливому державно-суспільному контролі та проблематика є особливо чутливою для політичної еліти та й для виборців. «Право на охорону здоров'я є ключовою темою дискусій у всьому світі, а забезпечення реалізації цього права й можливості населення отримати доступ до потрібної медичної допомоги перебуває у центрі уваги» [1, с.31].

В цьому аспекті доречно погодитися з медичною спільнотою, котра вказує, що «турбота про здоров'я має бути не тільки завданням для державних органів влади і медичних працівників, вона має бути особистим устремлінням кожної людини. Особливо у той час, коли у місті і країні залишаються високими

захворюваність на туберкульоз і злоякісні новоутворення, а також захворюваність серцево-судинними недугами та ВІЛ/СНІД інфекцію, показники яких у місті перевищують середні національні, що потребує неординарних заходів для подолання цих проблем» [2].

Завдання забезпечення громадського здоров'я в державному масштабі, на нашу думку має потрійну природу.

По-перше слід вести мову про формування належної правової політики у сфері забезпечення, захисту, охорони та гарантування медичних прав людини, громадянина, окремих груп осіб (військовослужбовців, дітей, вагітних жінок) та й загалом всього населення.

Слід зазначити, що проблем у забезпеченні таких правових механізмів безумовно сьогодні не бракує. Доречно виокремити основні з них.

До основних проблем правового забезпечення громадського здоров'я насамперед слід віднести фрагментарність та недостатню системність нормативно-правового регулювання. Тут слід вести мову не тільки про відсутність комплексного оновленого кодифікованого нормативного акту, а загалом про методологічні проблеми інституту медичного права. Доречно погодитися з Р. Лемехою в тому, що «Нині, активно ведуться дискусії про існування медичного права як самостійної галузі, співвідношення медичного права з сформованими галузями права (цивільним, кримінальним, конституційним, адміністративним та ін.), предмета його регулювання, роль і місце у правовій системі, відокремлення законодавства про охорону здоров'я у структурі законодавства в цілому. Очевидно, що незалежно від науково-юридичної відповіді на подібні питання, правове регулювання охорони здоров'я та життя людей є однією з найбільш суспільно значущих сфер діяльності, пов'язаною із виникненням специфічних правових відносин, що врегульовуються відповідними нормативно-паровими актами» [3, с.41]

Незважаючи на суттєве оновлення законодавства у сфері охорони здоров'я протягом останніх років, чинна нормативна база все ще характеризується значною кількістю колізій, дублюванням окремих повноважень органів державної влади, відсутністю єдиного концептуального підходу до регулювання суспільних відносин у сфері громадського здоров'я. Така ситуація ускладнює ефективне правозастосування, створює неоднозначність тлумачення правових норм та негативно впливає на реалізацію державної політики у відповідній сфері.

Попри те європейські стандарти та практика окремих країн ЄС вказує, що саме належне правове регулювання створює первинне підґрунтя оновлення підходу до захисту медичних прав населення країни. Для прикладу проаналізуємо досвід Польщі, де «система громадського здоров'я регулюється законом, прийнятим 2015 року. Основні положення цього закону випливають із необхідності виконання десяти оперативних функцій громадського здоров'я на державному та регіональному рівнях. Генеральною метою польського законодавства стало створення ефективної моделі громадської охорони здоров'я за рахунок координації та інтеграції зусиль цілого суспільства у напрямі профілактики хвороб, продовження тривалості життя і промоції здоров'я. Головним координатором дій учасників системи громадського здоров'я визначено Міністра охорони здоров'я, основним завданням якого у цьому напрямі є приготування проекту Національної Програми Здоров'я на підставі рекомендацій Ради із справ Громадського Здоров'я. До вказаної Ради входять представники усіх зацікавлених сторін, у т.ч. Президента Польської Республіки, всіх Міністерств і відомств, Національного Фонду Здоров'я, громадських рад медичних і фармацевтичних працівників, організації працедавців, науково-дослідних інституцій, головні спеціалісти тощо. Національна Програма Здоров'я розробляється на п'ять років. Для її виконання формується Комітет управління НПЗ. Законом також визначено порядок підзвітності, відповідальності всіх учасників та принципи фінансування системи громадського здоров'я» [4, с.318].

Такий підхід дозволяє забезпечити координацію зусиль багатьох сфер суспільно-правового життя та убезпечити громадськість без невиваженого правового регулювання.

Другу групу проблем становлять організаційно-інституційні недоліки функціонування системи громадського здоров'я. Йдеться про недостатній рівень координації діяльності органів державної влади, органів місцевого самоврядування, закладів охорони здоров'я, спеціалізованих державних установ та інших суб'єктів, які беруть участь у реалізації політики громадського здоров'я. Відсутність належної міжвідомчої взаємодії нерідко призводить до дублювання функцій, неефективного використання фінансових ресурсів, затримок у прийнятті управлінських рішень та зниження ефективності профілактичних і протиепідемічних заходів.

Наступною суттєвою проблемою є недостатня превентивна спрямованість державної політики. Традиційно система охорони здоров'я зосереджується переважно на лікуванні вже існуючих захворювань, тоді як профілактика, формування здорового способу життя, мінімізація факторів ризику та популяризація здоров'язбережувальної поведінки населення залишаються недостатньо ефективними. Саме профілактична модель розвитку системи громадського здоров'я повинна стати одним із пріоритетів сучасної державної політики.

Особливої актуальності набуває проблема забезпечення належного рівня біологічної, санітарно-епідеміологічної та екологічної безпеки. Досвід пандемії COVID-19, а також негативні наслідки широкомасштабної збройної агресії проти України засвідчили необхідність формування сучасної системи реагування на біологічні загрози, масові інфекційні захворювання, погіршення екологічної ситуації, руйнування об'єктів критичної інфраструктури та інші фактори, які безпосередньо впливають на стан громадського здоров'я.

Не менш важливою проблемою залишається забезпечення рівного доступу населення до медичних послуг. Незважаючи на реформування системи охорони здоров'я, у різних регіонах України зберігається нерівномірність медичного забезпечення, особливо в сільській місцевості, на деокупованих територіях та в районах, що постраждали від бойових дій. Суттєвими викликами залишаються кадровий дефіцит, недостатній рівень матеріально-технічного забезпечення медичних закладів, обмежена доступність високоспеціалізованої медичної допомоги та нерівномірний розвиток цифрової медичної інфраструктури.

Важливим напрямом удосконалення правового забезпечення громадського здоров'я є також розвиток цифровізації медичної сфери. Йдеться про впровадження сучасних інформаційних технологій, електронних медичних систем, цифрового моніторингу стану здоров'я населення, використання великих масивів медичних даних для прогнозування епідеміологічної ситуації, а також забезпечення належного рівня кібербезпеки та захисту персональних медичних даних.

Особливої уваги потребує проблема поширення неправдивої інформації з приводу дескридитації статусу пацієнта, проблеми безпеки персональних даних та аспекти поширення медичних зображень (в контексті репродуктивних та сексуальних прав людині останні набувають особливо суттєвого значення).

У контексті медичної візуалізації Р. Дженніфер і Е. Антуанетта аналізують етичні та правові аспекти використання медичних зображень [5]. Вони підкреслюють, що використання таких зображень без попередньої згоди пацієнтів не лише порушує приватність, а й може мати серйозні юридичні наслідки для медичних закладів. Вчені наголошують на необхідності впровадження сучасних технологічних рішень для захисту конфіденційності медичних даних.

Українські науковці вказують, що «розвиток цифрових технологій створює нові виклики для захисту зображення, зокрема через несанкціоноване

розповсюдження та комерціалізацію без попередньої згоди особи. Сучасні правові норми повинні враховувати як суб'єктивні, так і об'єктивні аспекти цього права, забезпечуючи баланс між економічними інтересами та захистом особистої гідності. Інтеграція міжнародних стандартів із національним законодавством є необхідною умовою для ефективного захисту прав осіб у глобалізованому світі. У сфері медичної візуалізації проблема набуває особливої актуальності, оскільки доступ до медичних зображень без належного контролю може негативно вплинути на якість діагностики та лікування, а також порушувати права пацієнтів. Тому важливо забезпечити як юридичний, так і технологічний захист цих даних, впроваджуючи сучасні засоби контролю та моніторингу» [6].

Також в контексті медичних проблем слід вказати на те, що розвиток біотехнологій спричиняє значні прогалини та колізії в правовому регулюванні нових медичних прав людини.

Подамо приклад у сфері репродуктивних прав.

Новітній прогрес у медицині та біотехнологіях дозволяє такий унікальний процес як реалізація репродуктивного права після власної смерті. Вказане називається посмертною репродукцією. Реалізується шляхом використання репродуктивного матеріалу людини, зокрема сперми, ембріону, яйцеклітин, вже після смерті особи з метою народження її генетичної дитини.

Досягнення в технологіях допоміжної репродукції дозволили застосовувати різні форми посмертної репродукції. Можливість використання кріоконсервованих сперматозоїдів та допоміжних репродуктивних методів, таких як екстракорпоральне запліднення, дозволяє жінці зачати дитину від померлого чоловіка. Кріоконсервація ембріонів дає змогу народити дитину після смерті батька, матері або обох батьків. Одним з можливих сценаріїв посмертної репродукції є отримання сперми померлої особи або особи, яка перебуває в постійному вегетативному стані, для використання її в репродуктивних цілях.

Разом з тим доречно говорити, що регулювання посмертного відтворення порушує безліч біоетичних, соціальних, правових та адміністративних питань. В цьому аспекті виникають багато проблем у тому числі й юридичного характеру: визначення права на запит на посмертне вилучення та/або посмертне використання сперми, яйцеклітин або ембріонів членом подружжя чи партнером а також спадкоємцями особи; вид інформаційної згоди, що оформляється при житті особи; питання спадкування та строків використання (збереження) гамет; визначення найкращих інтересів майбутньої дитини.

Регулювання посмертного відтворення порушує правові питання щодо законного батьківства, оскільки після вилучення та збереження гамет запліднення та імплантація можуть не відбуватися протягом певного часу. Це викликає проблеми в кількох юрисдикціях, оскільки генетичний батько може не бути визнаний законним батьком дитини через певний період часу після смерті [7].

По-друге, площина забезпечення належної правової політики для нації в умовах реформування медичної системи, загроз інфрастуктурно-безпекового характеру лежить також в організаційних гарантіях.

Проте вагомо, щоб вони мали домінантно превентивний характер. Безумовно, забезпечення належної інфраструктури закладів охорони здоров'я, фахових спеціалістів, безпечних та ефективних лікарських засобів має вагоме значення для пацієнта, що вже має певну медико-соматичну проблему. Але, підхід держави, який би вказував на можливості упередження проблеми є набагато мудрішим, виваженим тай економічно доцільним. Фахівці вказують, що «Організаційно-методичну, координаційну та оперативну роботу з гігієнічного навчання та виховання населення здійснюють обласні, міські та районні Центри здоров'я, але до санітарно-освітньої роботи мають залучатись усі медичні працівники. У кожному лікувально-профілактичному закладі повинен бути складений план цієї роботи, перелік лекторів та відповідальних, тем лекцій,

бесід, графік їх проведення тощо. Ця робота має проводитися Центрами здоров'я, кабінетами та окремими інструкторами-методистами із санітарної освіти із залученням засобів масової інформації в тісній взаємодії з громадськими (опікунськими та наглядовими) радами при лікувально-профілактичних закладах, громадськими організаціями сприяння хворим». Тут ми погоджуємося особливо в тому, що інформаційна політика превенції повинна займати чільне місце в публічно-владній діяльності у сфері забезпечення громадського здоров'я.

У сучасних умовах така інформаційно-превентивна діяльність не може обмежуватися лише традиційними формами санітарно-просвітницької роботи. Її зміст повинен відповідати сучасним суспільним викликам, охоплюючи формування культури здорового способу життя, розвиток навичок відповідальної поведінки щодо власного здоров'я, популяризацію профілактичних медичних оглядів, вакцинації, психогігієни, належного харчування, фізичної активності та своєчасного звернення за медичною допомогою. Саме формування відповідальної правосвідомості населення щодо збереження здоров'я має розглядатися як один із ключових напрямів державної політики у сфері громадського здоров'я.

Особливого значення набуває використання сучасних цифрових комунікаційних інструментів. Держава повинна активно використовувати офіційні електронні ресурси, соціальні мережі, мобільні застосунки, телемедичні сервіси та інші цифрові платформи для оперативного інформування населення про потенційні загрози здоров'ю, профілактичні заходи, програми скринінгу, календарі профілактичних щеплень, а також рекомендації щодо дій в умовах надзвичайних ситуацій, епідемій чи техногенних катастроф. Такий підхід дозволяє забезпечити оперативність поширення інформації, її доступність та охоплення максимально широкого кола осіб.

Водночас інформаційна політика у сфері громадського здоров'я повинна супроводжуватися ефективними механізмами протидії дезінформації.

Поширення неправдивих або маніпулятивних відомостей щодо методів лікування, вакцинації, профілактики інфекційних захворювань чи діяльності органів охорони здоров'я здатне істотно знизити ефективність державних програм та негативно вплинути на рівень довіри населення до системи охорони здоров'я. Саме тому одним із напрямів діяльності уповноважених органів має стати своєчасне спростування недостовірної інформації, проведення інформаційно-роз'яснювальної роботи та забезпечення громадян доступом до офіційних і науково обґрунтованих джерел інформації.

Крім того, організаційні гарантії забезпечення громадського здоров'я мають передбачати постійне вдосконалення міжвідомчої взаємодії. Ефективна реалізація державної політики неможлива без узгодженої діяльності органів охорони здоров'я, освітньої сфери, соціального захисту, органів місцевого самоврядування, правоохоронних органів, військових адміністрацій, громадських об'єднань та міжнародних партнерів. Така взаємодія дозволяє комплексно реагувати на сучасні виклики, забезпечуючи безперервність профілактичних, лікувальних і реабілітаційних заходів.

І останньою (третьою) групою проблем, які на нашу думку слід виокремити – це безумовно питання резистентності медицини у час військових загроз.

М. Малачинська вказує, що «руйнування інфраструктури охорони здоров'я, нестача медикаментів та персоналу суттєво обмежують доступність послуг з охорони репродуктивного здоров'я. Така ситуація підвищує ризики ускладнень під час вагітності, передчасних пологів та материнської смертності. Зусилля з відновлення системи охорони здоров'я та забезпечення безперервної медичної допомоги є вкрай необхідними» [8].

Окремої уваги потребує проблема забезпечення психічного здоров'я населення. Повномасштабна війна спричинила різке збільшення кількості осіб, які потребують психологічної та психіатричної допомоги, соціальної

реабілітації, комплексної підтримки після отриманих травм, втрати близьких або вимушеного переміщення. У зв'язку з цим державна політика у сфері громадського здоров'я повинна передбачати комплексний розвиток системи охорони психічного здоров'я як одного з ключових напрямів забезпечення національної безпеки та людського потенціалу держави.

Водночас питання забезпечення резистентності системи охорони здоров'я в умовах війни не обмежується лише відновленням пошкодженої медичної інфраструктури чи кадрового потенціалу. Йдеться про формування стійкої системи громадського здоров'я, здатної безперервно функціонувати в умовах воєнного стану, масових переміщень населення, енергетичних криз, кіберзагроз та інших надзвичайних обставин. Саме тому концепція резистентності має охоплювати не лише здатність системи реагувати на кризові ситуації, а й її спроможність швидко адаптуватися до нових викликів, мінімізувати негативні наслідки та забезпечувати безперервність надання медичної допомоги.

Важливим елементом такої стійкості є створення ефективної системи кризового управління у сфері охорони здоров'я. Це передбачає розроблення планів реагування на різні види загроз, формування резервів лікарських засобів, медичного обладнання та засобів індивідуального захисту, удосконалення механізмів медичної евакуації, забезпечення безперебійного функціонування критично важливих медичних інформаційних систем, а також підготовку медичних працівників до роботи в умовах надзвичайних ситуацій та бойових дій.

Не менш важливого значення набуває розвиток системи реабілітаційної допомоги. Збройна агресія спричинила істотне збільшення кількості осіб, які потребують тривалого фізичного, психологічного та соціального відновлення. Це стосується не лише військовослужбовців, а й цивільного населення, яке зазнало поранень, втрати працездатності або інших наслідків війни.

Науковці зауважують, що повномасштабна війна, розпочата Російською Федерацією проти України, призвела до безпрецедентних людських втрат,

масових поранень та глибоких психологічних травм серед як військовослужбовців, так і цивільного населення. Водночас ця реальність виявила не лише величезні виклики, що стоять перед системою охорони здоров'я, але й структурну крихкість існуючих механізмів соціальної та психологічної підтримки.

У цьому контексті питання медичної та психологічної реабілітації виходять далеко за межі суто медичного чи соціального виміру, набуваючи статусу фундаментального правового обов'язку держави та стаючи вирішальним інструментом захисту прав людини під час воєнного часу. Конституція України гарантує право кожного на охорону здоров'я та медичну допомогу (ст. 49), тоді як міжнародно-правові документи, включаючи Конвенцію про права інвалідів (2006), прямо зобов'язують держави-учасниці створювати належні умови для реабілітації та соціальної інтеграції осіб, які постраждали від травми, інвалідності або психологічної травми. Ці норми підкреслюють, що реабілітацію не слід розглядати як дискреційну державну послугу чи привілей, а як право, що підлягає виконанню та вимагає ефективних механізмів реалізації та належної інституційної підтримки [9].

У зв'язку з цим державна політика повинна забезпечувати доступність комплексної реабілітації, впровадження сучасних міжнародних стандартів реабілітаційної медицини, розвиток мультидисциплінарних команд та інтеграцію реабілітаційних послуг у загальну систему охорони здоров'я.

Особливої уваги потребує також забезпечення медико-біологічної безпеки держави. Воєнні дії створюють додаткові ризики виникнення епідемічних спалахів, погіршення санітарно-епідемічної ситуації, забруднення довкілля небезпечними речовинами, пошкодження об'єктів водопостачання та критичної інфраструктури. За таких умов одним із пріоритетних напрямів державної політики має стати постійний моніторинг стану громадського здоров'я,

своєчасне виявлення потенційних загроз та оперативне впровадження комплексу профілактичних і протиепідемічних заходів.

Таким чином, можемо констатувати, що в сучасних умовах питання медичного права, захисту прав громадян у сфері охорони здоров'я набуває ширшого розуміння, та потребує тлумачення та аналізу також в контексті правової політики національної безпеки.

### 7.2. Репродуктивне здоров'я української нації

Репродуктивне здоров'я є складовою громадського здоров'я й визначається на міжнародному та національному рівні як вагома складова суспільного добробуту. Доступ до послуг репродуктивного здоров'я, який дозволяє людям жити повноцінним життям та насолоджуватися безпечним і задовільним сексуальним життям, є життєво важливим компонентом загального здоров'я.

Захист цієї сфери лежить в межах встановлених Цілей сталого розвитку, в першу чергу через формування та реалізацію концепції гендерної рівності та прав людини.

У Програмі дій, прийнятій на Міжнародній конференції з питань народонаселення та розвитку, яка була проведена в Каїрі у 1994 році подано розуміння репродуктивного здоров'я і воно тлумачиться міжнародною спільнотою дуже широко, оскільки охоплює фізичний, розумовий та соціальний добробут у всіх питаннях, що стосуються репродуктивної системи та її функцій та процесів. Отож правове регулювання окрім узвичаєного розуміння репродуктивного здоров'я через убезпечення материнства, дитинства, вагітності, регулювання аспектів контрацепції та переривання вагітності, сурогатного материнства та інших репродуктивних технологій повинно всеосяжно підходити до проблематики.

Право на репродуктивне здоров'я підтримується міжнародними документами та нормативними актами, спрямованими на захист прав людини. У

2015 році Генеральна Асамблея Організації Об'єднаних Націй схвалила 17 цілей сталого розвитку з метою сприяння організаційній функціональності та інтеграції сталого розвитку, а отже, для задоволення поточних і майбутніх потреб зацікавлених сторін і забезпечення кращого та сталого майбутнього для всіх, збалансування економічного, соціального та екологічного розвитку. Ціль сталого розвитку № 3 найбільш прямо стосується репродукції і репродуктивного здоров'я «Забезпечення здоров'я та сприяння добробуту для всіх у всіх вікових групах». Одним з підцілей цієї цілі є «Забезпечення всім належного доступу до сексуального та репродуктивного здоров'я і репродуктивних прав відповідно до принципів прав людини», котра визначає важливість доступу до інформації та послуг у галузі репродуктивного здоров'я для всіх людей, незалежно від їхньої статі, віку та соціального статусу, вказуючи на необхідність забезпечення гідного стану здоров'я для всіх груп населення, включаючи зменшення смертності матерів та немовлят, покращення якості життя та забезпечення доступу до необхідних медичних послуг. Ця ціль також визначає важливість захисту репродуктивних прав людей та забезпечення їхнього права на вільний вибір у сфері сімейного планування та репродукції. Вона підкреслює необхідність усунення будь-яких обмежень або дискримінації, які можуть перешкоджати людям у здійсненні їхніх репродуктивних прав.

Наукова спільнота вказує, що репродуктивні права визнають право кожної людини на вільний і самостійний вибір щодо питань свого репродуктивного здоров'я, включаючи планування сім'ї, народження дітей і доступ до різних репродуктивних послуг та технологій.

В.Берч зауважує, що «репродуктивні права включають в себе право на вільний вибір кількості дітей, інтервалів між народженнями, а також право на доступ до інформації та послуг, пов'язаних з репродуктивним здоров'ям. Вони дозволяють людині приймати рішення про своє репродуктивне майбутнє відповідно до її власних цінностей і переконань. Медичне право включає в себе

норми і принципи, які регулюють медичну практику, відносини між медичними працівниками та пацієнтами, а також забезпечують дотримання етичних стандартів у медичній сфері. Таким чином, репродуктивні права гарантують гідність та автономію особи в прийманні важливих рішень щодо її репродуктивного здоров'я. Це особливо важливо в сучасному суспільстві, де медичні досягнення та технології надають більше можливостей для вибору та контролю над репродуктивними процесами» [10, с.94].

Право на репродукцію також вміщує в собі етичних контекст, враховуючи моральні аспекти пов'язані з відповідальністю за народження та виховання дітей, а також з підтримкою та захистом прав дитини, включає в себе обов'язок відповідально ставитися до створених дітей та забезпечення належних умов для їхнього фізичного, емоційного та соціального розвитку. Етичний аспект включає в себе питання планування сім'ї, зокрема вибір оптимального часу та кількості дітей, які можуть бути здоровими та морально підготовленими для прийняття в сім'ю. Етика вимагає, щоб при репродукції було враховано інтереси та права дитини, яка буде народжена, створення умов для її здорового розвитку, захисту від будь-якого виду насильства або зловживання та забезпечення поваги до її особистості.

Репродуктивне, материнське, новонароджене, дитяче та підліткове здоров'я є наріжним каменем здорового розвитку наступного покоління та рушійною силою прогресу населення та суспільства в майбутньому, особливо в епоху старіння населення та низької народжуваності. Слід погодитися з науковцями, котрі вказують, що сучасним завданням сектору громадського здоров'я є протидія дискримінації та нерівності в доступі до різних медичних послуг, збільшення тривалості життя населення та формування здорового способу життя для майбутніх поколінь.

Хронічний стрес є основним фактором, що впливає на репродуктивну систему як жінок, так і чоловіків, зокрема порушення менструального циклу,

овуляторні збої, гормональні дисбаланси, підвищений ризик викиднів зниження рівня тестостерону, погіршення якості сперми, проблеми з лібідо. Психоемоційна травма, яку переживають українці, особливо ті, хто перебував у зонах активних бойових дій, прямо пов'язана з репродуктивними розладами. Таку проблему не можна нехтувати на правовому та державно-управлінському рівні.

### 7.3. Питання рівного доступу у сфері репродуктивних прав людини

Слід констатувати, що питання рівності та недискримінації та подолання проблем пов'язаних у цій сфері має вагоме значення для забезпечення правової, демократичної держави.

Репродуктивні характеристики людини – це особлива сфера суспільного життя і проблема рівності доступ до репродуктивних послуг відрізняється залежно від статі, оскільки чоловіки та жінки в усьому світі мають нерівний доступ до необхідної інформації та послуг, необхідних для повного благополуччя, задовільного сексуального життя, захисту від інфекцій, що передаються статевим шляхом, запобігання небажаній вагітності та лікування безпліддя.

Репродуктивне здоров'я, зміна чисельності та вікової структури населення може мати серйозні економічні, соціальні та геополітичні наслідки в багатьох країнах, тому необхідним завданням сучасної науки є проведення комплексних, міжкомплементарних досліджень щодо вивчення проблем репродуктивного здоров'я, щоб розробляти ефективні стратегії для їх вирішення, що дозволить розробити програми підтримки материнства та дитинства, забезпечити доступ до якісних послуг репродуктивного здоров'я та контрацепції, а також підвищити рівень освіти населення з питань сексуального та репродуктивного здоров'я. Вирішення цих проблем важливо для забезпечення сталого розвитку суспільства та покращення якості життя населення.

Відомі причини такого нерівного доступу варіюються від соціальних та культурних до економічних. Наприклад, обмежений процес прийняття рішень та фінансової автономії для жінок може обмежувати їхній доступ до своєчасних та ефективних послуг репродуктивного здоров'я, необхідних для лікування та запобігання несприятливим наслідкам для здоров'я. З іншого боку, навіть чоловіки можуть мати обмежений доступ до послуг через культурні та часові обмеження, а в аспекті українських реалій додамо ще військові труднощі життя захисників чоловічої статі.

Наукові дослідження, що стосуються гендерної рівності та протидії дискримінації при реалізації репродуктивних прав доводять, що расова та етнічна невідповідність у здоров'ї жінок існувала десятиліттями, незважаючи на зусилля, спрямовані на посилення доступу до репродуктивного здоров'я жінок та їх використання. Досягнення рівності в охороні здоров'я вимагає розуміння поточних расово-етнічних розривів у репродуктивному здоров'ї та узгоджених зусиль для розробки та впровадження стратегій для усунення розривів [11].

Додати слід, що проблема має мультидисциплінарний характер, адже дискримінація в медико-репродуктивній сфері не тільки безумовно значно вища для жінок, проте вона значно посилюється додатковими соціальним обтяжувальними ознаками, зокрема такими як бідність та територіальна доступність медичних послуг.

Цю думку репрезентують ґрунтовні наукові дослідження фахівців, зокрема що проводилися в Ефіопії.

Дослідники вказали, що в цій країні третього світу «Частка вагітних жінок, які отримали допологовий догляд, становила всього 65,5% (95% ДІ: 63,8–71,0%). Більшість вагітних жінок народжували вдома (68,4%; 95% ДІ: 66,8–70,0%). Близько третини (95% ДІ: 30,4–33,6%) звернулися за негайним післяпологовим доглядом. Жінки, які мали право звертатися за послугами з охорони здоров'я матері, відвідували принаймні початкову школу, жінки та їхній партнер мали

оплачувану роботу, були в супроводі партнера, мали сильну соціальну підтримку та були схваленими щодо справедливих гендерних норм. Тим не менш, жінки, які проживали далеко від медичних закладів, мали великі сім'ї та жили в скотарських умовах, негативно впливали на користування послугами з охорони здоров'я матері. Старомодні гендерні норми, відсутність доступу до фінансування, страх за свою безпеку та відсутність місцевого та культурно чутливого догляду були перешкодами для користування послугами з охорони здоров'я матері» [12].

Загалом експерти міжнародного рівня зауважують, що правова політика багатьох держав значно покращилася в цьому аспекті, проте все ж констатують, що незважаючи на покращення національного охоплення медичним обслуговуванням, нерівність зберігається, і жінки репродуктивного віку, особливо ті, що мешкають у сільській місцевості та з нижчих соціально-економічних прошарків, стикаються зі значними перешкодами в доступі до основних послуг [13].

Гендерна нерівність прослідковується також в невідповідному жіночому тягарі в контексті відповідальності за зачаття та пологи.

Покращення здоров'я до зачаття є життєво важливим для здоров'я матері та дитини, проте суспільні уявлення про те, хто несе за це відповідальність, залишаються недостатньо паритетними та гендерно рівними. жінки несуть більшу частину тягаря. Це трапляється в охороні здоров'я, дослідженнях та повсякденному житті. Чоловіків часто не враховують у розмовах про здоров'я під час вагітності. Сучасні підходи до покращення здоров'я до вагітності зосереджуються на виборі та діях жінок, таких як дієта та куріння, а не на ширших проблемах – партнерська підготовка до зачаття та народження майбутнього покоління. Міжнародні експерти вказують, що «здоров'я до вагітності має бути спільною відповідальністю партнерів, медичних працівників,

уряду та суспільства» [14], тому вони пропонують державні програми рівноправно залучати чоловіків до охорони здоров'я.

Проблематика нерівного доступу та дискримінації посилюється в умовах військових загроз та міграційних процесів, що посилюються у зв'язку з бажанням людей захистити своє онтологічне право на життя.

За даними Всесвітньої організації охорони здоров'я, жінки-мігранти та біженки мають підвищений ризик зґвалтування, небажаної вагітності та небезпечних абортів [15]. Ба більше, навіть в сучасних умовах існують прецеденти прямого втручання в репродуктивін права цієї групи осіб. Наприкінці 2020 року широкого розголосу набув прецедент примусової стерилізацію латиноамериканських іммігрантів, яких утримували в центрі утримання Імміграційної митної та правоохоронної служби США [16].

Професор І.Жаровська вказує, що «Гендерна дискримінація значно впливає на доступ до медичних послуг, якість лікування та загальний рівень здоров'я жінок. Часто вона проявляється у недостатній увазі до жіночих проблем у сфері охорони здоров'я, а також у структурних бар'єрах, що обмежують можливості жінок отримати необхідну медичну допомогу.

Жінки можуть стикатися з обмеженим доступом до репродуктивного здоров'я, включаючи контрацепцію, аборти та медичний супровід вагітності. У багатьох країнах законодавчі або соціальні обмеження ускладнюють отримання цих послуг, що негативно позначається на здоров'ї жінок. Крім того, у медичних дослідженнях часто недостатньо враховуються особливості жіночого організму, що призводить до менш ефективного діагностування та лікування захворювань» [17].

### 7.4. Насильство та його вплив на репродуктивне здоров'я нації

Відповідно до висловленої позиції ВООЗ, сексуальне насильство являє собою широкий спектр примусових статевих актів [18], передбачає як безпосередньо докінчене діяння, так і замах на таке діяння, та охоплює будь-який

сексуальний акт або спробу залучення особи до таких дій без її згоди, зокрема небажані дії та зауваження, пов'язані із сексуальністю, незалежно від стосунків кривдника з жертвою чи умов, у яких це відбувається. Здебільшого в узгодженому міжнародному юридичному тлумаченні сексуальне насильство може мати різні форми, як-от сексуальні домагання, зґвалтування, спроби зґвалтування, принизливі сексуальні акти, недоречні дотики та небажані сексуальні зауваження.

Проявами сексуального насильства є сексуальна агресія, зґвалтування, сексуальне домагання, сексуальне рабство, примусові шлюби та інші дії сексуального характеру. За окремими дослідженнями, поширеність цього явища є дуже інтенсивною: приблизно 35 % респондентів протягом свого життя зазнавали зґвалтування, спроби зґвалтування чи інших форм сексуального насильства [19].

Також на міжнародному рівні констатовано, що небезпечний секс є другим за важливістю фактором ризику інвалідності та смерті в найбідніших громадах світу та дев'ятим за важливістю в розвинених країнах. Недоступними є дешеві ефективні методи запобігання небажаній вагітності, забезпечення безпечних абортів, допомоги жінкам під час вагітності та пологів, а також профілактики та лікування інфекцій, що передаються статевим шляхом. Статистика світового рівня вказує, що щороку понад 120 мільйонів пар незабезпечені належними контрацептивними засобами, 80 мільйонів жінок переживають небажану вагітність (45 мільйонів з яких закінчуються абортом), понад півмільйона жінок помирають від ускладнень, пов'язаних з вагітністю, пологами та післяпологовим періодом, а 340 мільйонів людей заражаються гонореєю, сифілісом, хламідіозом або трихомонадою [20].

Найбільше з проблемою насильства стикаються жінки та підлітки. Насильство щодо жінок є одним із найпоширеніших порушень прав людини, а також проблемою громадського здоров'я, яка потребує негайної уваги. Його

іноді називають гендерно зумовленим насильством, оскільки воно підтримується та, своєю чергою, увічнює гендерну нерівність, яка ставить жінок та дівчат у підлегле становище. Це насильство має багато руйнівних наслідків для життя та здоров'я жінок, включаючи їхнє сексуальне та репродуктивне здоров'я, а також безпосередньо порушують право людини на гідність.

Т.Сироїд зазначає, що «сексуальне і репродуктивне здоров'я жінок пов'язане з численними правами людини, в тому числі з правом на життя, правом на свободу від катувань, правом на охорону здоров'я, правом на недоторканність приватного життя, правом на освіту та забороною дискримінації, гарантованих Міжнародною хартією прав людини. Забезпечення цих прав є зобов'язанням держав.

Незважаючи на ці зобов'язання, порушення прав жінок на сексуальне і репродуктивне здоров'я є частими випадками. Вони приймають безліч форм, включаючи відмову в доступі до послуг, які потрібні тільки жінкам, або надання низької якості, залежність доступу жінок до послуг від дозволу третьої сторони, а також проведення процедур, пов'язаних з репродуктивним і сексуальним здоров'ям жінок, без їхньої згоди, в тому числі примусові стерилізації, примусовий огляд на предмет збереження незайманості і примусовий аборт. Права жінок у галузі сексуального і репродуктивного здоров'я також піддаються ризику в разі проведення операцій, що калічать жіночі геніталії, та у випадку ранніх шлюбів» [21].

В своєму докторському дисертаційному дослідженні І.Андрусяк зазначає, що «На поширеність сексуального насильства впливають і соціальні традиції побуту, оскільки спостереження такої поведінки від старших починає вважатися звичною поведінкою для людини, традиції й національно-ментальні стереотипи в подальшому можуть визначати поведінку у власній родині. Саме цим пояснюємо результати досліджень, проведених у різних регіонах нашої планети. В окремих культурно-групових суспільствах існує правило латентності такої

поведінки, сприйняття агресії, таким чином постраждалі особи не розуміють того, що проти них здійснено протиправну поведінку, часто вони виправдовують її чи сприймають як належну.» [22, с.182]

Репродуктивний примус та насильство, як і насильство з боку інтимного партнера, пов'язані з поганим психічним та сексуальним здоров'ям і порушують репродуктивні права людини. Вони проявляються в різних формах впливу на здоров'я, включаючи тяжкі симптоми посттравматичного стресового розладу та депресії, а також погіршення показників фізичного та сексуального здоров'я, таких як інфекції, що передаються статевим шляхом, незапланована вагітність та зниження сексуальної активності [23].

Науковці констатують, що досвід міжособистісного насильства значно відрізнявся залежно від сексуальної ідентичності. Контролюючи демографічні характеристики, порівняно з виключно гетеросексуальними жінками, переважно гетеросексуальні та бісексуальні жінки значно частіше повідомляли про фізичне, сексуальне та емоційне насильство. Переважно гетеросексуальні жінки та лесбійки частіше повідомляли про серйозне фізичне насильство. Переважно гетеросексуальні жінки більш ніж утричі частіше перебували у насильницьких стосунках протягом останніх трьох років, а всі три підгрупи сексуальних меншин у два-три рази частіше зазнавали домагань. Бісексуальні жінки повідомляли про значно вищий рівень депресії, ніж будь-яка інша група сексуальної ідентичності, та мали нижчі бали за психічним здоров'ям, ніж виключно гетеросексуальні жінки. У моделях лінійної регресії міжособистісне насильство сильно прогнозувало гірше психічне здоров'я лесбіянок та бісексуальних жінок. Переживання кількох видів міжособистісного насильства було найсильнішим предиктором стресу, тривоги та депресії. [24]

В умовах війни питання сексуального насильства отримує контекст можливих військових злочинів.

Стаття 54 Римського статуту надає повноваження прокуратурі приділяти особливу увагу сексуальному та гендерному насильству, насильству щодо дітей у своїх розслідуваннях і судових переслідуваннях. Ці злочини вважаються стратегічним пріоритетом для органів розслідування. Для виконання цього мандату розроблено сучасну політику щодо гендерних питань, яка зосереджена на актах СН, репродуктивного насильства та інших формах насильства за ознакою статі, які є злочинами згідно з Римським статутом [25]. Відповідно до цього документа, сексуальне насильство – це форма гендерно зумовленого насильства, яка полягає у вчиненні або спробі вчинення сексуальних дій, при цьому вкрай важливо, що останні набувають сексуального характеру навіть без фізичного контакту, наприклад, психологічне насильство, яке охоплює погрози зґвалтування або каліцтва статевих органів.

Окрема група сексуальних злочинів характеризується тим, що вони вчиняються як елемент воєнного впливу на протилежну сторону, її соціум. Це не просто кримінальне правопорушення, а саме залякування, пригнічення волі, геноцид цивільного населення. Безумовно, це суперечить нормам міжнародного гуманітарного права, дозволеним засобам і способам ведення бойових дій. Попри правову заборону такого насилля, у сучасних умовах, зокрема, російсько-української війни, воно досить поширене з боку країни-агресорки. За даними ООН, кількість випадків СН, пов'язаного з конфліктами, у 2023 році порівняно з 2022 роком збільшилася у півтора раза [26].

Отож, навіть коротких аналіз проблематики дає нам можливість прийти до висновку щодо необхідності комплексної правової концепції (державної стратегії) щодо репродуктивного здоров'я нації в Україні шляхом акценту на загрозах та можливостях боротьби з ними. Чільне місце в комплексі заходів боротьби має бути приділено боротьбі з військовими, інформаційними, дискримінаційними, гендерними, соціально-стереотипними, екологічними кризами, які як доведено суттєво впливають на репродукцію нації.

Провідними науковцями України (І Комарницька, В.Ковальчук та інші ) запропонований комплексний механізм протидії насильству у сфері репродуктивного здоров'ю:

- існування адміністративних, правових та кримінальних норм для протидії насильству (у більшості правових систем такі норми представлені у трьох групах: міжнародні; кримінальні; спеціальні);
- комплексна політика забезпечення репродуктивного здоров'я нації;
- комплекс каральних заходів у разі насильницьких дій [27].

Запропонований науковцями підхід є вагомим для подолання проблеми, оскільки охоплює базові складові державної політики у сфері протидії насильству та забезпечення репродуктивного здоров'я населення. Поєднання нормативно-правового регулювання, комплексної політики у сфері охорони репродуктивного здоров'я та застосування юридичної відповідальності до осіб, які вчиняють насильницькі дії, створює основу для функціонування системи захисту прав людини. Такий підхід відповідає сучасному розумінню ролі держави у забезпеченні безпеки громадян та формуванні умов для збереження здоров'я населення, оскільки насильство є не лише кримінально-правовою, а й медичною, соціальною, психологічною та демографічною проблемою.

Проте, на нашу думку, сучасні наукові дослідження та міжнародний досвід свідчать, що ефективна протидія насильству не може обмежуватися виключно застосуванням правових санкцій. Каральні механізми є важливим інструментом притягнення винних до відповідальності, однак вони переважно спрямовані на реагування на вже вчинене правопорушення. Натомість значно більшої уваги потребують заходи, спрямовані на попередження насильства, своєчасне виявлення його випадків та усунення факторів ризику, які сприяють його виникненню. Саме тому сучасна модель державної політики має базуватися на принципах превентивності, міжвідомчої взаємодії та комплексності.

Доцільним є розширення запропонованого підходу шляхом включення комплексу превентивних заходів. Насамперед йдеться про формування культури ненасильницької поведінки, утвердження принципів рівності, взаємної поваги та відповідального ставлення до репродуктивного здоров'я. Важливим напрямом є проведення інформаційно-просвітницьких кампаній серед населення, які мають сприяти підвищенню обізнаності щодо форм насильства, його наслідків, механізмів захисту прав постраждалих та доступних сервісів допомоги. Особливу роль у цьому процесі відіграють заклади освіти, які можуть формувати навички ненасильницької комунікації, відповідальної поведінки та гендерної рівності ще з раннього віку.

Окремого значення набуває система раннього виявлення випадків насильства. Практика багатьох держав свідчить, що саме своєчасна ідентифікація осіб, які перебувають у групі ризику або вже стали постраждалими, значно підвищує ефективність подальших заходів допомоги. У цьому процесі провідна роль належить працівникам закладів охорони здоров'я, сімейним лікарям, акушерам-гінекологам, психологам, педагогам, соціальним працівникам та правоохоронцям. Їхня підготовка повинна включати не лише знання законодавства, а й уміння розпізнавати ознаки фізичного, сексуального, психологічного чи економічного насильства, коректно взаємодіяти з постраждалими та забезпечувати їхнє скерування до відповідних служб підтримки.

Важливою складовою комплексного підходу є забезпечення доступності медичної допомоги постраждалим від насильства. Медичне втручання має бути спрямоване не лише на лікування отриманих ушкоджень, а й на профілактику довгострокових наслідків для репродуктивного здоров'я. До таких заходів належать своєчасне надання екстреної медичної допомоги, проведення необхідних лабораторних досліджень, профілактика інфекцій, що передаються статевим шляхом, застосування екстреної контрацепції у визначених

законодавством випадках, лікування гінекологічних та урологічних ускладнень, а також забезпечення подальшого медичного спостереження. Не менш важливим є надання психологічної підтримки, адже психоемоційні наслідки насильства нерідко є тривалими та безпосередньо впливають на репродуктивне здоров'я, перебіг вагітності, сексуальне життя та якість життя загалом.

Соціальна підтримка постраждалих також повинна бути невід'ємною складовою державної політики. Йдеться про забезпечення функціонування кризових центрів, спеціалізованих притулків, центрів психосоціальної допомоги, безоплатної правової допомоги, програм соціального супроводу та реінтеграції осіб, які постраждали від насильства. Ефективність такої підтримки значною мірою залежить від доступності відповідних послуг незалежно від місця проживання, матеріального становища чи соціального статусу людини. Особливої уваги потребують жінки репродуктивного віку, вагітні, діти, особи з інвалідністю та інші вразливі категорії населення.

Суттєвого вдосконалення потребує міжвідомча взаємодія між органами державної влади, закладами охорони здоров'я, правоохоронними органами, службами у справах дітей, органами соціального захисту, освітніми установами та громадськими організаціями. Саме координація їхньої діяльності забезпечує безперервність допомоги постраждалим, оперативний обмін інформацією, уникнення дублювання функцій та ефективніше використання наявних ресурсів. Важливим інструментом реалізації такого підходу є розроблення єдиних міжвідомчих алгоритмів реагування на випадки насильства, стандартизованих протоколів взаємодії та системи професійної підготовки фахівців різних сфер.

Не менш важливою складовою є розвиток системи професійної освіти та підвищення кваліфікації спеціалістів, які працюють із постраждалими. Медичні працівники, психологи, соціальні працівники, поліцейські, судді, прокурори та педагоги повинні регулярно проходити навчання щодо сучасних підходів до профілактики насильства, особливостей комунікації з постраждалими,

принципів дотримання конфіденційності, недопущення повторної травматизації та міждисциплінарної взаємодії. Це сприятиме підвищенню якості надання допомоги та формуванню довіри населення до державних інституцій.

В межах цього дослідження також вкажемо на те, що особливу увагу необхідно приділяти системі моніторингу та оцінювання ефективності державної політики у сфері протидії насильству. Регулярний аналіз статистичних даних, проведення епідеміологічних досліджень, вивчення причин і факторів ризику, оцінювання результативності профілактичних програм та якості наданих послуг дозволяють своєчасно виявляти проблемні аспекти та коригувати напрями державної політики. Науково обґрунтований моніторинг також створює передумови для розроблення нових програм, орієнтованих на реальні потреби населення.

Визначене вище, на нашу думку, доцільно розглядати як необхідний фундамент державної політики, однак його ефективність значно зросте за умови розширення до інтегрованої моделі, яка поєднує правові, медичні, психологічні, соціальні, освітні та профілактичні механізми. Правова політика повинна забезпечувати не лише своєчасне реагування на випадки насильства, а й усунення причин його виникнення, зменшення негативного впливу на репродуктивне здоров'я населення, підвищення рівня громадського здоров'я та зміцнення демографічного потенціалу держави. Саме комплексність, безперервність допомоги, міжвідомча координація та орієнтація на потреби постраждалих повинні стати основними принципами сучасної системи протидії насильству та охорони репродуктивного здоров'я.

***Висновки до Розділу 7***

Проведений нами комплексний аналіз проблем громадського , у тому числі репродуктивного здоров'я дає нам можливість прийти до таких висновків.

1. Категорія громадського здоров'я є цінною соціально-правовою аксіологемою, що включає комплекс соціальних відносин особистісного,

соматичного та суспільно-комунікаційного й державного рівнів та спрямоване на забезпечення права людини на життя, здоров'я та забезпечення належного рівня добробуту.

Цей інститут націлений на формування належного рівня здоров'я населення, профілактику захворювань, мінімізацію ризиків для життя і здоров'я людини та створення безпечного середовища її існування. У сучасних умовах питання громадського здоров'я виходить за межі виключно медичної сфери, набуваючи значення одного із пріоритетних напрямів державної правової політики та складової національної безпеки.

Розглядуваний теоретико-правовий концепт безапеляційно поєднаний з ефективністю функціонування системи громадського здоров'я та передбачає існування комплексного механізму правових, організаційних, економічних, інформаційних та інституційних заходів. Водночас сучасний стан правового регулювання характеризується низкою системних проблем, серед яких фрагментарність нормативної бази, недостатня міжвідомча координація, нерівний доступ населення до медичних послуг, недостатній рівень цифрової трансформації медичної сфери, а також наявність прогалин у правовому регулюванні новітніх біомедичних технологій.

Особливої актуальності набуває необхідність забезпечення рівного доступу до медичної допомоги як одного з фундаментальних елементів права людини на охорону здоров'я. Реалізація цього права повинна ґрунтуватися на принципах верховенства права, недискримінації, соціальної справедливості, гендерної рівності та людиноцентризму із врахуванням потреб найбільш вразливих категорій населення.

Сучасні глобальні виклики, пов'язані з пандеміями, розвитком біотехнологій, цифровізацією охорони здоров'я та повномасштабною збройною агресією проти України, зумовлюють необхідність перегляду традиційних підходів до державної політики у сфері громадського здоров'я. Пріоритетного

значення набувають формування резистентної системи охорони здоров'я, розвиток превентивної медицини, удосконалення механізмів кризового управління, забезпечення медико-біологічної безпеки, цифрового захисту медичних даних та гарантування безперервності надання медичної допомоги навіть в умовах надзвичайних ситуацій.

2. Репродуктивне здоров'я є невід'ємною складовою громадського здоров'я та одним із ключових об'єктів правового забезпечення у сфері охорони здоров'я населення. Його зміст не обмежується виключно медичним аспектом, а охоплює систему правових, соціальних, етичних та організаційних гарантій, спрямованих на забезпечення фізичного, психічного і соціального благополуччя людини у сфері репродукції. Міжнародні стандарти, насамперед положення Програми дій Міжнародної конференції з питань народонаселення та розвитку, Цілі сталого розвитку ООН та міжнародні акти у сфері прав людини, визначають репродуктивне здоров'я як невід'ємний елемент людської гідності, права на охорону здоров'я, приватність, сімейне життя та свободу репродуктивного вибору. Відповідно, державна політика у цій сфері повинна забезпечувати комплексний підхід, який поєднуватиме ефективне правове регулювання, доступність медичних послуг, розвиток репродуктивної освіти та гарантування реалізації репродуктивних прав кожної особи.

Для України проблема збереження репродуктивного здоров'я нації набуває особливої актуальності в умовах повномасштабної війни, демографічної кризи та погіршення психоемоційного стану населення. Хронічний стрес, вимушене переміщення, погіршення доступності медичної допомоги та інші наслідки збройної агресії безпосередньо впливають на репродуктивний потенціал населення, що зумовлює необхідність формування комплексної державної політики, спрямованої на його збереження та відновлення. За таких умов охорона репродуктивного здоров'я повинна розглядатися не лише як складова медичної

політики, а і як один із пріоритетних напрямів забезпечення демографічної безпеки, людського капіталу та сталого розвитку Української держави.

3. Проведений аналіз дає підстави стверджувати, що забезпечення рівного доступу до реалізації репродуктивних прав є однією з ключових гарантій дотримання принципів верховенства права, людської гідності, недискримінації та фактичної рівності. Репродуктивні права мають комплексний характер і перебувають на перетині особистих немайнових прав, права на охорону здоров'я, права на приватне і сімейне життя та права на свободу від дискримінації. Відтак їх належна реалізація потребує не лише формального нормативного закріплення, але й створення державою ефективних механізмів рівного доступу до відповідних медичних, інформаційних та соціальних послуг.

Дослідження свідчать, що сучасні виклики у сфері реалізації репродуктивних прав мають переважно не нормативний, а фактичний характер. Незважаючи на міжнародно-правове закріплення принципу рівності та заборони дискримінації, істотний вплив на доступ до репродуктивних послуг продовжують справляти соціально-економічний статус особи, стать, місце проживання, рівень освіти, фінансова спроможність, культурні стереотипи, міграційний статус, а також наслідки збройних конфліктів. Така ситуація свідчить про необхідність переходу від формальної рівності до забезпечення рівності можливостей шляхом застосування позитивних зобов'язань держави.

Особливої уваги потребує впровадження гендерно чутливої правової політики, яка повинна ґрунтуватися на визнанні спільної відповідальності жінки і чоловіка за реалізацію репродуктивної функції. Правове регулювання має відходити від традиційної моделі покладення основного тягаря репродуктивної відповідальності виключно на жінку та формувати комплексний підхід, що передбачає рівноправну участь обох партнерів у питаннях планування сім'ї, підготовки до батьківства та охорони репродуктивного здоров'я.

Окремого нормативного реагування потребують випадки множинної (інтерсекційної) дискримінації, коли обмеження реалізації репродуктивних прав зумовлене одночасною дією декількох дискримінаційних факторів. Практика свідчить, що найбільш уразливими залишаються жінки із сільської місцевості, особи з низьким рівнем доходів, внутрішньо переміщені особи, мігранти, біженці, особи з інвалідністю та населення територій, які постраждали від воєнних дій.

В умовах збройної агресії проти України проблема рівного доступу до реалізації репродуктивних прав набуває додаткового правового виміру. Воєнний стан істотно ускладнює доступ до медичних послуг, підвищує ризики сексуального насильства, вимушеної міграції, порушення права на безпечне материнство та безперервність медичного супроводу вагітності. За таких умов держава відповідно до своїх конституційних та міжнародно-правових зобов'язань повинна забезпечити функціонування ефективних механізмів безперервного надання репродуктивної медичної допомоги незалежно від місця перебування особи, її соціального статусу чи інших індивідуальних характеристик.

4. Насильство є одним із найбільш небезпечних чинників, що негативно впливає на репродуктивне здоров'я населення, порушує фундаментальні права людини, підриває демографічний потенціал держави та створює довгострокові медичні, психологічні, соціальні й правові наслідки. Сексуальне та гендерно зумовлене насильство, репродуктивний примус, насильство з боку інтимного партнера становлять комплексні загрози не лише для окремої особи, а й для громадського здоров'я загалом. У зв'язку з цим протидія насильству повинна розглядатися як один із пріоритетних напрямів державної політики у сфері охорони репродуктивного здоров'я та забезпечення прав людини.

Ефективне вирішення зазначеної проблеми можливе лише за умови формування комплексної правової моделі, яка поєднуватиме превентивні,

медичні, соціальні, психологічні та юридичні механізми захисту. Поряд із удосконаленням законодавства та забезпеченням невідворотності юридичної відповідальності необхідно розвивати систему раннього виявлення випадків насильства, підвищувати доступність спеціалізованої медичної й психологічної допомоги, забезпечувати ефективну міжвідомчу взаємодію та здійснювати системну інформаційно-просвітницьку діяльність. На нашу думку, комплексний, людиноцентричний підхід, заснований на принципах верховенства права, поваги до людської гідності, недискримінації та міжнародних стандартах захисту прав людини, здатний забезпечити ефективну протидію насильству, мінімізувати його негативний вплив на репродуктивне здоров'я нації та сприяти зміцненню громадського здоров'я України.

## Список використаних джерел

1. Сергата Є. В. Особливості нормативно-правових актів, що гарантують медичне забезпечення співробітників МВС в мирний та воєнний час. *Україна. Здоров'я нації.* 2024. № 4. С. 31–37.

2. Показники здоров'я населення та діяльності закладів охорони здоров'я м. Одеси за 2015–2016 рр. Одеса, 2017. 333 с.

3. Лемеха Р. І. Медичне право України як галузь права, наука та навчальна дисципліна: теоретико-правовий підхід. *Право і суспільство*. 2022. № 5. С. 40–45.

4. Децик О. З. Порівняльна характеристика законодавства про громадське здоров'я в Польщі та Україні. *Україна. Здоров'я нації*. 2017. № 3. С. 318–322. URL: http://nbuv.gov.ua/UJRN/Uzn_2017_3_65 (дата звернення: 08.07.2026).

5. Ren J., Esce A. Ethics in Practice: Autonomy and Shared Decision-Making. *AAO-HNS Bulletin*. 2024. Nov. 14. URL: https://bulletin.entnet.org/clinical-patient-

care/article/22926489/ethics-in-practice-autonomy-and-shared-decisionmaking (date of access: 08.07.2026).

6. Пономарьова О. О. Правове регулювання права на медичне зображення: порівняльно-правовий аналіз. *Аналітично-порівняльне правознавство*. 2025. № 4 (3). С. 510–518.

7. Галайко А. Право на посмертну репродукцію і репродуктивне здоров'я нації. *Право людини на мир: доктрина та сучасні проблеми правового забезпечення*: матеріали міжнародної правової школи (м. Ужгород, 30 січня 2025 р.). С. 35-39.

8. Malachinska M. Problems of access to healthcare services in the armed conflict zones: Literature review. *Reproductive Endocrinology*. 2024. Vol. 73. P. 8–13. DOI: https://doi.org/10.18370/2309-4117.2024.73.8-13.

9. Shevtsova A. V. Medical and psychological rehabilitation of military personnel, their family members, and the civilian population: a theoretical and legal analysis. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 91, ч. 3. С. 263–267.

10. Берч В. В. Соматичні права та медичне право: питання захисту гідності та автономії. *Аналітично-порівняльне правознавство*. 2023. № 5. С. 92–95.

11. Ren J., Esce A. Ethics in Practice: Autonomy and Shared Decision-Making. *AAO-HNS Bulletin*. 2024. Nov. 14. URL: https://bulletin.entnet.org/clinical-patient-care/article/22926489/ethics-in-practice-autonomy-and-shared-decisionmaking (date of access: 08.07.2026).

12. Semahegn A., Tiruneh G. T., Mirkuzie A. et al. Gender dynamics affecting women's uptake of maternal health service in agrarian and pastoral settings in Ethiopia: a community-based cross-sectional study. *Reproductive Health*. 2026. Vol. 23. Art. 98. DOI: https://doi.org/10.1186/s12978-026-02325-w.

13. Osborne A., James P. B., Bangura C. Determinants of poor access to health care among women of reproductive age in Sierra Leone: a cross-sectional study. *BMC*

*Health Services Research*. 2025. Vol. 25. Art. 211. DOI: https://doi.org/10.1186/s12913-025-12363-y.

14. Hickman M. E., Khare M., Schoenaker D. et al. Gender norms and responsibility for preconception health improvement: challenges and recommendations for action from the 2024 UK preconception EMCR network conference. *Reproductive Health*. 2026. DOI: https://doi.org/10.1186/s12978-026-02402-0.

15. WHO recommendations on adolescent sexual and reproductive health and rights. Geneva: World Health Organization, 2018. 88 p. URL: https://apps.who.int/iris/bitstream/handle/10665/275374/9789241514606-eng.pdf?ua=1 (date of access: 08.07.2026).

16. Manian M. Immigration detention and coerced sterilization: History tragically repeats itself. *ACLU*. 2020. Sept. 29. URL: https://www.aclu.org/news/immigrants-rights/immigration-detention-and-coerced-sterilization-history-tragically-repeats-itself/ (date of access: 08.07.2026).

17. Zharovska I. Discrimination in Ensuring the Nation's Public Health. *Veritas: Legal and Psychological-Pedagogical Research*. 2025. Vol. 1, No. 1. P. 10–16. DOI: https://doi.org/10.23939/veritas2025.01.010.

18. Pan American Health Organization. Understanding and addressing violence against women: intimate partner violence. Geneva : World Health Organization, 2012. URL: https://apps.who.int/iris/handle/10665/77432 (date of access: 08.07.2026).

19. Ellsberg M., Ovince J., Murphy M., Blackwell A., Reddy D., Stennes J., Hess T., Contreras M. No safe place: Prevalence and correlates of violence against conflict-affected women and girls in South Sudan. *PLOS One*. 2020. Vol. 15, No. 10. DOI: https://doi.org/10.1371/journal.pone.0237965.

20. Glasier A., Gülmezoglu A. M., Schmid G. P., Moreno C. G., Van Look P. F. Sexual and reproductive health: a matter of life and death. *The Lancet*. 2006. Vol. 368, No. 9547. P. 1595–1607.

21. Сироїд Т. Г. Міжнародно-правові основи захисту сексуального та репродуктивного здоров'я жінок. *Juris Europensis Scientia*. 2020. № 3. С. 151–155.

22. Андрусяк І. П. Запобігання та протидія домашньому насильству: теоретико-правове дослідження : дис. ... д-ра юрид. наук : 12.00.01. Львів : Національний університет «Львівська політехніка», 2024. 582 с. URL: https://lpnu.ua/sites/default/files/2024/dissertation/29132/disertaciya-andrusyak.pdf (дата звернення: 08.07.2026).

23. Sheeran N., Vallury K., Sharman L. S. et al. Reproductive coercion and abuse among pregnancy counselling clients in Australia: Trends and directions. *Reproductive Health*. 2022. Vol. 19, No. 1. Art. 170. DOI: https://doi.org/10.1186/s12978-022-01479-7.

24. Szalacha L. A., Hughes T. L., McNair R. et al. Mental health, sexual identity, and interpersonal violence: Findings from the Australian Longitudinal Women's Health Study. *BMC Women's Health*. 2017. Vol. 17. Art. 94. DOI: https://doi.org/10.1186/s12905-017-0452-5.

25. International Criminal Court Office of the Prosecutor. Crimes involving sexual, reproductive, and other gender-based violence: Policy on Gender-Based Crimes. 2023. URL: https://www.icc-cpi.int/sites/default/files/2023-12/2023-policy-gender-en-web.pdf (date of access: 08.07.2026).

26. Соломко І. Від сексуального насильства в Україні торік постраждали 52 чоловіки, 31 жінка і двоє дітей – звіт ООН. *Голос Америки*. 2024. 24 квіт. URL: https://www.holosameryky.com/a/oon_sexualne_nasylstvo_viyna_zvit/7581867.html (дата звернення: 08.07.2026).

27. Kovalchuk V., Komarnytska I. I., Rizenko O., Pasternak V., Kostiukova I. Public health of the nation and reproductive violence. *Reproductive Endocrinology*. 2025. No. 76. P. 57–64. DOI: https://doi.org/10.18370/2309-4117.2025.76.57-64.

# РОЗДІЛ 8
# КЛІНІЧНЕ ЗАСТОСУВАННЯ ТРИВИМІРНОГО МОДЕЛЮВАННЯ В МЕДИЦИНІ

**Автори:**

**Романюк Олександр Никифорович,** *доктор технічних наук, професор*

*Завідувач кафедри программного забезпечення, Вінницький національний технічний університет;*

**Павлов Сергій Володимирович,** *доктор технічних наук, професор, професор кафедри біомедичної інженерії та оптико-електронних систем, Вінницький національний технічний університет***;**

**Денищич Людмила Петрівна,** *кандидат медичних наук, доцент, Вінницький національний медичний університет імені М.І. Пирогова;*

**Майданюк Володими Павлович,** *кандидат технічних наук, доцент кафедри программного забезпечення, Вінницький національний технічний університет*

Тривимірне моделювання стало одним із важливих інструментів персоналізованої медицини, оскільки дає змогу відтворювати органи, патологічні утворення й функціональні процеси конкретного пацієнта. Поняття тривимірної моделі охоплює цифрову реконструкцію, фізичний об’єкт, надрукований пошаровим способом, віртуальне операційне поле та основу для комп’ютерної симуляції. Вихідними даними є серії КТ, МРТ, ультразвукової й ангіографічної візуалізації, конусно-променевої томографії або оптичного сканування. Після сегментації потрібних структур створюють просторову сітку, перевіряють її геометрію та використовують для вимірювань, планування, навігації, виготовлення шаблонів чи індивідуальних виробів.

Клінічна цінність визначається не видовищністю об’ємного зображення, а його здатністю відповідати на конкретне діагностичне або лікувальне запитання. Найбільший ефект технологія має у спеціальностях, де складна просторова анатомія безпосередньо впливає на ризик втручання: кардіології, онкології, травматології та ортопедії, нейрохірургії, стоматології й щелепно-лицевій хірургії. Модель доповнює стандартний аналіз томограм, підтримує міждисциплінарне обговорення та дозволяє випробувати варіанти лікування до їх реалізації. Водночас якість результату залежить від первинних зображень, коректності сегментації, клінічної верифікації й прозорого позначення невизначеності; повноцінні цифрові двійники та біодрук поки переважно залишаються напрямами контрольованого дослідження.

### 8.1. Використання тривимірного моделювання в кардіології

У кардіології тривимірне моделювання особливо цінне через складну геометрію серця, постійну рухливість його структур і тісний функціональний зв’язок між анатомією та гемодинамікою. Звичайні двовимірні зрізи КТ або МРТ містять повну інформацію про досліджуваний об’єм, однак лікареві доводиться подумки відновлювати взаємне розташування камер, клапанів, магістральних судин і дефектів. Просторова реконструкція переносить цю розумову операцію в цифрове середовище, де модель можна обертати, розсікати довільними площинами, робити прозорою, вимірювати та зіставляти з майбутнім пристроєм. Для отримання моделі використовують кардіосинхронізовану КТ, МРТ серця, тривимірну ехокардіографію та ангіографічні дані; вибір методу залежить від того, чи потрібно детально відобразити кальциновані структури, м’які тканини, рух клапанів або судинний просвіт [1, с. 1-5].

Одним із найпереконливіших напрямів є планування лікування вроджених вад серця. За складних поєднань дефектів міжшлуночкової перегородки, аномалій відходження великих судин, однокамерної гемодинаміки або повторних операцій просторові відношення часто не вкладаються у стандартні

схеми. Персоналізована модель дає змогу оцінити, чи достатній внутрішньосерцевий простір для формування тунелю, яким буде його напрямок, чи не виникне компресії вихідного тракту та як розташовані коронарні артерії відносно запланованої лінії розрізу. У дитячій кардіохірургії фізична модель корисна ще й тим, що її можна оглянути з боку хірургічного доступу, відпрацювати послідовність маніпуляцій і узгодити план між кардіологом, радіологом, хірургом та анестезіологом. Це не скасовує аналізу вихідних зображень, але зменшує ризик різного трактування складної анатомії.

У структурній кардіології моделі застосовують під час підготовки транскатетерної імплантації аортального клапана, втручань на мітральному й тристулковому клапанах, закриття вушка лівого передсердя, параклапанних витоків і дефектів перегородок. Цифрова реконструкція дозволяє визначити розміри фіброзного кільця, висоту відходження коронарних артерій, обсяг і розподіл кальцифікації, кут аорти, конфігурацію вихідного тракту лівого шлуночка та можливі зони зіткнення пристрою з тканинами. Для мітральних втручань особливе значення має оцінка сідлоподібної форми кільця, взаємодії стулок і підклапанного апарату. Віртуальне розміщення протеза або оклюдера допомагає порівняти кілька типорозмірів, передбачити неповне прилягання, обструкцію чи компресію сусідніх структур і тим самим зробити вибір пристрою більш обґрунтованим .

Фізичний 3D-друк додає тактильний компонент і особливо корисний там, де необхідно відпрацювати доставку пристрою або перевірити його взаємодію зі складною геометрією. Жорсткі моделі добре відтворюють кісткові чи кальциновані елементи, проте для клапанів і судин потрібні еластичні полімери, здатні хоча б наближено імітувати деформацію тканини. На такій моделі можна випробувати розкриття стент-клапана, орієнтацію катетера, герметичність оклюдера або траєкторію доступу. Однак механічна подібність не є автоматичною: матеріал може правильно відтворювати форму, але не мати

відповідної товщини, анізотропії та в'язкоеластичних властивостей. Тому результати стендової симуляції слід трактувати як додаткову інформацію, а не як абсолютний прогноз поведінки живої тканини.

Окремий клас становлять обчислювальні моделі, у яких анатомічна геометрія поєднується з механікою рідини та твердого тіла. На основі КТ, МРТ або ехокардіографії можна побудувати пацієнт-специфічний домен для чисельного моделювання кровотоку, оцінити поля швидкості, тиску, зсувного напруження, турбулентність і зони застою. Такі підходи досліджують при коарктації аорти, аневризмах, складних шунтах, патології клапанів, коронарних стенозах та після реконструктивних операцій. Їхня перевага полягає у переході від опису форми до прогнозу функції: можна порівнювати різні діаметри протеза, варіанти анастомозу або кути імплантації. Водночас точність залежить від граничних умов, властивостей стінки, часової роздільної здатності та припущень моделі, тому клінічне використання потребує валідації на незалежних вимірюваннях.

У електрофізіології тривимірні реконструкції поєднують з картуванням електричної активності. Геометрія передсердь і шлуночків, рубцевих зон, легеневих вен та коронарного синуса допомагає планувати абляцію, а злиття передопераційної КТ або МРТ з електроанатомічною картою покращує просторову орієнтацію. Для складних шлуночкових тахікардій модель може показати товщину міокарда, післяінфарктний рубець, аневризму і близькість коронарних судин. Перспективним є моделювання поширення збудження та персоналізований прогноз ефекту абляційних ліній, однак електрофізіологічна поведінка серця визначається не лише геометрією, а й клітинними властивостями, фіброзом, автономною регуляцією та медикаментозним впливом. Саме тому повноцінна електрична модель потребує інтеграції даних кількох рівнів.

Важливою сферою є оцінка коронарних артерій та аорти. Тривимірна модель полегшує розуміння аномального відходження коронарної артерії, її проходження між аортою і легеневим стовбуром, складних хронічних оклюзій, біфуркаційних уражень та взаємного розташування гілок перед повторною операцією. Для аневризм і розшарувань аорти реконструкція показує протяжність ураження, істинний і хибний просвіти, відходження вісцеральних гілок та придатність зон фіксації ендопротеза. У поєднанні з внутрішньосудинними даними вона може підтримувати вибір довжини стент-графта і конфігурації фенестрацій. Проте артефакти руху, недостатнє контрастування дрібних гілок і помилки порогової сегментації здатні змінити геометрію просвіту, тому критичні вимірювання мають перевірятися на вихідних зрізах.

Тривимірні моделі використовують не лише для прийняття рішень, а й для навчання. Симулятори катетеризації, коронарографії, клапанних втручань і хірургічних доступів дозволяють багаторазово відпрацьовувати техніку без ризику для пацієнта. Пацієнт-специфічний симулятор особливо корисний перед рідкісною або нестандартною процедурою, коли типові тренажери не відтворюють необхідну анатомію. Для студентів і лікарів модель полегшує формування просторового мислення, а для пацієнта стає зрозумілим засобом пояснення вади, запланованої операції та потенційних обмежень. Комунікаційна функція не є другорядною: краще розуміння може підтримувати усвідомлену згоду, однак демонстрація моделі повинна супроводжуватися поясненням, що вона є спрощеним представленням, а не точною копією всіх властивостей органа.

Розвиток доповненої, віртуальної та змішаної реальності дає змогу працювати з моделлю без фізичного друку. Хірург може бачити напівпрозоре серце, приховувати окремі шари, вимірювати відстані, спільно переглядати модель з колегами та накладати її на операційне поле. Перевагами є швидкість оновлення, відсутність витрат матеріалу і можливість відображати рух у часі.

Недоліками залишаються залежність від точності реєстрації, затримка системи, обмежене поле зору та відсутність тактильного відчуття. У кардіології, де орган рухається і змінює форму протягом циклу, статичне накладання швидко втрачає відповідність, тому найбільш перспективними є моделі, синхронізовані з фазою серцевого циклу та інтраопераційною візуалізацією.

Отже, клінічна роль тривимірного моделювання в кардіології полягає у поєднанні анатомічної наочності, кількісної оцінки та попереднього випробування втручання. Найбільш зрілими є застосування у складних вроджених вадах, структурних процедурах, аортальній патології та навчанні. Подальше поширення залежить від стандартизації сегментації, доказів впливу на значущі клінічні результати, скорочення часу підготовки моделей і чіткого контролю якості. Огляд сучасних кардіоваскулярних застосувань підкреслює, що технологія вже вийшла за межі демонстраційних прототипів, але її користь найбільша тоді, коли модель створюється для визначеного рішення і перевіряється фахівцями, відповідальними за це рішення [1, с. 1-6].

### 8.2. Застосування у діагностиці онкологічних захворювань

В онкології тривимірне моделювання виконує подвійну функцію: воно допомагає просторово охарактеризувати пухлину в організмі та створює інженерні платформи для виявлення біомаркерів, дослідження пухлинного мікрооточення і прогнозування відповіді на лікування. У клінічній візуалізації вихідними даними є КТ, МРТ, ПЕТ/КТ, ПЕТ/МРТ, ультразвукові дослідження та, за потреби, цифрова патологія. Сегментація дозволяє відокремити первинне утворення, метастази, зони некрозу, судини, протоки й критичні органи. На відміну від простого об’ємного рендерингу, персоналізована модель може бути основою для точного вимірювання об’єму, площі контакту, просторової неоднорідності та динаміки під час серійних обстежень. Таке подання не замінює морфологічного підтвердження діагнозу, але доповнює стадіювання і передопераційну оцінку [2, с. 1-12].

Найочевидніша перевага полягає у відтворенні взаємовідношень пухлини з судинами та функціонально важливими структурами. Для утворень печінки модель може одночасно показувати портальні й печінкові вени, жовчні протоки, сегментарну будову та передбачуваний залишковий об'єм паренхіми. У нирковій онкології вона демонструє положення пухлини відносно чашково-мискової системи й ниркових судин; у легеневій - бронхосудинну анатомію сегмента; у пухлинах підшлункової залози - контакт із верхньою брижовою артерією, веною та ворітною веною. Така реконструкція допомагає уточнити технічну резектабельність, вибрати межі резекції, оцінити потребу в судинній реконструкції та сформувати спільне розуміння випадку на мультидисциплінарному консиліумі.

Для діагностичної інтерпретації важливим є не лише зовнішній контур новоутворення, а й його внутрішня гетерогенність. Різні ділянки пухлини можуть мати неоднакове контрастування, перфузію, дифузію, метаболічну активність і клітинність. Тривимірне картування таких ознак формує так звані просторові фенотипи або середовища пухлини, які можуть бути пов'язані з агресивністю, гіпоксією, некрозом і стійкістю до терапії. Радіомічні алгоритми перетворюють сегментований об'єм на набір кількісних ознак форми й текстури, а машинне навчання шукає зв'язок із гістологією, мутаційним профілем або прогнозом. Проте ці моделі чутливі до протоколу сканування, реконструкції зображення та способу сегментації, тому перед клінічним застосуванням потребують зовнішньої валідації та оцінки відтворюваності.

Тривимірне моделювання підтримує планування біопсії, особливо коли пухлина містить некротичні або неоднорідні ділянки. Поєднання морфологічних і функціональних зображень допомагає обрати мішень із найвищою ймовірністю отримання діагностичного матеріалу та уникнути великих судин, плеври, кишки чи інших небезпечних структур. У нейроонкології просторове суміщення МР-перфузії, спектроскопії, дифузійних даних і трактографії може визначати

найбільш інформативну зону для стереотаксичної біопсії. У кісткових пухлинах модель допомагає спланувати канал біопсії так, щоб він надалі був видалений разом із препаратом і не забруднював майбутній реконструктивний доступ. Водночас будь-яка навігація залежить від точності реєстрації та не повинна підміняти інтраопераційний контроль положення інструмента.

Під час хірургічного лікування модель перетворює діагностичну інформацію на план резекції. Вона дає змогу порівнювати органозберігаючі та розширені втручання, прогнозувати дефект і заздалегідь проєктувати реконструкцію. Показовим є досвід використання 3D-реконструкції при поширеному раку яєчника, де необхідно оцінити множинне ураження очеревини та близькість пухлинних конгломератів до кишки, сечоводів, великих судин і діафрагми. У ретроспективному дослідженні 60 пацієнток групи з тривимірною візуалізацією та з поєднанням візуалізації і друку мали коротшу тривалість операції та меншу крововтрату порівняно з оцінкою лише за двовимірними КТ-зображеннями. Водночас відмінностей у частоті рецидивів і загальних післяопераційних ускладнень переконливо не показано, що підкреслює потребу в більших проспективних дослідженнях [3, с. 1-10].

У променевій терапії тривимірна модель є основою окреслення мішені та органів ризику, розрахунку дозового розподілу і контролю положення пацієнта. Адитивне виробництво розширює ці можливості завдяки індивідуальним болюсам, фіксаторам, фантомам і аплікаторам для брахітерапії. Надрукований болюс може точніше повторювати складний контур шкіри, зменшуючи повітряні проміжки, а персоналізований аплікатор допомагає стабілізувати геометрію джерела відносно пухлини. Для перевірки плану друкують антропоморфні фантоми з матеріалів, підібраних за рентгенівською щільністю. Однак клінічна безпека вимагає дозиметричної перевірки кожного нового матеріалу й технології, оскільки внутрішня пористість, напрямок друку та нестабільність складу можуть змінювати ослаблення випромінювання.

Інший напрям стосується діагностичних пристроїв, створених методами 3D-друку. Мікрофлюїдні чипи, сенсорні масиви, тримачі для оптичних та електрохімічних детекторів можуть бути швидко адаптовані до конкретного біомаркера або набору біомаркерів. Геометрія каналів і реакційних камер визначає змішування, час контакту та концентрацію аналіту, а пошарове виробництво дозволяє інтегрувати кілька функцій в одному компактному пристрої. Такі системи досліджують для аналізу циркулюючих пухлинних клітин, нуклеїнових кислот, білків та метаболітів. Огляд онкологічних застосувань підкреслює потенціал швидкого прототипування й персоналізації, але також наголошує, що 3D-друк поки не замінює валідовані лабораторні методи, а повинен проходити аналітичну та клінічну верифікацію [2, с. 1].

Отже, у діагностиці онкологічних захворювань тривимірне моделювання найбільш корисне для просторового опису пухлини, оцінки резектабельності, вибору мішені для біопсії, планування променевої терапії та створення персоналізованих діагностичних платформ. Його перевагою є інтеграція різнорідних даних у наочну й вимірювану модель, а обмеженням – залежність від якості сегментації та ризик хибної впевненості в геометричній точності. Тому клінічний файл має містити відомості про джерело даних, часову точку, метод сегментації й межі невизначеності.

### 8.3. Тривимірне моделювання у травматології та ортопедії

У травматології та ортопедії тривимірне моделювання набуло широкого поширення завдяки високій контрастності кісткової тканини на КТ і безпосередньому зв’язку між геометрією та механічною функцією. Для складного перелому просторова реконструкція показує кількість і положення фрагментів, напрямок ліній перелому, ступінь імпресії суглобової поверхні та співвідношення з судинно-нервовими структурами. Особливо корисними є моделі таза, кульшової западини, плато великогомілкової кістки, проксимального відділу плечової кістки, стопи та хребта, де звичайна

рентгенографія або окремі зрізи не завжди дають цілісне уявлення. Модель можна «розібрати» на фрагменти, виконати віртуальну репозицію й порівняти кілька варіантів фіксації до операції.

Передопераційне планування включає визначення доступу, послідовності репозиції, положення пластини, довжини й напрямку гвинтів. Фізична копія кістки дозволяє попередньо контурювати стандартну пластину, що скорочує маніпуляції в рані та зменшує багаторазове згинання імплантата. Цифрове середовище дає змогу моделювати остеотомію, дзеркально відновлювати пошкоджену ділянку за контралатеральною стороною та оцінювати вісь кінцівки. Для деформацій після неправильного зрощення це особливо важливо: хірург може визначити центр деформації, кут і площину корекції, а потім перенести план за допомогою індивідуального різального або свердлильного шаблона.

Пацієнт-специфічні навігаційні шаблони фіксуються на унікальній поверхні кістки й задають напрямок свердління, резекції або встановлення компонента. Їх застосовують у коригувальних остеотоміях, ендопротезуванні, операціях на хребті, резекції пухлин і реконструкції великих дефектів. Перевагою є перенесення цифрового плану в операційну без складної оптичної навігації; обмеженням - залежність від точного прилягання. Якщо під час сегментації не враховано остеофіт, якщо поверхня змінилася після видалення м’яких тканин або шаблон встановлено з перекосом, траєкторія може бути неправильною. Тому дизайн повинен передбачати однозначну посадку, контрольні вікна й інтраопераційну перевірку.

В ендопротезуванні тривимірна модель допомагає оцінити кістковий запас, деформацію, центри ротації та взаємну орієнтацію компонентів. При складній ревізії кульшового суглоба вона показує розміри дефекту вертлюжної западини, положення колон і можливі зони опори для аугментів або індивідуального компонента. У колінному суглобі цифрове планування пов’язують з

відновленням механічної осі, ротаційним позиціонуванням і балансом м'яких тканин. Для молодих пацієнтів з пухлинними або посттравматичними дефектами застосовують індивідуальні пористі імплантати з титанових сплавів, геометрія яких відповідає дефекту, а внутрішня решітчаста структура сприяє зменшенню маси й потенційній остеоінтеграції.

Доказова база найкраще сформована для 3D-друкованих моделей і шаблонів у лікуванні переломів. Узагальнюючий огляд 2025 року, який проаналізував систематичні огляди та метааналізи, показав переваги 3D-друк-асистованої хірургії щодо тривалості операції, крововтрати та частини післяопераційних ускладнень у низці локалізацій. Для окремих переломів також відзначено кращі функціональні або рентгенологічні показники. Водночас автори звертають увагу на високу статистичну неоднорідність, відмінності технологій і якість первинних досліджень. Отже, позитивний середній ефект не означає однакової користі для кожного типу перелому; найбільш виправданим є застосування в анатомічно складних випадках, де модель реально змінює план операції [4, с. 1-9].

У хірургії хребта тривимірна реконструкція використовується для оцінки ніжок дуг, ротації хребців, вроджених аномалій, пухлин і посттравматичних деформацій. Віртуальне проведення гвинта дозволяє заздалегідь визначити діаметр, довжину та безпечний коридор, а шаблон може спрямовувати інструмент під час встановлення. Водночас хребет є рухомою багатосегментарною системою: положення пацієнта під час передопераційної КТ та на операційному столі відрізняється, а декомпресія або остеотомія змінює геометрію. Тому статичний шаблон не повинен створювати ілюзію повної навігаційної незалежності; у складних випадках його поєднують з флюороскопією, інтраопераційною КТ або оптичною навігацією.

Тривимірне моделювання також підтримує лікування ортопедичних пухлин. За допомогою МРТ визначають м'якотканинний і внутрішньокістковий компонент, за КТ - кортикальну структуру, після чого дані суміщають для

планування меж резекції. Віртуальна остеотомія допомагає зберегти максимально можливий обсяг здорової кістки й суглобову поверхню, а друкований шаблон відтворює обрану площину. Після резекції дефект може бути реконструйований алотрансплантатом, модульним протезом або індивідуальним імплантатом. Критично важливо закладати онкологічний запас і враховувати похибку реєстрації: геометрична точність не може бути досягнута ціною недостатньої радикальності.

Основними бар'єрами залишаються час сегментації, вартість, стерилізація, відповідальність за дизайн і різниця між віртуальною та реальною механікою. Кістка на моделі може бути геометрично точною, але її міцність, якість кортикального шару та остеопороз відтворюються обмежено. Для імплантатів необхідні контроль сировини, параметрів друку, термічної обробки, поверхні та втомної міцності. Тому клінічне впровадження має будуватися як керований виробничо-медичний процес із простежуваністю даних, перевіркою розмірів і чітким розподілом відповідальності між хірургом, інженером та виробником.

### 8.4. Застосування у нейрохірургії та неврології

У нейрохірургії тривимірне моделювання має особливу вагу, оскільки навіть невелика похибка траєкторії може призвести до ушкодження функціонально значущої кори, провідних шляхів або судин. Типова модель поєднує структурну МРТ, тонкошарову КТ кісток, КТ- чи МР-ангіографію, венографію, функціональну МРТ і дифузійно-тензорну трактографію. Після реєстрації модальностей хірург отримує єдиний просторовий контекст: пухлина, кора, шлуночки, артерії, вени, череп і основні пучки білої речовини відображаються як окремі керовані шари. Це дозволяє оцінювати не лише відстань, а й кут доступу, глибину, можливість ретракції та зони, де анатомічна невизначеність є найбільшою [5, с. 4–5].

При внутрішньочерепних пухлинах модель використовується для вибору положення пацієнта, розміру й локалізації краніотомії, напрямку коридору та

послідовності виділення судин. Для менінгіом важливо показати відношення до венозних синусів і живильних артерій; для гліом - межі інфільтрації відносно функціональної кори та трактів; для пухлин основи черепа - кісткові канали, черепні нерви й магістральні судини. Віртуальне планування не усуває біологічної невизначеності меж гліоми, але допомагає заздалегідь визначити ділянки, де максимальна резекція може конфліктувати зі збереженням функції. У таких випадках модель доповнює нейрофізіологічне картування й операцію у свідомості, а не замінює їх.

У судинній нейрохірургії тривимірна ангіографічна реконструкція є стандартним способом оцінки аневризм і артеріовенозних мальформацій. Вона показує шийку аневризми, відходження гілок, напрямок купола, перфорантні судини та можливі проєкції кліпсування. Фізичні еластичні моделі застосовують для репетиції мікрохірургічного або ендоваскулярного втручання, вибору форми кліпси, катетера, стента чи потік-відхиляючого пристрою. Для мальформацій модель може відображати живильні артерії, нідус і дренувальні вени, що полегшує поетапне планування емболізації та резекції. Однак дрібні перфоранти можуть бути нижче просторової роздільної здатності, а еластичність надрукованої судини відрізняється від живої, тому симуляція має межі.

Тривимірні моделі підтримують стереотаксичні процедури: біопсію, дренування, імплантацію електродів глибокої стимуляції мозку, стереоелектроенцефалографію та лазерну абляцію. Планувальна система дозволяє побудувати траєкторію, що проходить повз борозни, шлуночки й судини, а також порівняти кілька точок входу. При епілепсії просторово поєднують МРТ, ПЕТ, ЕЕГ-джерела та результати нейропсихологічного картування, щоб сформувати гіпотезу епілептогенної мережі. Тривимірне подання особливо корисне для обговорення складної конфігурації електродів, але остаточне рішення повинно спиратися на сукупність електрофізіологічних даних, а не на красу візуалізації.

Окремим напрямом є навчання й симуляція. Надруковані моделі черепа, шлуночкової системи, судин та пухлин дають змогу відпрацьовувати трепанацію, ендоскопічну навігацію, кліпсування, шунтування та накладання швів. Моделі з різною твердістю матеріалів можуть відтворювати кістку, тверду мозкову оболонку й м'які тканини, хоча точне відтворення мозкової консистенції залишається складним. Змішана реальність дозволяє накласти віртуальну анатомію на манекен або фізичну модель, поєднавши тактильний і візуальний досвід. За даними огляду цифрової нейрохірургії, 3D-реконструкція, 3D-друк, навігація, роботизовані системи, штучний інтелект і цифрові двійники дедалі частіше розглядаються як частини єдиного технологічного контуру [5, с. 1, 9–10].

У неврології тривимірне моделювання застосовується переважно для кількісного аналізу, а не для друку. Автоматизоване визначення об'єму гіпокампа, кори, шлуночків, вогнищ демієлінізації чи ішемічного ураження підтримує моніторинг нейродегенеративних, запальних і судинних хвороб. Просторові карти атрофії можуть бути зіставлені з нормативною базою, а мережеві моделі - показувати порушення структурних і функціональних зв'язків. Після інсульту 3D-реконструкція ураження допомагає аналізувати зв'язок між локалізацією та дефіцитом, планувати нейрореабілітацію, роботизовані вправи або неінвазивну стимуляцію. Водночас такі висновки мають імовірнісний характер: однакова анатомічна локалізація не гарантує однакового клінічного прояву через індивідуальну організацію мереж і пластичність.

Найсуттєвішою технічною проблемою нейрохірургічної моделі є зсув мозку. Після відкриття твердої оболонки, втрати спинномозкової рідини, резекції частини пухлини та зміни тиску анатомія відхиляється від передопераційної МРТ. Статична навігація поступово втрачає точність, особливо в глибині. Для оновлення використовують інтраопераційну МРТ, ультразвук, поверхневе сканування та деформівні алгоритми реєстрації. Саме тут тривимірна модель має

перейти від фіксованої карти до динамічної системи, яка враховує зміни під час операції. Проте кожне автоматичне оновлення повинно відображати невизначеність і бути перевіреним оператором.

З етичного й організаційного погляду цифрова нейрохірургія потребує захисту даних, контролю версій, сумісності форматів і чітких правил відповідальності. Алгоритм може запропонувати сегментацію або траєкторію, але лікар повинен бачити вихідні зображення та розуміти, де автоматичний результат ненадійний. Особливо небезпечним є перенесення моделі між різними часовими точками без урахування росту пухлини, набряку або зміни положення судин. Тому перед використанням необхідно підтвердити дату дослідження, коректність реєстрації та відповідність положенню пацієнта.

Узагальнюючи, тривимірне моделювання в нейрохірургії та неврології поєднує персоналізовану анатомію з функціональними й мережевими даними. Воно підвищує якість планування, навчання й комунікації, але не усуває фундаментальних джерел невизначеності: мікроскопічної інфільтрації, руху тканин, неповноти візуалізації та індивідуальної функціональної варіабельності. Найбільш перспективним є не окремий красивий 3D-об’єкт, а система, що оновлюється інтраопераційними даними, відображає похибку та взаємодіє з навігацією, роботикою й клінічним рішенням [5, с. 10–13].

### 8.5. Стоматологія та щелепно-лицева хірургія

Стоматологія є однією з найбільш цифровізованих галузей медицини, оскільки поєднує конусно-променеву КТ, інтраоральне оптичне сканування, фотографію, сканування обличчя та комп’ютерне проєктування. Об’єднання цих даних формує віртуального пацієнта, у якому можна одночасно аналізувати зубні ряди, оклюзію, кісткову основу й м’якотканинний профіль. Тривимірні моделі використовують для діагностики аномалій прикусу, планування ортодонтичного переміщення, цифрового воскового моделювання, виготовлення кап, тимчасових і постійних ортопедичних конструкцій. На відміну від традиційного гіпсового

відбитка, цифрова модель легко копіюється, порівнюється в динаміці та інтегрується з виробництвом.

В імплантології планування починається з оцінки об'єму кістки, положення нижньощелепного каналу, гайморової пазухи, сусідніх коренів і майбутньої ортопедичної конструкції. Протетично орієнтований підхід передбачає, що позиція імплантата визначається не лише наявною кісткою, а й оптимальним виходом коронки. Хірургічний шаблон переносить цей план у порожнину рота та задає точку входу, кут і глибину свердління. Точність залежить від якості КТ, сканування, суміщення даних, стабільності опори шаблона та допусків друку. Тому навіть за повністю навігаційного протоколу потрібні перевірка посадки, контроль охолодження і готовність змінити план за клінічної невідповідності.

У щелепно-лицевій хірургії тривимірне моделювання особливо важливе при асиметріях, ортогнатичних операціях, травмах, пухлинних резекціях і реконструкції нижньої щелепи. Віртуальне хірургічне планування дозволяє виконати остеотомії, перемістити фрагменти, оцінити оклюзію та м'якотканинний ефект. Оклюзійні сплінти, різальні й позиціонувальні шаблони переносять план у операційну. При реконструкції вільним малогомілковим трансплантатом заздалегідь визначають сегменти, кути остеотомій і положення відносно дефекту, а індивідуальна пластина фіксує заплановану форму. Це скорочує імпровізацію під час тривалої операції, але вимагає враховувати онкологічний запас і можливі зміни дефекту після остаточного патоморфологічного рішення.

Адитивне виробництво застосовують для анатомічних моделей, шин, шаблонів, тимчасових протезів, індивідуальних титанових пластин, імплантатів скронево-нижньощелепного суглоба та каркасів для регенерації кістки. Вибір матеріалу визначається призначенням: модель для пояснення може бути виготовлена з недорогого полімеру, тоді як пристрій, що контактує з тканиною або підлягає імплантації, потребує біосумісності, стерилізаційної стабільності й

контрольованих механічних властивостей. Сучасний огляд щелепно-лицевих застосувань відзначає найбільшу зрілість пацієнт-специфічних імплантатів, хірургічних шаблонів, сплінтів і кісткових моделей, а біодруковані регенеративні каркаси поки переважно належать до дослідницького рівня [6, с. 1-18].

Перевагою стоматологічного цифрового процесу є висока повторюваність і можливість швидкого виробництва, однак похибки накопичуються на кожному етапі. Металеві реставрації створюють артефакти КТ, слина й рух впливають на сканування, алгоритм може неправильно сумістити поверхні, а полімер після друку усаджується під час промивання та полімеризації. Клінічно значущою є не лише середня точність, а локальна похибка в зоні опори, контакту або проходження інструмента. Тому цифровий файл повинен перевірятися до виробництва, а готовий виріб - після друку й постобробки. Для повторного застосування важливі простежуваність партії матеріалу та документування циклу стерилізації.

Подальший розвиток галузі пов’язаний з інтегрованим плануванням зубних рядів, скелета й обличчя та з автоматичним визначенням зубів, каналів, патологічних вогнищ і цефалометричних орієнтирів. Генеративні алгоритми пропонуватимуть форму пластини, імплантата або протеза, проте остаточне рішення має враховувати клінічний огляд, стан пародонта, суглоба і м’яких тканин.

### 8.6. Використання тривимірного моделювання для проведення віртуальних медичних операцій

Поняття віртуальної медичної операції охоплює комп’ютерне відтворення майбутнього хірургічного втручання на основі тривимірної моделі конкретного пацієнта. На відміну від звичайного перегляду томографічних зрізів, у такому середовищі лікар може змінювати положення об’єкта, моделювати доступ, виконувати умовне розсічення або видалення тканин, переміщувати фрагменти,

добирати імплантати та оцінювати можливий результат ще до реальної операції. Віртуальна операція не є тотожною дистанційному роботизованому втручанню і не замінює клінічного рішення; її слід розглядати як цифрову репетицію, засіб передопераційного аналізу та безпечного порівняння альтернатив. Сучасні підходи поєднують системи віртуальної, доповненої та змішаної реальності, тривимірне моделювання, навігацію і симуляційне навчання, формуючи єдиний цифровий контур підготовки операції [8, с. 1204–1206].

Основою віртуального втручання є пацієнт-специфічна анатомічна модель. Її створення починається з одержання КТ, МРТ, ультразвукових, ангіографічних, ендоскопічних або оптичних даних, вибраних відповідно до клінічного завдання. Для кісткових структур пріоритетною зазвичай є тонкошарова КТ, для м'яких тканин і центральної нервової системи – МРТ, для судин – контрастна КТ- чи МР-ангіографія, а для поверхні обличчя, зубних рядів і шкіри – фотограмметрія або оптичне сканування. Мультимодальні набори реєструють у спільній системі координат, після чого сегментують органи, патологічні утворення, судини, нерви, кістки та інші критичні структури. Уже на цьому етапі визначається межа достовірності майбутньої симуляції: помилка у вихідному зображенні або сегментації надалі відтворюватиметься в усіх віртуальних діях [5, с. 1, 4–5].

Після сегментації формують полігональну або воксельну модель, усувають дефекти поверхні, перевіряють замкненість сітки, топологію, масштаб і відповідність контрольним вимірюванням. Для простого планування достатньою може бути геометрична реконструкція, однак відтворення маніпуляцій потребує додаткової інформації про товщину, рухомість, пружність, анізотропію та зв'язки тканин. У системах планування пластичних і реконструктивних втручань геометричні моделі поєднують із мультимодальними діагностичними даними, формують гібридні об'єкти та синтезують очікуваний післяопераційний вигляд. Такий підхід дозволяє не лише показати анатомію, а й послідовно відтворити зміну її конфігурації під час операції та у процесі відновлення [9, с. 57–65].

Віртуальне хірургічне планування доцільно розглядати як послідовність взаємопов'язаних задач. Спочатку визначають мету втручання і допустимий функціональний ризик, далі обирають положення пацієнта, доступ і траєкторії інструментів, моделюють резекцію або реконструкцію, оцінюють дефект та спосіб його заміщення, а потім перевіряють план на зіткнення з критичними структурами. Цифрове середовище дає змогу повернутися до будь-якого кроку, змінити розміри резекції, положення остеотомії чи тип імплантата та порівняти результати. Саме можливість багаторазового повторення без ризику для пацієнта відрізняє віртуальну операцію від традиційного передопераційного обговорення, де значна частина просторових рішень залишається уявною.

Реалістичність симуляції залежить від того, наскільки правильно відтворено механіку тканин. Жорстке тіло може бути достатнім для моделювання положення кісткового фрагмента або протеза, але не для мозку, печінки, серця чи судин, які деформуються під дією інструмента, тиску, гравітації та зміни наповнення. Для м'яких тканин застосовують моделі скінченних елементів, масово-пружинні системи, позиційно-залежну динаміку та інші чисельні підходи. Висока фізична точність потребує значних обчислювальних ресурсів, тоді як інтерактивна симуляція має реагувати майже без затримки. Тому практичні системи шукають компроміс між деталізацією й швидкістю, а клінічно значущі параметри мають задаватися за даними конкретного пацієнта, а не лише за усередненими властивостями тканин.

У нейрохірургії віртуальні операції особливо корисні через високу щільність функціонально важливих структур у невеликому об'ємі. Мультимодальна модель може одночасно містити пухлину, кору, шлуночки, артерії, вени, черепні нерви та тракти білої речовини. Хірург моделює положення голови, форму краніотомії, кут мікрохірургічного коридору, обсяг кісткової резекції та послідовність наближення до патології. Для аневризм можна порівнювати проєкції кліпсування, для стереотаксичної біопсії – кілька

траєкторій, що оминають судини й шлуночки, а для пухлин основи черепа – оцінювати доступність різних анатомічних вікон. Огляд цифрової нейрохірургії підкреслює, що 3D-реконструкція, симуляція, навігація, роботизовані системи та штучний інтелект поступово інтегруються в єдиний процес планування [5, с. 4–5, 9–10].

Найважливішим обмеженням нейрохірургічної симуляції є зміна анатомії під час реального втручання. Після відкриття твердої мозкової оболонки, втрати спинномозкової рідини, резекції частини пухлини або виникнення набряку відбувається зсув мозку, через що передопераційна модель перестає точно відповідати операційному полю. Подолання цієї проблеми потребує інтраопераційної МРТ або ультразвуку, поверхневого сканування, відстеження інструментів і деформівної реєстрації. Отже, найбільш перспективною є не статична віртуальна операція, а модель, яку можна оновлювати в реальному часі та яка відображає похибку суміщення. Водночас автоматичне оновлення має контролюватися хірургом, оскільки неправильно оцінена деформація може бути небезпечнішою за відсутність підказки [5, с. 10–13].

У серцево-судинній хірургії та інтервенційній кардіології віртуальна репетиція охоплює вибір доступу, позиціонування клапанів, оклюдерів і стент-графтів, моделювання катетерної траєкторії та прогноз гемодинамічних наслідків. На персоналізованій моделі можна порівняти типорозміри пристрою, оцінити ризик перекриття коронарних артерій, обструкції вихідного тракту або неповного прилягання до стінки. Для складних вроджених вад симуляція допомагає визначити просторову можливість внутрішньосерцевого тунелю чи реконструкції магістральних судин. Поєднання геометрії з обчислювальною гідродинамікою переводить планування від оцінки форми до аналізу функції, хоча результат залежить від граничних умов, властивостей судинної стінки та якості вихідної візуалізації [1, с. 1].

У травматології та ортопедії віртуальна операція часто починається з цифрового розділення уламків і їх послідовної репозиції. Хірург може відновити анатомічну форму за неушкодженою контралатеральною кісткою, визначити площину остеотомії, довжину та напрямок гвинтів, положення пластини або компонента ендопротеза. У випадках деформації хребта моделюють корекцію, безпечні коридори для транспедикулярних гвинтів і баланс хребтово-тазових параметрів. Результат симуляції може бути перенесений у операційну за допомогою індивідуальних різальних і свердлильних шаблонів або навігації. Узагальнені дані щодо 3D-друк-асистованого лікування переломів свідчать про потенційне скорочення часу операції та крововтрати, але ефект залежить від локалізації, складності випадку й якості досліджень [4, с. 1-9].

Щелепно-лицева та реконструктивна хірургія є одним із найнаочніших прикладів повного циклу віртуальної операції. Після суміщення КТ, сканів зубних рядів і поверхні обличчя виконують віртуальні остеотомії, переміщують фрагменти, контролюють оклюзію та прогнозують м’якотканинний профіль. При реконструкції нижньої щелепи малогомілковим трансплантатом визначають довжину сегментів, кути розпилів, положення відносно дефекту і конфігурацію фіксаційної пластини. Для пластичних втручань важливим є синтез очікуваного післяопераційного вигляду, однак такий прогноз слід подавати як модельований сценарій, а не як гарантований результат, оскільки загоєння, рубцювання та реакція м’яких тканин мають індивідуальну варіабельність.

В онкохірургії віртуальне планування спрямоване на досягнення достатньої радикальності за максимально можливого збереження функціональної тканини. Тривимірна модель показує взаємовідношення пухлини з судинами, протоками, нервами та сусідніми органами, дозволяє моделювати різні межі резекції і визначати майбутній дефект. Для печінки важливими є сегментарна будова, портальні та печінкові вени і залишковий об’єм паренхіми; для нирки – положення пухлини щодо судин і чашково-мискової системи; для підшлункової

залози – контакт з магістральними судинами. Віртуальна операція може також підтримувати планування складної циторедукції, однак жодна геометрична модель не здатна достовірно показати мікроскопічну інвазію, тому остаточні межі визначаються онкологічними принципами й інтраопераційними даними [2, с. 1; 3, с. 1].

Віртуальна, доповнена та змішана реальність виконують різні функції в межах одного технологічного процесу. Віртуальна реальність повністю занурює користувача у цифрове операційне поле і найбільше підходить для репетиції та навчання. Доповнена реальність накладає контури пухлини, судин або запланованої траєкторії на реальне зображення пацієнта чи ендоскопічний відеопотік. Змішана реальність дозволяє взаємодіяти з голографічною моделлю у просторі, змінювати прозорість шарів, виконувати вимірювання і спільно обговорювати план. Стан розвитку цих технологій показує поступовий перехід від демонстраційних моделей до клінічно орієнтованих систем, однак їх безпека визначається не якістю візуального ефекту, а точністю реєстрації, стабільністю відстеження та зрозумілістю інтерфейсу [8, с. 1204–1206].

Реєстрація є критичним етапом перенесення віртуального плану у реальну операційну. Необхідно встановити точну відповідність між координатами моделі, пацієнта, інструментів і пристрою візуалізації. Для цього застосовують анатомічні орієнтири, штучні маркери, поверхневе зіставлення, оптичне або електромагнітне відстеження. Похибка може виникати через рух пацієнта, деформацію м’яких тканин, перекриття маркерів, затримку відображення або неправильне калібрування. У високоризикових втручаннях слід оцінювати не лише середню помилку реєстрації, а й локальну точність біля критичної структури. Віртуальна підказка має зникати або позначатися як ненадійна, якщо система втрачає відстеження чи виходить за межі валідованого діапазону.

Важливим напрямом є навчання хірургів. Типовий симулятор формує базові психомоторні навички, тоді як пацієнт-специфічна віртуальна операція готує до

конкретної складної анатомії. Користувач може відпрацьовувати послідовність кроків, розпізнавання орієнтирів, реакцію на ускладнення та командну взаємодію. Цифрове середовище дає змогу об'єктивно фіксувати час, довжину траєкторії інструмента, кількість небезпечних контактів, надмірну силу та відхилення від плану. Такі метрики підтримують структуроване оцінювання компетентності, але мають бути пов'язані з реальними клінічними навичками. Високий результат у симуляторі не гарантує безпомилкової роботи з живою тканиною, якщо модель не відтворює необхідної складності або допускає нереалістичні дії [8, с. 1204–1206].

Подальше вдосконалення віртуальних операцій пов'язане зі штучним інтелектом. Алгоритми автоматизують сегментацію, розпізнають анатомічні орієнтири, будують поверхні, пропонують безпечні траєкторії та порівнюють варіанти імплантації. Генеративні методи можуть створювати форму пластини, протеза або реконструктивного елемента відповідно до заданих обмежень. Під час симуляції машинне навчання використовується для прогнозу деформації, класифікації етапу операції та виявлення небезпечного наближення інструмента. Проте автоматична рекомендація має бути перевірюваною: лікар повинен бачити вихідні дані, межі сегментації, показник невизначеності й причини запропонованого рішення. Особливої обережності потребують рідкісні патології та зображення з артефактами, для яких навчальна вибірка може бути недостатньою [5, с. 9–13].

Концепція цифрового двійника розширює віртуальну операцію від одноразової репетиції до моделі, що постійно пов'язана з конкретним пацієнтом. Такий двійник може поєднувати анатомію, механіку тканин, фізіологічні сигнали, лабораторні показники, дані інструментів і перебіг відновлення. До операції він використовується для порівняння сценаріїв, під час втручання – для оновлення положення й стану структур, після операції – для прогнозування ускладнень та планування реабілітації. Повноцінний двійник має не лише

відтворювати пацієнта, а й кількісно показувати невизначеність прогнозу. Сучасні медичні цифрові двійники залишаються різнорідними за зрілістю, проте саме поєднання механістичних моделей і даних пацієнта створює основу для перевірки альтернативних втручань in silico [7, с. 184–191].

Оцінювання системи віртуальних операцій має охоплювати кілька рівнів. На геометричному рівні перевіряють точність сегментації, відхилення поверхонь, розміри й положення орієнтирів. На функціональному рівні оцінюють реалістичність деформації, реакцію на інструмент та відповідність фізіологічним вимірюванням. На користувацькому рівні визначають час виконання, кількість помилок, когнітивне навантаження і зручність інтерфейсу. Клінічна валідація повинна показати, чи змінює система план, скорочує тривалість операції, крововтрату, променеве навантаження або частоту ускладнень. Важливо відокремлювати технічну точність від клінічної користі: система може добре відтворювати анатомію, але не покращувати результат, якщо її застосовують у простих випадках або вона ускладнює робочий процес.

Ризики віртуальних операцій пов’язані з якістю даних, людським фактором, залежністю від програмного забезпечення та кібербезпекою. Застаріле обстеження може не відповідати актуальному положенню пухлини або судин, артефакти спотворюють межі, а користувач інколи довіряє яскравій 3D-візуалізації більше, ніж вихідним зрізам. Тривимірна реконструкція водночас містить унікальні анатомічні ознаки, тому передавання моделей у хмарні сервіси потребує шифрування, автентифікації, контролю доступу і документованої згоди. Необхідні контроль версій, повторна перевірка моделі перед втручанням, резервний план та можливість продовжити операцію без цифрової системи. Віртуальна підказка повинна підтримувати професійне судження, а не підміняти його.

Організація віртуальної операції в медичному закладі потребує чіткого розподілу ролей: лікар формулює клінічне завдання й затверджує анатомічні

межі, інженер відповідає за обробку даних, а фахівець з якості документує перевірку та версію файлу. Для України перспективним є створення міждисциплінарних лабораторій, які обслуговують кілька клінічних підрозділів, розробляють локальні протоколи й накопичують валідовані кейси. Вітчизняні публікації розглядають 3D-моделювання, віртуальну та доповнену реальність і симуляційне навчання як основу віртуальних медичних операцій, водночас наголошуючи на ресурсних обмеженнях [8, с. 1204–1206]. Економічну доцільність слід оцінювати за витратами на персонал і обладнання та за можливим скороченням тривалості операції, повторних втручань і ускладнень.

Отже, тривимірне моделювання перетворює підготовку хірургічного втручання на керований цифровий експеримент. Його найбільша цінність полягає у можливості побачити складну анатомію з позиції майбутнього доступу, багаторазово відпрацювати послідовність дій, порівняти альтернативи та перенести обраний план у операційну за допомогою навігації, доповненої реальності, шаблонів або роботизованих систем. Водночас віртуальна операція залишається моделлю з обмеженою точністю, а її безпечне використання потребує якісних вихідних даних, валідації, відображення невизначеності та збереження провідної ролі лікаря. Подальший розвиток пов’язаний із динамічними цифровими двійниками, штучним інтелектом і реальним часом, але клінічне впровадження має визначатися не технологічною новизною, а доведеним поліпшенням результатів лікування [7, с. 184–191; 9, с. 57–65].

## 8.7. Перспективи використання штучного інтелекту і цифрових двійників

Узагальнення досвіду різних спеціальностей показує, що тривимірне моделювання виконує чотири взаємопов’язані функції: робить складну анатомію наочною, забезпечує кількісні вимірювання, дозволяє випробувати втручання до

його виконання та переносить цифровий план у реальний простір за допомогою шаблонів, навігації чи індивідуальних виробів. Кардіологія найбільше використовує моделі рухомих структур і гемодинаміки, онкологія – просторове стадіювання та планування лікування, ортопедія – репозицію й імплантати, нейрохірургія – мультимодальні траєкторії, а стоматологія – наскрізний цифровий процес.

Штучний інтелект здатний скоротити найбільш трудомісткий етап – сегментацію. Нейронні мережі автоматично виділяють камери серця, кістки, зуби, пухлини, судини й мозкові структури, визначають орієнтири та формують початкову тривимірну сітку. Наступними кроками є автоматичне виправлення дефектів геометрії, пошук безпечних коридорів і генеративне проєктування імплантатів. Проте алгоритм може непомітно помилятися за рідкісної патології, артефактів або нетипового протоколу, тому потрібні перевірка меж на вихідних зрізах, геометричні тести й документоване затвердження лікарем.

Найперспективнішою є інтеграція анатомії з функцією. Штучний інтелект може поєднувати зображення, лабораторні показники, геномні дані, електрофізіологію, сигнали носимих пристроїв та електронну медичну документацію. За такого підходу модель перестає бути статичним знімком і стає компонентом персоналізованого прогнозу. Повноцінний медичний цифровий двійник пов’язаний з конкретним пацієнтом, оновлюється новими даними, моделює альтернативні сценарії та формує прогноз для підтримки рішення. Найрозвиненішими напрямами залишаються кардіологія й онкологія, але клінічна зрілість проєктів істотно відрізняється [7, с. 184–191].

У кардіології цифровий двійник може порівнювати варіанти абляції, ресинхронізації або імплантації клапана; в онкології – моделювати ріст пухлини й відповідь на терапію; в ортопедії – навантаження імплантата та ремоделювання кістки; у нейрохірургії – деформацію мозку й зміну функціональних мереж; у стоматології – переміщення зубів і перебудову тканин. Реалістичний прогноз

потребує поєднання механістичних рівнянь з машинним навчанням: перші підтримують причинну інтерпретацію, друге виявляє складні закономірності великих масивів даних.

Перед широким упровадженням необхідно розв'язати питання сумісності даних, конфіденційності, кібербезпеки, упередженості та регуляторного нагляду. Тривимірний файл містить унікальну анатомічну інформацію, а динамічний двійник може додатково об'єднувати генетичні дані, спосіб життя й перебіг хвороби. Тому потрібні мінімізація доступу, шифрування, журналювання дій і прозора згода. Навчальні вибірки мають відображати різноманіття популяції, а лікар повинен уникати автоматизаційного упередження та бачити показник невизначеності прогнозу.

Доказовість має виходити за межі геометричної точності. Для кожного сценарію слід встановити, чи змінює модель клінічне рішення, скорочує час операції, зменшує ускладнення, поліпшує функціональний результат і виправдовує витрати. Потрібні багатоцентрові дослідження, стандартизовані кінцеві точки та постійний моніторинг систем після впровадження. Найреалістичніша перспектива полягає не в заміні лікаря, а в спільному середовищі, де штучний інтелект прискорює обробку, 3D-модель забезпечує просторове розуміння, шаблон переносить план у процедуру, а цифровий двійник перевіряє альтернативні сценарії [5, с. 13; 7, с. 184–191].

### *Висновки до Розділу 8*

Тривимірне моделювання є важливим інструментом персоналізованої медицини, який забезпечує перетворення результатів КТ, МРТ, ультразвукової, ангіографічної, конусно-променевої та оптичної візуалізації на цифрові або фізичні пацієнт-специфічні моделі. Такі моделі дають змогу наочно відтворювати складні анатомічні структури, виконувати просторові вимірювання, оцінювати взаємне розташування органів і патологічних утворень,

моделювати варіанти лікування та переносити сформований цифровий план у клінічну практику за допомогою навігаційних шаблонів, індивідуальних імплантатів, комп'ютерної навігації та технологій доповненої реальності.

Найбільшу клінічну цінність тривимірне моделювання має у спеціальностях, де складна просторова анатомія безпосередньо впливає на безпечність і результативність втручання. У кардіології воно використовується для аналізу вроджених вад серця, планування транскатетерних і клапанних втручань, оцінювання патології аорти й коронарних судин, моделювання гемодинаміки та підготовки електрофізіологічних процедур. В онкології тривимірні моделі забезпечують просторове відображення пухлини, визначення її взаємозв'язку із судинами, протоками, нервами й органами ризику, уточнення резектабельності, вибір ділянки для біопсії, планування хірургічного та променевого лікування.

У травматології та ортопедії тривимірне моделювання дає змогу виконувати віртуальну репозицію кісткових фрагментів, планувати остеотомії, визначати положення пластин і гвинтів, створювати індивідуальні шаблони та імплантати. У нейрохірургії поєднання даних МРТ, КТ, ангіографії, функціональної МРТ і трактографії сприяє вибору безпечного хірургічного доступу, плануванню стереотаксичних процедур і збереженню функціонально важливих структур. У стоматології та щелепно-лицевій хірургії сформовано наскрізний цифровий процес – від отримання зображень до виготовлення хірургічних шаблонів, оклюзійних шин, протезів, пластин і пацієнт-специфічних імплантатів.

Водночас точність і клінічна достовірність тривимірних моделей залежать від якості вихідних зображень, правильності сегментації та реєстрації, параметрів побудови геометрії, характеристик матеріалів і клінічної перевірки результатів. Тривимірна модель не замінює вихідних медичних зображень, морфологічної верифікації та професійного рішення лікаря. Її використання має

супроводжуватися контролем похибок, документуванням етапів створення та визначенням меж невизначеності.

Перспективи подальшого розвитку пов’язані з використанням штучного інтелекту для автоматичної сегментації, пошуку анатомічних орієнтирів, вибору безпечних траєкторій і генеративного проєктування індивідуальних виробів. Інтеграція тривимірних моделей із лабораторними, генетичними, електрофізіологічними та іншими динамічними даними створює передумови для формування медичних цифрових двійників. Отже, тривимірне моделювання підвищує наочність, точність і обґрунтованість клінічних рішень, однак його ефективне впровадження потребує стандартизації робочих процесів, багатоцентрової клінічної валідації, оцінювання економічної доцільності та забезпечення захисту персональних даних.

## Список використаних джерел

1. Ravi S. N. Three-Dimensional Printing in Cardiovascular Medicine: Clinical Applications and Technological Advancements. Journal of Cardiovascular Translational Research. 2026. Vol. 19. Art. 8. DOI: 10.1007/s12265-025-10733-9.

2. Wu J., Liang B., Lu S., Xie J., Song Y., Wang L., Gao L., Huang Z. Application of 3D printing technology in tumor diagnosis and treatment. Biomedical Materials. 2024. Vol. 19, No. 1. Art. 012002. DOI: 10.1088/1748-605X/ad08e1.

3. Cai Z., Zhang K., Li L., Suo Y. Application of 3D reconstruction and 3D printing technology in advanced ovarian cancer surgery: a retrospective study. Frontiers in Oncology. 2024. Vol. 14. Art. 1432970. DOI: 10.3389/fonc.2024.1432970.

4. Xiao L., Tang P., Yang S., et al. Comparing the efficacy of 3D-printing-assisted surgery with traditional surgical treatment of fracture: an umbrella review. Journal of

Orthopaedics and Traumatology. 2025. Vol. 26, No. 1. Art. 3. DOI: 10.1186/s10195-025-00819-0.

5. Yuan Z., Shi Z., Wang Z. Digital neurosurgery in the era of intelligent medicine: a scoping review. Frontiers in Medicine. 2025. Vol. 12. Art. 1700166. DOI: 10.3389/fmed.2025.1700166.

6. Wang X., Mu M., Yan J., Han B., Ye R., Guo G. 3D printing materials and 3D printed surgical devices in oral and maxillofacial surgery: design, workflow and effectiveness. Regenerative Biomaterials. 2024. Vol. 11. Art. rbae066. DOI: 10.1093/rb/rbae066.

7. Laubenbacher R., Mehrad B., Shmulevich I., et al. Digital twins in medicine. Nature Computational Science. 2024. Vol. 4. P. 184-191. DOI: 10.1038/s43588-024-00607-6.

8. Titova N. V., Romanyuk S. O., Kotlyk S. V., Romanyuk O. N., Pavlov S. V. Conducting virtual medical surgeries abroad and in Ukraine. Матеріали XVIII міжнародної науково-практичної конференції «Інформаційні технології і автоматизація – 2025», Одеса, 30–31 жовтня 2025 р. Одеса : ОНТУ, 2025. С. 1204–1206.

9. Романюк С. О., Павлов С. В., Романюк О. Н., Тітова Н. В. Інтелектуалізовані високопродуктивні системи планування пластичних і реконструктивних операцій на обличчі людини. Оптико-електронні інформаційно-енергетичні технології. 2020. № 2 (40). С. 57–65. DOI: 10.31649/1681-7893-2020-40-2-56-64.

# ПІСЛЯМОВА

Цифровізація дедалі виразніше змінює не окремі способи здійснення професійної діяльності, а саму архітектуру суспільних відносин, механізми прийняття рішень, характер взаємодії людини з державою та приватними суб'єктами, способи продукування, накопичення й використання інформації, а також критерії юридичної, економічної та професійної відповідальності. Саме тому предметне поле монографії закономірно охопило цифровий конституціоналізм, електронне правосуддя, міжнародно-правове регулювання штучного інтелекту й цифрових доказів, цифрову модернізацію податкової політики, трансформацію обліково-аналітичних систем підприємств, проблематику громадського та репродуктивного здоров'я, а також клінічне застосування тривимірного моделювання і цифрових двійників.

Об'єднання настільки різних за предметом напрямів в одному дослідженні виявило принципово важливу спільну рису: цифрова трансформація не може бути адекватно оцінена виключно за критеріями технологічної новизни, швидкості, економічної ефективності чи функціональної зручності. У кожній із досліджуваних сфер технологія входить у вже сформовану систему прав, компетенцій, професійних стандартів, інституційних гарантій та юридичної відповідальності. Відповідно, питання про допустимість цифрового рішення завжди є водночас питанням про межі втручання, прозорість процедур, достовірність даних, розподіл ризиків, можливість контролю та наявність механізмів захисту особи від несприятливих наслідків технологічно опосередкованого рішення.

Особливо виразно ця закономірність простежується у площині конституційного права. Цифрові технології вже не перебувають поза межами конституційної матерії, оскільки саме через цифрове середовище дедалі частіше реалізуються особисті, політичні, соціальні та культурні права. Цифрова грамотність, доступність технологій, захист від алгоритмічної дискримінації, інформаційна автономія, охорона персональних даних і гарантування прав особи

в умовах автоматизованого управління поступово перетворюються на складові сучасного конституційного дискурсу. Для України цей процес додатково поєднаний із необхідністю забезпечення кіберстійкості держави, захисту інформаційної інфраструктури та водночас збереження належного рівня свободи, приватності й цифрової автономії людини.

Не менш істотних трансформацій зазнає судова влада. Цифровізація правосуддя відкриває можливості для спрощення доступу до суду, підвищення оперативності процедур, електронного обміну документами та використання нових інструментів роботи з доказовою інформацією. Водночас технологічне удосконалення судової системи не може відбуватися за рахунок процесуальних гарантій. Ідентифікація учасників, надійність електронних доказів, захист інформації, доступність цифрових сервісів, сумісність платформ та можливість ефективної участі особи у провадженні залишаються юридично значущими умовами справедливого судового розгляду. Відтак цифрове правосуддя має оцінюватися не за кількістю впроваджених електронних сервісів, а за спроможністю таких сервісів забезпечувати функціонально повноцінну реалізацію права на судовий захист. Тематика відповідного розділу монографії саме й охоплює українську та європейську моделі електронного правосуддя, процесуальні гарантії доступу, ідентифікації, доказування та безпеки.

Аналогічної оцінки потребує вплив цифрових технологій на міжнародне право. Використання штучного інтелекту, цифрових доказів і алгоритмічних систем не заперечує усталених засад міжнародно-правового регулювання, однак істотно ускладнює умови їх практичного застосування. Достовірність походження цифрової інформації, її цілісність, можливість верифікації, непрозорість алгоритмічного висновку, ризики дискримінації та питання відповідальності стають новими елементами правової оцінки. Саме тому технологічна адаптація міжнародного права повинна супроводжуватися розвитком гарантій приватності, недискримінації, процесуальної добросовісності та довіри до механізмів прийняття рішень.

Економічний блок монографії засвідчує іншу, однак змістовно споріднену тенденцію. Цифровізація податкової політики та обліково-аналітичних систем змінює традиційне уявлення про державне адміністрування й управління підприємством. Автоматизований облік, електронний аудит, інтеграція даних, прогнозна аналітика, штучний інтелект, технології Big Data, цифрові системи контролю та підтримки управлінських рішень формують принципово інший рівень інформаційної спроможності як держави, так і суб'єктів господарювання. Для України цифрова модернізація податкової сфери водночас пов'язана з європейською інтеграцією, інституційною адаптацією та необхідністю поєднання ефективності фіскального адміністрування з принципами рівності, справедливості та правової визначеності.

У корпоративному вимірі цифрова обліково-аналітична система вже не зводиться до автоматизації бухгалтерського обліку. Вона поступово трансформується в інтегровану інформаційну платформу, де взаємодіють цифровий документообіг, контроль, аудит, аналітика, прогнозування, податкове адміністрування та підтримка управлінських рішень. У межах дослідженої моделі цифрова трансформація охоплює цифровізацію даних, автоматизацію процесів, інтеграцію систем, інтелектуалізацію аналітики, цифровий контроль та управлінську адаптивність. Це дозволяє говорити про зміну самої логіки управління: інформація перестає бути лише ретроспективним відображенням діяльності й набуває значення ресурсу прогнозування та формування управлінських альтернатив.

Медичний вимір цифровізації ще виразніше демонструє необхідність обмежувати технологічний оптимізм вимогами професійної та етичної відповідальності. Тривимірне моделювання, віртуальне планування втручань, штучний інтелект і цифрові двійники створюють нові можливості для персоналізації лікування, просторового аналізу анатомії, моделювання операцій і прогнозування результатів. Проте достовірність цифрової моделі безпосередньо залежить від якості вихідних даних, коректності сегментації, клінічної верифікації та належного відображення невизначеності. Технологічне

рішення не усуває професійної відповідальності лікаря і не може автоматично замінювати клінічне судження. У самій монографії підкреслено, що клінічне впровадження тривимірного моделювання має визначатися не технологічною новизною як такою, а доведеним покращенням результатів лікування.

Проблематика громадського та репродуктивного здоров'я доповнює технологічний вимір соціальним і правозахисним контекстом. Стан здоров'я населення залежить не виключно від клінічної спроможності системи охорони здоров'я, а й від доступності достовірної інформації, рівності доступу до відповідних послуг, міжвідомчої координації, здатності держави протидіяти дезінформації та забезпечувати безперервність профілактичних, лікувальних і реабілітаційних заходів. Особливої гостроти ці питання набувають в умовах воєнних загроз, коли стійкість медичної системи стає складовою загальної суспільної стійкості.

Сукупність проведених досліджень дозволяє окреслити ще одну важливу закономірність: цифровізація одночасно розширює можливості та збільшує концентрацію влади над даними, процедурами й рішеннями. Алгоритм здатний прискорити розгляд інформації, але водночас ускладнити розуміння логіки рішення; цифрова платформа може розширити доступ до послуги, але створити новий бар'єр для особи, яка не має достатньої цифрової компетентності; автоматизація може зменшити кількість рутинних операцій, але перенести ризик помилки з індивідуальної дії на системний рівень. Саме тому питання цифрової грамотності, доступності технологій, кібербезпеки, перевірюваності автоматизованих рішень і персоніфікованої відповідальності мають розглядатися як взаємопов'язані компоненти сучасної регуляторної політики. Питання цифрової грамотності та спеціального захисту вразливих категорій користувачів безпосередньо порушуються й у дослідженні цифрового конституціоналізму.

У цьому сенсі ключовим результатом міждисциплінарного прочитання представлених у монографії проблем є усвідомлення того, що ефективне регулювання цифрової трансформації не може будуватися за принципом

постфактумного реагування на вже реалізовану технологію. Право, професійні стандарти, етичні правила, механізми інституційного контролю та моделі відповідальності мають формуватися одночасно з упровадженням технологічних рішень. Для високоризикових сфер, зокрема, правосуддя, охорони здоров'я, публічного адміністрування, оподаткування, обробки персональних даних, така синхронізація набуває особливої ваги, оскільки наслідки технологічної помилки можуть безпосередньо впливати на правовий статус, майнове становище, здоров'я або реалізацію фундаментальних прав людини.

Перспективний напрям подальших досліджень тому пов'язаний із переходом від опису окремих цифрових інструментів до формування комплексних моделей їх правової та інституційної інтеграції. Потребують подальшого доктринального опрацювання природа цифрових прав, межі алгоритмічного управління, стандарти доказової надійності цифрової інформації, механізми перевірки автоматизованих рішень, моделі цифрової зрілості установ і підприємств, критерії клінічної валідності цифрових медичних технологій, а також способи забезпечення реальної відповідальності за рішення, у формуванні яких істотну роль відіграють алгоритмічні системи. У самому дослідженні цифрового конституціоналізму подальша наукова перспектива пов'язується, зокрема, з формуванням цілісної теорії цифрових прав, удосконаленням механізмів їх гарантування та аналізом цифрової нерівності.

Отже, цифрова трансформація права, медицини та економіки є не паралельним розвитком трьох автономних сфер, а проявом єдиного процесу перегляду усталених механізмів регулювання, професійної діяльності та інституційної взаємодії. Його подальший напрям залежатиме від того, наскільки технологічні можливості будуть узгоджені з принципами правової визначеності, безпеки, пропорційності, недискримінації, професійної відповідальності та поваги до людської автономії. Саме здатність утримати цей баланс має стати визначальним критерієм оцінювання цифрових реформ незалежно від сфери їх застосування.

Представлена колективна монографія не завершує дискусію про нормативні та практичні наслідки цифровізації. Її зміст, навпаки, засвідчує відкритість відповідного наукового поля та необхідність подальшої взаємодії правників, економістів, медиків, фахівців із цифрових технологій і представників суміжних галузей знань. Швидкість технологічних змін об'єктивно унеможливлює формування остаточних відповідей, однак саме міждисциплінарна наукова рефлексія дозволяє своєчасно визначати межі допустимого, формувати належні регуляторні моделі та запобігати ситуаціям, у яких технологічна ефективність досягається ціною послаблення правових, професійних чи етичних гарантій.

## ДЛЯ НОТАТОК

## ДЛЯ НОТАТОК

Наукове видання

# ЦИФРОВІ ТЕХНОЛОГІЇ У ПРАВІ, МЕДИЦИНІ ТА ЕКОНОМІЦІ: РЕГУЛЯТОРНІ МОДЕЛІ ТА ПРАКТИЧНІ ВИКЛИКИ

Колективна монографія

Друкується в авторській редакції

Формат 60x84 $^{1}/_{16}$. Обсяг 21,16 ум. друк. арк., 21,01 обл.-вид. арк.
Наклад 300 пр. Зам. 119. Видавець і виготовлювач – Вежа-Друк
(м. Луцьк, вул. Шопена, 12, тел. + 38 066 936 25 49).
Свідоцтво Держ. комітету телебачення та радіомовлення України
ДК № 4607 від 30.08.2013 р.