ВЛАДА НАД КОДОМ

Стандарт цифрового публічного права

Інститут цифрового суспільства та публічного права майбутнього

Робочий проєкт для обговорення v1.0 — 28 вересня 2026 р.

Статус документа

Стадія. Робочий проєкт для обговорення v1.0 від 28 вересня 2026 року. Реєстровий запис буде присвоєно з початком публічного обговорення.

Видавець. Видано Інститутом цифрового суспільства та публічного права майбутнього ЄОПП.

Юридична сила. Стандарт є інструментом м'якого права. Він не має обов'язкової сили, доки компетентний орган не надасть йому такої сили власним актом.

Публічне обговорення. Публічне обговорення триває щонайменше шістдесят (60) днів. Зауваження запрошуються від органів публічної влади, наглядових органів, судів та омбудсменів, науковців, громадянського суспільства і постачальників. Зауваження подаються під іменем автора й оприлюднюються разом із ним; анонімні та конфіденційні зауваження не приймаються.

DRAFT

Вступ

Публічна влада дедалі частіше здійснюється через цифрові системи: моделі автоматизованого оцінювання ризиків визначають, кого перевірятиме орган, цифрові гаманці відкривають чи закривають доступ до транскордонних послуг, платформи даних впливають на те, як лікарні розподіляють ресурси. Галузеве право оцінює кожну з таких систем фрагментарно. Законодавство про захист даних з'ясовує, чи законно обробляються персональні дані, законодавство про штучний інтелект — чи відповідає модель вимогам, визначеним з огляду на ризик, законодавство про кібербезпеку — чи належно реагують на інциденти й повідомляють про них. Жоден галузевий режим не ставить комплексного питання, якому присвячено цей Стандарт: чи зберігає відповідальна публічна установа правову й фактичну здатність розуміти, спрямовувати, перевіряти й виправляти цифровий механізм, через який вона здійснює публічну владу, а за потреби — припинити його дію?

Держава зберігає владу над кодом не тому, що володіє договором, політикою чи платформою. Вона зберігає її лише тоді, коли доведено, що законна публічна влада здатна розуміти, спрямовувати, перевіряти, виправляти, забезпечувати засоби захисту й підтримувати технічні та соціотехнічні механізми, через які виконується публічна функція, а за потреби — виходити з них. Владу над кодом доводять, а не декларують.

Стандарт складається з чотирьох частин. Частина I (Нормативне ядро) викладає базову вимогу, одинадцять принципів, десять спроможностей контролю та основоположні тести й поняття. Частина II (Метод) викладає оцінювання впливу цифрового публічного права, тобто визначений Стандартом метод, яким перевіряють, чи дотримано Нормативного ядра в кожній публічній функції. Частина III (Застосування) описує, як використовується Стандарт: режими використання, Файл цифрової публічної функції, три ступені перевірки та висновки за їх результатами, форми, в яких компетентний орган може надати Стандарту юридичної сили, і співвідношення з іншими інструментами. Частина IV (Ведення Стандарту та інструменти м'якого права) пояснює, як Стандарт виносять на публічне обговорення, ухвалюють, змінюють і впроваджують.

DRAFT

Частина I — Нормативне ядро

I.1 Мета і природа

I.1.1 Стандарт цифрового публічного права «Влада над кодом» (далі — «Стандарт») визначає мінімальні умови, які мають залишатися виконаними щоразу, коли публічна функція виконується, опосередковується, обмежується, пріоритезується або суттєво формується за допомогою цифрових систем.

I.1.2 Стандарт є правовим стандартом: цілісною сукупністю нормативних вимог разом із визначеним методом їх застосування, покликаною забезпечити однакове застосування в різних установах і юрисдикціях. Його зміст ґрунтується на конституційному, адміністративному, галузевому праві та праві прав людини, яке вже регулює публічну владу. Стандарт не створює нових матеріальних прав і не витісняє застосовного права, яке визначає зміст і обов'язковість кожної вимоги в кожній юрисдикції.

I.1.3 Стандарт застосовується до цифрових публічних функцій, які відповідають тесту функціональної сфери застосування (I.8.1), незалежно від того, виконує функцію публічний орган чи приватний суб'єкт від його імені.

I.2 Нормативна мова

I.2.1 **«Має» (must)** позначає або методологічну передумову обґрунтованого висновку за Стандартом, або обов'язок, установлений застосовним правом. У кожному Файлі цифрової публічної функції зазначається, яка з підстав застосовується. Невиконання вимоги «має» блокує відповідну категорію рішень.

I.2.2 **«Слід» (should)** виражає настійну рекомендацію Стандарту, від якої установа може відступити лише із задокументованим мотивованим обґрунтуванням.

I.2.3 **«Може» (may)** позначає дозволений варіант.

I.2.4 Методологічна вада за Стандартом сама по собі не є судовим висновком про незаконність. Так само рішення не застосовувати Стандарт не звільняє установу від її чинних юридичних обов'язків.

I.3 Визначення

I.3.1 **Цифрове публічне право** — галузь права, що стосується правового встановлення, здійснення, опосередкування та контролю публічної влади в цифрово залежному середовищі.

I.3.2 **Код** — технічно формалізовані й операційно дієві механізми, через які цифрова система виконує, опосередковує, обмежує, пріоритезує чи іншим чином суттєво формує публічну функцію. Він охоплює вихідний і виконуваний програмний код; алгоритми, обчислювальні правила, моделі прийняття рішень і моделі штучного інтелекту; конфігурації систем, порогові значення, ваги, параметри та налаштування за замовчуванням; моделі даних, схеми, класифікації та навчальні, тестові, довідкові чи операційні набори даних; системи керування робочими процесами, правила

DRAFT

автоматизованих рішень і ескалації; програмні інтерфейси, механізми інтероперабельності та обміну даними; механізми ідентифікації, автентифікації, авторизації, облікових даних і контролю доступу; системи журналювання, моніторингу, ранжування, фільтрації, зіставлення, рекомендацій і сповіщень; архітектуру платформ, хмарні конфігурації та вбудовані засоби безпеки; технічні специфікації, вимоги закупівель, ліцензійні умови та функції систем, які контролює постачальник; а також протоколи взаємодії людини і машини, якщо вони структурують, обмежують, спрямовують чи скеровують здійснення публічної влади.

I.3.3 Закони, політики, адміністративні інструкції, договори та людський розсуд не стають кодом лише тому, що вони письмові чи формалізовані. Вони підпадають під визначення лише настільки, наскільки їх перенесено в цифрову систему, вбудовано в неї або введено в дію через неї.

I.3.4 Влада над кодом — юридично обґрунтована й інституційно дієва здатність органів публічної влади розуміти, спрямовувати, обмежувати, перевіряти, тестувати, оскаржувати, виправляти, скасовувати дію, зупиняти, замінювати і, за потреби, припиняти технічні системи, через які здійснюються публічні функції. Вона вимагає, щоб відповідальна установа зберігала юридичну відповідальність за функцію; достатні інституційні знання й технічну компетентність; доступ до відповідних доказів, записів, даних, моделей, конфігурацій, журналів та аудиторської інформації; дієвий контроль над суттєвими змінами системи; здатність повідомляти, пояснювати, забезпечувати перегляд, оскарження, виправлення і засоби захисту; безперервність роботи, якщо постачальник, платформа, модель чи інфраструктурний компонент відмовляє або стає недоступним; а також повноваження і практичну спроможність втрутитися, якщо система дає незаконні, несумісні з конституційними вимогами, небезпечні, дискримінаційні, ненадійні чи інституційно неприйнятні результати.

I.3.5 Влада над кодом не вимагає, щоб публічна установа володіла власним програмним забезпеченням чи сама його розробляла. Аутсорсинг, закупівлі, ліцензування, залежність від хмарних сервісів, пропрієтарні системи та участь приватного сектору сумісні з владою над кодом за умови, що вони не позбавляють відповідальну установу практичної здатності виконувати свої юридичні обов'язки.

I.3.6 Оцінювання впливу цифрового публічного права (DPLIA) — визначений Стандартом метод, викладений у Частині II, для виявлення, аналізу, ухвалення рішень, документування та перегляду публічно-правових наслідків цифрової публічної функції. DPLIA є частиною Стандарту, а не окремим інструментом.

I.3.7 Файл цифрової публічної функції (далі — «Файл») — єдиний офіційний документ, у якому фіксується оцінювання за Стандартом (III.2).

I.3.8 Відповідальна установа — публічна установа, юридично відповідальна за публічну функцію, що оцінюється.

I.3.9 Компетентний орган — публічний орган, що має юридичне повноваження надати Стандарту юридичної сили в межах своєї компетенції; **акт про запровадження** — акт, яким він це робить (III.5).

I.3.10 Висновок за результатами оцінювання за Стандартом — результат оцінювання на будь-якому ступені перевірки (III.4). Він не є сертифікатом, знаком відповідності чи декларацією законності.

DRAFT

I.4 Базова вимога

> **Базова вимога**
>
> Будь-яка установа, юридично відповідальна за цифрову публічну функцію, зберігає повноваження, знання, доступ, докази, спроможності та практичні засоби, необхідні, щоб розуміти, спрямовувати, обмежувати, перевіряти, оскаржувати, виправляти, скасовувати дію, зупиняти, замінювати і, за потреби, припиняти технічні та соціотехнічні механізми, через які ця функція виконується.

I.4.1 Базову вимогу перевіряють через десять спроможностей контролю (I.6) та шість контрольних точок (II.3). Положення про право власності та заяви про політику мають значення, але не є доказом. Питання завжди полягає в тому, чи права, доступ, повноваження, докази й операційні спроможності існують, розподілені, придатні до використання і перевірені в реалістичних умовах.

I.5 Принципи

Наведені нижче одинадцять принципів визначають мінімальні умови законного, конституційно спадкоємного, інституційно відповідального та стійкого цифрового опосередкування публічних функцій.

Принцип 1. Ідентифікація публічної функції. Кожну діяльність, що здійснюється за допомогою цифрових систем, оцінюють за її функцією та практичними наслідками, а не за інституційною назвою, договірною формою, моделлю власності чи технологічним описом.

Принцип 2. Юридичні повноваження та конституційна спадкоємність. Цифрова трансформація не має переривати дії принципів законності, компетенції, процедурної справедливості, рівності, пропорційності, обґрунтування рішень, підзвітності, судового захисту та ефективного засобу захисту.

Принцип 3. Публічна відповідальність, що не підлягає делегуванню. Відповідальна публічна установа зберігає юридичну та інституційну відповідальність за публічну функцію, зокрема тоді, коли технічну розробку, експлуатацію, інфраструктуру, обробку даних чи підтримку рішень забезпечує приватний суб'єкт.

Принцип 4. Інституційна влада над кодом. Відповідальна установа зберігає достатні юридичні повноваження, технічний доступ, знання, договірні права, організаційну спроможність і операційні можливості, щоб розуміти, контролювати, тестувати, виправляти, скасовувати дію, зупиняти, замінювати або припиняти відповідну систему. Докази цієї спроможності впорядковуються за чотирма сферами доказування (I.7).

Принцип 5. Простежуваність і цілісність доказів. Система створює і зберігає достатні докази своєї правової підстави, проєктних припущень, джерел даних, операційних правил, суттєвих змін, рішень, втручань, помилок і результатів.

DRAFT

Принцип 6. Можливість оскарження та засоби захисту. Особи, яких це стосується, мають доступ до змістовного повідомлення, пояснення, перегляду, виправлення, оскарження та засобу захисту відповідно до характеру й наслідків цифрової публічної функції.

Принцип 7. Врядування на всіх шести рівнях. Дотримання застосовного права неможливо встановити лише через аналіз алгоритму чи технічного компонента. Правовий, інституційний, технічний, операційний і суспільний рівні, а також рівень даних оцінюються разом.

Принцип 8. Контроль над приватними суб'єктами та залежностями. Договори, ліцензії, закупівельні умови, обмеження інтелектуальної власності, залежність від хмарних сервісів, правила платформ і пропрієтарні системи не мають перешкоджати органу публічної влади виконувати свої юридичні обов'язки чи здійснювати дієвий контроль.

Принцип 9. Безпека, стійкість і безперервність. Цифрова система проєктується та врядовується так, щоб зберігати безперервність, цілісність, доступність, відновлюваність і законне функціонування публічної функції в разі передбачуваних збоїв, відмов, атак, виходу постачальника чи технологічних змін.

Принцип 10. Забезпечення впродовж життєвого циклу. Оцінювання триває після впровадження. Суттєві зміни законодавства, мети, даних, моделей, конфігурації системи, постачальників, інфраструктури, ризиків чи інституційної спроможності зумовлюють пропорційне повторне оцінювання.

Принцип 11. Цілісне інституційне судження. Остаточне рішення не зводиться до технічного бала чи автоматизованого результату перевірки відповідності. Відповідальна установа ухвалює і документує мотивоване публічно-правове судження на підставі шести контрольних точок, аналізу шести рівнів, причинно-наслідкового синтезу, рівня впевненості в доказах, залишкових ризиків та умов подальшої роботи.

I.6 Десять спроможностей контролю

I.6.1 Базова вимога набуває операційного змісту через десять спроможностей контролю. У канонічному порядку це: Розуміти → Спрямовувати → Документувати → Перевіряти → Пояснювати → Виправляти → Втручатися → Зберігати докази → Забезпечувати безперервність → Виходити.

I.6.2 Спроможності кумулятивні та обов'язкові. Сильна позиція в одній не компенсує відсутності іншої, потрібної для виконання юридичних обов'язків функції; усі десять розглядаються разом.

I.6.3 Володіння вихідним кодом не є визначальним чинником. Залежно від конституційного значення функції та характеру приватної залежності доступ до вихідного коду може бути необхідним, корисним, але не необхідним, або зайвим. Питання функціональне, а не про право власності.

I.6.4 Необхідна глибина кожної спроможності залежить від конституційного значення функції, тяжкості й зворотності можливих наслідків, ступеня приватної залежності та того, наскільки важко особі отримати докази того, що сталося. Стандарт не встановлює відповідальності незалежно від вини за кожен збій системи і не вимагає, щоб кожен орган мав власну службу розробки програмного забезпечення.

ДРАФТ

№	Спроможність	Необхідна здатність установи	Приклади доказів	Сфера доказування
1	Розуміти	Описати, як механізм суттєво впливає на функцію, її операційні межі та відомі режими відмов.	Карта функції; опис архітектури; аналіз обмежень; дані про компетентність персоналу; незалежне технічне пояснення.	Знати
2	Спрямовувати	Контролювати законні цілі, політику, операційні пороги, коло осіб, яких це стосується, і будь-які суттєві зміни цього.	Реєстр прав на рішення; погодження змін; дієві умови договорів щодо змін; журнал погоджень.	Керувати
3	Документувати	Відтворити відповідні дані, правила, версії, втручання та шлях ухвалення будь-якого рішення.	Походження даних; історія конфігурацій і версій; адміністративні й технічні записи.	Знати
4	Перевіряти	Забезпечити кваліфіковану, належно незалежну перевірку роботи системи, журналів, засобів контролю та доказів, які має постачальник. Право на аудит треба реалізовувати, а не лише мати.	Реалізовувані права доступу; проведені аудити; результати тестів; записи про доступ.	Відповідати
5	Пояснювати	Надавати зрозумілі, конкретні для справи підстави, достатні, щоб особа зрозуміла рішення і, за потреби, оскаржила його.	Тести пояснень з користувачами; мотивовані рішення; шаблони обґрунтувань; процедури розкриття.	Знати
6	Виправляти	Виявляти й виправляти помилки в даних, логіці та результатах і поширювати виправлення на всі рішення, яких помилка стосувалася.	Тести виправлення і поширення; виявлення справ, яких стосується помилка; записи про повторний розгляд.	Відповідати
7	Втручатися	Скасовувати дію, обмежувати, зупиняти роботу або безпечно повертати систему до попереднього стану уповноваженими діями.	Перевірені процедури втручання; навчені посадовці; повноваження та журнали ескалації.	Керувати
8	Зберігати докази	Зберігати докази придатними для скарг, перегляду, судових проваджень, розслідувань і навчання згідно із законними правилами зберігання.	Графік зберігання; заборона знищення документів у зв’язку зі спором; захищені журнали; контроль доступу.	Відповідати
9	Забезпечувати безперервність	Виконувати основні юридичні обов’язки під час збою, атаки чи відмови постачальника.	Перевірений резервний механізм; альтернативний канал; навчання з відновлення; ресурси безперервності.	Підтримувати

№	Спроможність	Необхідна здатність установи	Приклади доказів	Сфера доказування
10	Виходити	Мігрувати, замінювати чи припиняти систему або постачальника, зберігаючи основний юридичний обов'язок.	Кошторисний план переходу; тести переносимості; права на допомогу; збереження незавершених вимог; проведене навчання з виходу.	Підтримувати

Таблиця I.1. Десять спроможностей контролю в канонічному порядку зі сферою доказування для кожної.

I.6.5 Записи мають бути достатніми для відтворення подій і засобів захисту за дотримання законних вимог щодо мінімізації даних, конфіденційності та строків зберігання. Виправлення має виявляти кожне рішення, якого стосується помилка й забезпечувати законний шлях до його перегляду, фіксуючи будь-які обмеження щодо повторного розгляду та їх наслідки.

I.7 Чотири сфери доказування

I.7.1 Чотири сфери доказування групують десять спроможностей за видом доказів, яких потребує кожна. Це допоміжний засіб упорядкування доказів, а не другий оцінюваний набір; сфери не змінюють канонічного порядку спроможностей.

Сфера	Спроможності	Питання	Типові докази
Знати	Розуміти · Документувати · Пояснювати	Чи може установа описати, як працює функція, де її межі та чому настав певний результат?	Архітектура, походження даних, карта залежностей, дані про спроможності персоналу, обґрунтування у справах.
Керувати	Спрямовувати · Втручатися	Чи може установа спрямовувати суттєві рішення та зміни й переривати роботу системи?	Договірні права та права доступу, записи про контроль змін, реалізовані (а не лише передбачені) права на втручання.
Відповідати	Перевіряти · Виправляти · Зберігати докази	Чи може установа піддатися перевірці, виправляти помилки й зберігати докази для перегляду?	Проведені аудити, записи про виправлення та їх поширення, записи про зберігання і заборону знищення документів.
Підтримувати	Забезпечувати безперервність · Виходити	Чи може установа продовжувати виконувати юридичні обов'язки і вийти із залежності?	Результати навчань, незалежні тести, реагування на інциденти, навчання з виходу.

Таблиця I.2. Чотири сфери доказування.

I.8 Основоположні тести та поняття

I.8.1 Тест функціональної сфери застосування

I.8.1.1 Стандарт застосовується, якщо виконано три кумулятивні умови: (a) здійснюється публічна влада — справа стосується здійснення, організації, перегляду чи безперервності конституційно значущої публічної функції, яку виконує публічний орган безпосередньо або приватний суб'єкт від його імені; (b) цифрова система суттєво впливає на це здійснення, формуючи його зміст, процедуру чи результат інакше, ніж було б без неї; (c) цей вплив має конституційне значення — зачіпає законність, підзвітність, права, демократичне врядування чи інституційну стійкість.

I.8.1.2 Суттєвий вплив може здійснюватися через рекомендації, налаштування за замовчуванням, офіційні реєстри чи сукупний ефект маршрутизації послуг. Значення має фактична робота системи, а не її назва: інструмент, названий «підтримкою рішень», може фактично визначати результати за лише номінальної участі людини.

I.8.1.3 Невиконання будь-якої умови виводить справу за межі сфери застосування Стандарту. Звичайні цифрові зручності без суттєвого публічно-правового значення не охоплюються; невелика система може все ж підпадати під Стандарт, якщо вона впливає на права чи перегляд. Невизначеність не доводить, що функція перебуває поза сферою застосування: неясна межа потребує доказів і задокументованої попередньої оцінки, а межу переглядають, коли функція чи її залежності суттєво змінюються.

I.8.2 Тест участі приватного суб'єкта

I.8.2.1 Якщо приватний суб'єкт бере участь у функції, що відповідає тесту функціональної сфери застосування, тест участі приватного суб'єкта з'ясовує, чи зумовлює така участь публічну відповідальність, що не підлягає делегуванню, та посилений контроль. Його складові: (a) функціональна заміна — суб'єкт виконує завдання, яке інакше мала б виконувати публічна установа; (b) практична незамінність — оцінюється через документацію, права на аудит, контроль над змінами, збереження доказів і здатність до виходу; (c) витіснення підзвітності — звичайні механізми публічно-правової підзвітності (обґрунтування, перегляд, засоби захисту) не досягають суб'єкта безпосередньо.

I.8.2.2 Якщо виконано всі складові, діяльність суб'єкта оцінюють так само суворо, як діяльність публічного органу, що виконує ідентичну функцію, і потрібен посилений контроль; серйозна окрема залежність може виправдовувати цільові запобіжники. Тест визначає потреби врядування. Питання присвоєння дій державі, прямої відповідальності постачальника та можливості оскаржити його дії в суді вирішуються застосовним правом.

I.8.2.3 Тест функціональної сфери застосування і тест участі приватного суб'єкта відповідають на різні питання послідовно й не зливаються: перший визначає публічно-правову справу, другий — чи несе конкретний приватний учасник у ній публічно-правові обов'язки.

DRAFT

I.8.3 Шестирівнева архітектура врядування

Рівень	Ключове питання
1. Конституційний і нормативно-правовий	Які повноваження, права, обов'язки та галузеві правила становлять функцію і чи відповідає мандат вимогам законності та пропорційності?
2. Інституційна відповідальність	Хто володіє функцією, фінансує, експлуатує, контролює й змінює її і чи простежується ця відповідальність крізь делегування та відносини з постачальниками?
3. Дані та інфраструктура	Від яких реєстрів, моделей, інтерфейсів, хмарних сервісів, механізмів інтероперабельності та архітектури безпеки залежить функція?
4. Рішення та надання послуг	Як функція виконується в момент ухвалення рішення — через алгоритми, автоматизацію чи структуру розсуду?
5. Підзвітність і нагляд	Чи досягають обґрунтування, аудит, скарги, апеляції та судовий контроль записів, створених на рівні рішень?
6. Стійкість і безперервність	Що відбувається з функцією під час збою, виходу постачальника, атаки, кризи чи переходу?

Таблиця I.3. Шестирівнева архітектура врядування.

I.8.3.1 Рівні аналітично відокремлені, але інституційно взаємозалежні. Вада на одному рівні зазвичай виявляється на іншому: непростежувана відповідальність (рівень 2) проявляється під час перевірки підзвітності (рівень 5); неперевірена залежність (рівень 3) стає кризою безперервності під час поновлення договору (рівень 6). Архітектура є причинно-наслідковою картою, а не сьомою контрольною точкою чи паралельним переліком перевірки.

I.8.4 Конституційна інфраструктура

I.8.4.1 Конституційна інфраструктура — цифрові системи (системи ідентифікації, реєстри, хмарні рішення, рівні інтероперабельності), які стали частиною інституційного фундаменту, через який особи реалізують права, а публічні органи виконують конституційні функції, тож їхня відмова перериває конституційне життя, а не лише створює операційні незручності. Інфраструктура є конституційно критичною, якщо її відмова чи втрата контролю над нею унеможливлює реалізацію основних прав або законне функціонування влади.

I.8.5 Публічна відповідальність, що не підлягає делегуванню

I.8.5.1 Орган публічної влади може делегувати завдання, не делегуючи пов'язаної з ним підзвітності: підзвітність не передається разом із завданням. Технічний аутсорсинг не може залишити особу без підзвітної установи чи дієвого шляху до виправлення. Твердження «відповідає постачальник» не є законною заміною інституційної підзвітності.

Частина II — Метод: оцінювання впливу цифрового публічного права

II.1 Природа методу

II.1.1 Стандарт визначає умови, які мають залишатися виконаними; DPLIA — визначений Стандартом метод, яким перевіряють, чи виконуються вони в конкретній публічній функції. DPLIA не замінює спеціалізованих правових, технічних, оцінок ризиків чи впливу на права там, де вони залишаються обов'язковими за законом. Метод розглядає їхні результати разом, як докази, у світлі Нормативного ядра.

II.1.2 Метод має бути здатним дійти сприятливого висновку, якщо докази це підтримують. Його цінність — у якості обґрунтувань, рішень і запобіжників, а не в кількості несприятливих висновків чи обсязі документації.

II.1.3 Контрольні точки — це висновки, а не бали. Жодного сукупного бала не обчислюють; законність неможливо встановити додаванням сприятливих оцінок спроможностей чи зважуванням незаконного дизайну проти очікуваної ефективності.

II.2 Шість кроків

II.2.1 DPLIA складається з шести кроків. Нумерація кроків упорядковує роботу; вона не дозволяє остаточно пройти контрольну точку до перевірки доказів, від яких вона залежить. Докази, отримані на пізнішому кроці, можуть змінити будь-який попередній висновок, а суттєва зміна може повернути оцінювання до кроку 1. Ранні висновки є попередніми, якщо залежать від пізніших доказів; інституційне рішення вимагає їх узгодження.

Крок	Назва	Зміст роботи	Результат у Файлі
1	Сфера застосування	Відкрити Файл на етапі задуму політики, закупівлі, поновлення, суттєвої зміни чи інциденту; визначити відповідальну особу, очікуваний результат і момент ухвалення рішення; застосувати тест функціональної сфери застосування; визначити ступінь перевірки (III.3).	Висновок скринінгу; відповідальна особа; межі; ступінь перевірки; підстава для повторного розгляду.
2	Карта функції	Визначити межі та залежності функції; скласти карту шести рівнів; застосувати тест участі приватного суб'єкта; визначити осіб, яких це стосується; скласти покажчик залучених спеціалізованих доказів.	Карта функції; покажчик залежностей і доказів; аналіз осіб, яких це стосується.
3	Шість контрольних точок	Перевірити функцію за кожною контрольною точкою та оцінити десять спроможностей, фіксуючи джерело доказів і рівень впевненості для кожного висновку.	Висновки за контрольними точками з підвисновками; оцінки спроможностей.

Крок	Назва	Зміст роботи	Результат у Файлі
4	Причинно-наслідковий синтез	Розглянути висновки за контрольними точками, спроможностями та рівнями як причинно-наслідкові ланцюги; окремо зазначити ризик, впевненість у доказах і цілісність впровадження.	Причинно-наслідковий синтез; залишкові ризики; окремі думки.
5	Інституційне рішення	Ухвалити мотивоване рішення в одній з восьми категорій з умовами, відповідальними, строками та наслідками.	Підписане рішення; реєстр умов; висновок за результатами оцінювання.
6	Перегляд упродовж життєвого циклу	Відстежувати роботу, повідомлення і засоби захисту; повторно оцінювати за графіком чи в разі суттєвої зміни; керувати переходом або виходом.	Календар переглядів; журнал підстав; оновлені висновки.

Таблиця II.1. Шість кроків DPLIA.

Крок 1 — Сфера застосування

II.2.2 Оцінювання розпочинається, коли функцію задумують, закуповують, поновлюють, суттєво змінюють або коли вона причетна до інциденту. Відповідальна установа відкриває Файл, призначає відповідальну особу та фіксує очікуваний публічний результат і рішення, для якого проводиться оцінювання. Тест функціональної сфери застосування (I.8.1) застосовується один раз, до оцінювання будь-якої контрольної точки; сам тест контрольною точкою не є.

II.2.3 Для функції, визнаної такою, що перебуває поза сферою застосування, складається мотивований запис скринінгу із зазначенням відповідальної особи та підстави для повторного розгляду. Звичайні юридичні та адміністративні обов'язки продовжують діяти. Для функції в межах сфери застосування установа визначає ступінь перевірки відповідно до III.3 і фіксує підстави.

Крок 2 — Карта функції

II.2.4 Карта функції визначає її межі та залежності: суб'єктів, дані, системи, постачальників, засоби захисту та резервні механізми, на які функція спирається. Вона відображає функцію на шести рівнях (I.8.3), застосовує тест участі приватного суб'єкта (I.8.2) до кожного суттєвого приватного учасника та визначає осіб, яких це стосується, їхню вразливість та інтереси, на які це впливає.

II.2.5 Спеціалізовані докази — оцінка впливу на захист даних, оцінка впливу на основоположні права (FRIA), тест безпеки — включаються до переліку доказів за посиланням із зазначенням джерела, версії, розпорядника, правової сфери та статусу перевірки. Завершений спеціалізований звіт — це доказ, який треба оцінити, а не остаточна відповідь на кожне питання його предмета. Доречне питання — що він встановлює щодо цієї функції і що лишається невирішеним на стиках.

Крок 3 — Шість контрольних точок

II.2.6 Шість публічно-правових контрольних точок («шість контрольних точок») перетворюють застосовні правові та конституційні вимоги до функції на чіткі висновки. Для кожної контрольної точки визначено ключове питання, питання, які вона охоплює, і правило блокування. Повне

оцінювання охоплює всі шість контрольних точок; будь-яке підпитання, визнане незастосовним, потребує задокументованої підстави.

Контрольна точка	Ключове питання	Охоплює	Правило блокування
1. Законний мандат	Чи має установа конкретну юридичну компетенцію та легітимну публічну мету для цієї функції?	Компетенцію та юрисдикцію; конкретність повноважень; публічну мету й коло осіб; обмеження мети; відповідність закодованого правила правовому.	Функція не може тривати без чіткої, чинної й достатньо конкретної правової підстави для її мети та кола осіб.
2. Дизайн, обґрунтований правами	Чи є дизайн необхідним, пропорційним, недискримінаційним і доступним з огляду на наявні альтернативи?	Докази проблеми та альтернативи; менш втручальні засоби; вигоди, тягарі та зворотність; групові й розподільчі наслідки; доступність; вразливість.	Дизайн не може бути впроваджений, якщо менш втручальний засіб досягає тієї ж мети або якщо групові наслідки не оцінено для функції 2-го чи 3-го ступеня перевірки. Звітування не може виправити незаконну дискримінацію чи непропорційне втручання.
3. Публічна відповідальність	Чи можна визначити одну публічну установу з поіменно визначеним відповідальним за рішення, яка відповідає за функцію?	Законний розподіл відповідальності між публічними, приватними й розподіленими суб'єктами; делегування, закупівлі та використання даних; шляхи ескалації.	До укладення закупівельних зобов'язань функція повинна мати поіменно визначеного публічного відповідального за рішення.
4. Операційний контроль	Чи може установа законно й дієво врядовувати дані, код, постачальників, зміни та втручання, що суттєво формують функцію?	Законний доступ до даних і їх виправлення; договірний контроль над суттєвими залежностями; контроль змін, версіонування, доступ до журналів і незалежне тестування; здатність перевіряти, виправляти, обмежувати й перенаправляти.	Для функцій, що зачіпають права, нездатність перевірити, втрутитися чи виправити суттєвий вплив блокує впровадження, доки контроль не доведено. Нереалізованої договірної обіцянки самої по собі недостатньо.

Контрольна точка	Ключове питання	Охоплює	Правило блокування
5. Докази, перегляд і засоби захисту	Чи можуть установа та особа відтворити, зрозуміти, оскаржити й виправити суттєвий результат чи збій?	Адміністративні й технічні докази; зрозумілі обґрунтування; змістовний людський чи інституційний перегляд; готовність до скарг, апеляцій, звернень до омбудсмена, регулятора й судового контролю; виправлення індивідуальних і системних помилок, зокрема їх поширення.	Для функцій, що зачіпають права, відсутність достатніх доказів, змістовного оскарження чи дієвого виправлення блокує звичайне впровадження. Опублікований опис чи номінальна присутність людини не доводять наявності засобу захисту.
6. Безперервність і вихід	Чи може установа виконувати юридичні обов'язки під час збою, атаки, відмови постачальника, змін, поновлення чи припинення договору та вийти без відмови від прав, доказів чи послуг?	Перевірена безперервність і нецифровий резерв; управління інцидентами та безпечне обмеження функціональності; переносимість, перехід і допомога в переході; збереження доказів, незавершених проваджень і виправлень під час переходу.	Безперервність і вихід перевіряються до того, як рішення про поновлення чи розірвання договору стане неминучим, а не після того, як залежність стала незворотною.

Таблиця II.2. Шість публічно-правових контрольних точок

II.2.7 Контрольна точка 4 не є загальною оцінкою кібербезпеки і не вирішує, чи має особа ефективний засіб захисту, — це питання контрольної точки 5. Контрольна точка 1 встановлює повноваження, яких жодна технічна спроможність не може забезпечити.

Крок 4 — Причинно-наслідковий синтез

II.2.8 Дотримання застосовного права неможливо встановити, аналізуючи алгоритм чи технічний компонент окремо. Причинно-наслідковий синтез розглядає висновки за контрольними точками, спроможностями та рівнями разом як ланцюги й ставить щодо кожного суттєвого висновку питання: (a) яка вихідна умова; (b) через який рівень вона поширюється; (c) який запобіжник має перервати поширення і чи його справді застосовували, чи лише задокументували; (d) який ризик лишається з урахуванням реального, а не номінального ефекту запобіжника. Сприятлива оцінка кожного компонента окремо не замінює аналізу їх спільної дії.

II.2.9 Три доказові судження фіксуються окремо і ніколи не зливаються:

- **Ризик** — потенційна шкода: тяжкість, імовірність, масштаб, тривалість, вразливість, зворотність і поширення.
- **Впевненість у доказах** — обґрунтованість висновку: висока, якщо чинні докази перевірено й належно підтверджено; помірна, якщо доступ чи тестування обмежені; низька, якщо докази відсутні, припущені чи суттєво оспорені.

- **Цілісність впровадження** — чи запобіжники розподілено, забезпечено ресурсами, відстежуються і реально застосовуються.

II.2.10 Низька оцінена ймовірність не компенсує відсутності доказів юридичних повноважень чи засобу захисту. Договірне право не доводить достатності персоналу чи дієвого використання.

Крок 5 — Інституційне рішення

II.2.11 Відповідальна установа ухвалює і документує мотивоване публічно-правове судження в одній з восьми категорій.

Категорія рішення	Коли застосовується	Типова підстава
Продовжити	Усі контрольні точки мають висновок «Пройдено» або «Не застосовується»; спроможності доведено з високою впевненістю в доказах.	Прогалин у спроможностях не виявлено.
Продовжити за обов'язкових до виконання умов	Контрольні точки мають висновок «Пройдено» або «Умовно»; один чи кілька запобіжників слабкі, але їх можна виправити, визначивши відповідального і строк.	Право на аудит існує, але не перевірене.
Пілот у контрольованих умовах	Нове застосування, докази щодо якого ще тільки мають з'явитися.	Спроможність закладена в дизайні, але не має історії застосування.
Переробити й подати повторно	Контрольну точку не пройдено, але функція в принципі законна за умови переробки.	Не забезпечено прав на доступ до даних чи аудит.
Зупинити	Брак спроможності створює триваючий ризик для прав, поки триває переробка.	Ризик активної шкоди.
Припинити	Функцію неможливо здійснювати законно за жодного реального дизайну.	Контрольну точку не пройдено, і це неможливо виправити.
Отримати додаткові юридичні повноваження	Дизайн функції обґрунтований, але бракує достатньої правової підстави.	Непроходження контрольної точки 1, не пов'язане з операційним контролем.
Передати на незалежне визначення	Впевненість у доказах надто низька, щоб оцінювач дійшов висновку.	Докази контролює постачальник або вони недоступні.

Таблиця II.3. Вісім категорій інституційного рішення.

II.2.12 У кожному рішенні фіксуються підстави, окремі думки, запобіжники, умови, поіменно визначені відповідальні, строки та наслідок, що настає автоматично, якщо умову не виконано вчасно. Умова без відповідального і строку умовою не є. «Продовжувати моніторинг» чи «відстежувати» — недостатня умова.

II.2.13 Умови можуть стосуватися вдосконалення під час законної роботи, але передумови мають бути перевірені до початку залежної діяльності. Висновок «Умовно» не дозволяє звичайного повного впровадження, якщо не виконано вимоги, що блокує.

II.2.14 Пілот потребує чинної правової підстави, захисту учасників, обмеженої сфери та механізму зупинки. Він не може бути винятком із заборони чи заміною правового мандата.

II.2.15 Підзвітна установа підписує рішення, визначає, хто перевіряє виконання умов, і фіксує дату наступного перегляду. Погодження постачальника не замінює публічного рішення. Докази того, що шкода вже завдається, вимагають негайних законних захисних заходів ще до завершення повнішого оцінювання.

Крок 6 — Перегляд упродовж життєвого циклу

II.2.16 Оцінювання не завершується з дозволом чи впровадженням. Суттєва зміна законодавства, мети, даних, моделей, конфігурації системи, постачальників, інфраструктури, ризику чи інституційної спроможності знову відкриває відповідні контрольні точки. Функція, схвалена як пілот, не може розширювати коло осіб, мету, дані чи інституційне охоплення без задокументованого повторного оцінювання: непомітне розширення без оцінювання не допускається. Рішення чинне лише в межах оціненої сфери та умов; невиконання умов тягне наслідок, визначений у рішенні, зокрема обмеження чи зупинення, якщо це виправдано.

II.2.17 Під час кожного перегляду установа підтверджує, що:

- календар повторних оцінювань і журнал підстав ведуться й актуальні;
- кожен висновок «Умовно» має відповідального, строк, метод перевірки та наслідок;
- безперервність і вихід перевірено до того, як рішення про поновлення чи розірвання договору стало неминучим;
- перегляд після впровадження охопив інциденти, дрейф моделі, скарги, виправлення та нерівні наслідки для різних груп.

II.2.18 Планування виходу починається на етапі дизайну та закупівлі, хоча його виконання фіксується на кроці 6. Перехід чи припинення зберігає обов'язки з надання послуг, докази, незавершені вимоги та підзвітність.

II.3 Висновки за контрольними точками та оцінки спроможностей

II.3.1 Висновки за контрольними точками. Кожна контрольна точка отримує один мотивований висновок:

Висновок	Значення
Пройдено	Доведено достатні повноваження та запобіжники.
Умовно	Вимогу можна виконати через обов'язкову до виконання, обмежену в часі умову до чи під час контрольованого впровадження. Умова має відповідального, строк, метод перевірки та наслідок невиконання.

DRAFT

Висновок	Значення
Не пройдено	Механізм не може законно діяти без переробки, додаткових повноважень чи припинення.
Невизначено	Впевненість у доказах надто низька для відповідального висновку; потрібні додаткові докази чи незалежне визначення.
Не застосовується	Функція в межах визначеної сфери не зачіпає цієї контрольної точки з задокументованих підстав.

Таблиця II.4. П'ять висновків за контрольними точками.

II.3.2 Для кожного висновку зазначається, чи його докази прямі, залучені зі спеціалізованої оцінки чи виведені. «Частково» не є висновком за контрольною точкою.

II.3.3 Відсутність належних повноважень, підзвітної установи, суттєвих доказів для перегляду чи змістовного засобу захисту блокує звичайне впровадження, що зачіпає права. Заборонене чи незаконно дискримінаційне використання неможливо «врівноважити». Висновок «Невизначено» щодо вимоги, яку не можна компенсувати, спричинений відсутністю, а не несприятливістю доказів, має такі самі наслідки для впровадження, як «Не пройдено», доки не отримано достатніх доказів. Критичні вади безперервності чи виходу так само блокують механізм, відмова якого унеможливила б виконання юридичних обов'язків.

II.3.4 Оцінки спроможностей. Кожна з десяти спроможностей оцінюється як «Так», «Частково» чи «Ні». Для кожної спроможності оцінювач розмежовує три питання, адже позитивні відповіді на перші два сумісні з негативною відповіддю на третє: (a) чи має установа юридичне повноваження чи право — законодавчий мандат, договірне положення про аудит, задокументоване право скасувати дію; (b) чи має вона практичну спроможність і ресурси, щоб його реалізувати, — навчений персонал, технічний доступ, час; (c) чи було спроможність продемонстровано в реалістичних умовах? Тестування може проводитися у формі імітації чи навчань, якщо реальне тестування загрожує правам чи безперервності послуг.

II.3.5 Твердження постачальника без інституційних доказів обмежує оцінку рівнем «Частково». Договір, що обіцяє переносимість даних, сам по собі не доводить спроможності «Виходити»; політика, що дозволяє людині скасувати рішення, не доводить спроможності «Втручатися», якщо уповноваженим посадовцям бракує часу, інформації чи статусу; публічний реєстр прозорості не доводить спроможності «Пояснювати» на рівні конкретності, потрібному для індивідуального оскарження; право на аудит отримує оцінку «Так» лише тоді, коли його реалізовано, а не лише передбачено.

II.3.6 Рівні доведеності. Докази запобіжника класифікуються як «задокументовано» (запобіжник існує на папері), «застосовано» (його застосовано щонайменше один раз) або «перевірено» (його перевірено в реалістичних умовах). Мінімальний рівень доведеності залежить від ступеня перевірки (III.3).

DRAFT

II.4 Орієнтовні зв'язки між спроможностями та контрольними точками

II.4.1 У кожному оцінюванні пояснюється, які оцінки спроможностей підтримують чи підривають кожен висновок за контрольною точкою. Наведені зв'язки орієнтовні й перетинаються; вони не групують спроможності та не замінюють сфер доказування.

Контрольна точка	Спроможності, що зазвичай дають докази
1. Законний мандат	Жодна не може забезпечити юридичних повноважень; «Розуміти» і «Документувати» дають докази відповідності закодованого правила правовому.
2. Дизайн, обґрунтований правами	Розуміти, Спрямовувати, Документувати.
3. Публічна відповідальність	Спрямовувати, Документувати.
4. Операційний контроль	Спрямовувати, Перевіряти, Виправляти, Втручатися.
5. Докази, перегляд і засоби захисту	Документувати, Перевіряти, Пояснювати, Виправляти, Зберігати докази.
6. Безперервність і вихід	Втручатися, Зберігати докази, Забезпечувати безперервність, Виходити.

Таблиця II.5. Орієнтовні доказові зв'язки.

II.5 Життєвий цикл системи

II.5.1 Шість кроків DPLIA відрізняються від шести фаз життєвого циклу системи, до яких застосовується DPLIA: (1) стратегічний задум; (2) дизайн і закупівля; (3) розробка та впровадження; (4) операційне врядування; (5) перегляд і адаптація; (6) припинення чи перехід. DPLIA можна застосовувати повністю або з глибиною, якої вимагає ступінь перевірки, у будь-якій фазі. Режими використання в III.1 відповідають цим фазам.

DRAFT

Частина III — Застосування

III.1 Шість режимів використання

III.1.1 Стандарт і DPLIA використовуються в шести пов'язаних режимах. Перші чотири — звичайні способи використання впродовж життєвого циклу; ще два поширюють Стандарт на виняткові події та системний аналіз. У кожному режимі Нормативне ядро є мірилом, а DPLIA — методом, яким досліджуються вади, невизначеність, причинно-наслідкові зв'язки, потрібні запобіжники та інституційні наслідки.

Режим	Що перевіряється
1. Перспективне оцінювання	До дизайну, закупівлі чи законодавчого дозволу: чи можна взагалі законно створити запропоновану цифрову публічну функцію.
2. Перегляд на етапі дизайну та розробки	Під час дизайну і створення: чи відповідає архітектура, що формується, контрольним точкам, поки зобов'язання ще можна змінити.
3. Оцінювання перед впровадженням	До схвалення, дозволу чи запуску: чи відповідає Стандарту функція в тому вигляді, в якому її створено, а не задумано.
4. Операційний перегляд і перегляд упродовж життєвого циклу	Під час звичайної роботи: чи функція й надалі відповідає Стандарту і чи потребує суттєва зміна повторного оцінювання.
5. Перегляд у зв'язку з інцидентом, збоєм, скаргою, судовим провадженням чи суперечкою	У відповідь на конкретну подію: яку контрольну точку чи рівень подія оголює і якого виправлення потребує.
6. Системний, порівняльний, законодавчий чи інституційний перегляд	Для кількох функцій, юрисдикцій чи сектору: закономірності, яких не видно в оцінюванні однієї функції.

Таблиця III.1. Шість режимів використання.

III.1.2 Кожне використання потребує визначеного наслідку для рішення та подальшого перегляду. Оцінювання запропонованої системи може завершитися переробкою чи відмовою від впровадження; оцінювання чинної функції може вимагати негайних захисних заходів поряд із довшим виправленням. Саме перегляд упродовж життєвого циклу (крок 6) робить кожен режим дієвим: перегляд, який нічого не змінює у Файлі, інституційного рішення не дає.

III.2 Файл цифрової публічної функції

III.2.1 Для кожного оцінювання ведеться один офіційний Файл цифрової публічної функції. Файл — інституційна пам'ять і доказова основа оцінювання, а не факультативний додаток. Це цілісний файл для ухвалення рішення, а не сховище документів: спеціалізовані докази включаються за посиланням із зазначенням джерела, версії, розпорядника та статусу перевірки, без дублювання договорів,

наборів даних чи журналів. Файл є офіційним адміністративним документом і зберігається відповідно.

III.2.2 Файл складається з шести розділів:

Розділ Файлу	Основний зміст
1. Скринінг і ступінь перевірки	Функція, відповідальна особа, підстава, висновки щодо сфери застосування, ступінь перевірки та його обґрунтування, межі, дата перегляду.
2. Функція та правова підстава	Мандат, мета, шлях ухвалення рішення, залежності, офіційний опис системи; відповідальна установа і підзвітна особа, що ухвалює рішення; системи, постачальники та приватні суб'єкти.
3. Врядування та особи, яких це стосується	Карта шести рівнів; тест участі приватного суб'єкта; розподіл відповідальності; особи, яких це стосується, їхні інтереси та вразливість; участь.
4. Контрольні точки та синтез	Висновки й підвисновки за контрольними точками із джерелом доказів; ризик, впевненість у доказах і цілісність впровадження; альтернативи; причинно-наслідковий синтез; окремі думки.
5. Спроможності та рішення	Оцінки десяти спроможностей із рівнями доведеності; запобіжники; інституційне рішення; умови, відповідальні, строки й наслідки; моніторинг, засоби захисту, безперервність і вихід.
6. Публічна підзвітність і життєвий цикл	Висновок за результатами оцінювання; публічне резюме; відповіді на зауваження, отримані під час обговорення; реєстровий запис; повідомлення й шляхи оскарження; дати переглядів, підстави, інциденти, зміни та подальші рішення.

Таблиця III.2. Шість розділів Файлу цифрової публічної функції.

III.2.3 Закупівельна документація має вимагати як попередніх умов укладення договору прав на аудит, докази, контроль змін і вихід, які перевіряють контрольні точки 3, 4 і 6. Право, заявлене вперше після підписання договору, свідчить про прогалину у Файлі, а не усуває її.

III.3 Ступені перевірки

III.3.1 Оцінювання проводиться на одному з трьох ступенів перевірки. Ступінь визначає, хто оцінює, скільки доказів потрібно і якою має бути незалежність перевірки. Це судження про пропорційність, яке ухвалюється на кроці 1 і переглядається щоразу, коли функція суттєво змінюється; воно не замінює висновків за контрольними точками.

	Ступінь 1 — Самооцінювання	Ступінь 2 — Перевірене оцінювання	Ступінь 3 — Незалежне оцінювання
Хто оцінює	Відповідальна установа.	Відповідальна установа з підписом поіменно визначеного рецензента, незалежного від функції, що оцінюється.	Сторона, незалежна від відповідальної установи.

	Ступінь 1 — Самооцінювання	Ступінь 2 — Перевірене оцінювання	Ступінь 3 — Незалежне оцінювання
Орієнтовні функції	Обмежене публічно-правове значення; зворотна допоміжна роль; немає автоматизації, що зачіпає права.	Суттєвий вплив на права, послуги чи довіру; помірна незворотність.	Високе конституційне значення чи незворотність; висока приватна залежність; масштабний вплив на вразливі групи; висновки, що блокують, чи оспорювані докази.
Мінімальний обсяг Файлу	Стислий Файл; поіменно визначена відповідальна особа; відповідні докази; пропорційний моніторинг. Контрольні точки можна зафіксувати як «Пройдено» чи «Не застосовується» на мінімальних доказах із зазначенням підстав.	Повний Файл; повний аналіз шести контрольних точок; публічне резюме; спеціалізовані додатки, яких вимагає функція.	Повний покажчик доказів; залучення осіб, яких це стосується; схвалення на вищому рівні керівництва.
Мінімальний рівень доведеності	Задокументовано.	Застосовано — для кожного суттєвого запобіжника.	Перевірено — для спроможностей, ключових для законності, засобів захисту, безперервності та виходу.
Результат	Висновок за результатами оцінювання за Стандартом.	Висновок за результатами оцінювання за Стандартом.	Висновок за результатами оцінювання за Стандартом.

Таблиця III.3. Три ступені перевірки.

III.3.2 Вибір ступеня. Ступінь визначається впливом функції, вразливістю осіб, яких це стосується, масштабом, зворотністю, приватною залежністю, новизною та асиметрією доказів. Самі лише назви на кшталт «правосуддя», «ідентифікація» чи «соціальне забезпечення» не визначають ступеня: треба проаналізувати функцію, її наслідки та залежності.

III.3.3 Конституційно критичні функції. Функція, що експлуатує конституційно критичну інфраструктуру (I.8.4), оцінюється на ступені 3 і додатково потребує поглибленого тестування безперервності та виходу, навчань з реагування на інциденти, періодичної незалежної перевірки, внесення до публічного реєстру та відповідальності вищого керівництва за безперервність основних публічних обов'язків.

III.3.4 Умови проведення оцінювання. Донорські, транскордонні, надзвичайні, безпекові чи галузеві умови можуть додавати вимоги. Вони ніколи не знижують ступеня перевірки і не зменшують глибини змістовного оцінювання. Та сама функція не отримує нижчого публічно-правового стандарту через те, що оцінювання замовлено для цілей фінансування.

III.3.5 Поза сферою застосування. Функції, яка не відповідає тесту функціональної сфери застосування, ступінь перевірки не присвоюється. Для неї складається запис скринінгу, передбачений II.2.3.

III.4 Висновок за результатами оцінювання

III.4.1 На кожному ступені перевірки результатом оцінювання є висновок за результатами оцінювання за Стандартом. У ньому зазначаються: функція та відповідальна установа; ступінь перевірки, особа оцінювача чи рецензента та його незалежність; сфера, критерії та використані докази, а також дата перевірки доказів; висновок за кожною контрольною точкою; оцінки десяти спроможностей і рівні доведеності; впевненість у доказах; інституційне рішення відповідальної установи, якщо його ухвалено; дата наступного перегляду.

III.4.2 Висновок за результатами оцінювання не є сертифікатом, знаком відповідності, декларацією законності чи заявою про те, що система відповідає вимогам. Його висновки підтримують, а не замінюють рішення компетентної установи. Завершення оцінювання ніколи не створює презумпції законності. Висновок чинний лише для зазначених у ньому сфери, версії та дати; Стандарт не визнає висновку, що ґрунтується на оцінюванні, не задокументованому в чинному Файлі.

III.5 Форми запровадження та юридична сила

III.5.1 Компетентний орган може надати Стандарту юридичної сили, закріпивши його як законодавчий обов'язок, міністерську чи адміністративну інструкцію, стандарт публічної служби чи судового адміністрування, закупівельну вимогу, метод регулятора, орієнтир для омбудсмена чи аудиту, запобіжну вимогу донора або добровільну політику. Юридична сила Стандарту залежить від акта про запровадження.

III.5.2 В акті про запровадження слід визначити орган, що його ухвалює, та його компетенцію, версію Стандарту, функції, на які він поширюється, і внутрішні наслідки недотримання. Акт розмежовує чинні юридичні обов'язки та додаткові зобов'язання, взяті як інституційна політика.

III.5.3 Акт про запровадження щонайменше має передбачати, що:

- кожна запропонована чи суттєво змінена цифрова публічна функція проходить скринінг до закупівлі, впровадження чи незворотного проєктного рішення;
- відповідальний орган публічної влади поіменно визначено, і він не може передати остаточну публічно-правову відповідальність за договором;
- функції ступеня перевірки 3 і конституційно критичні функції проходять незалежне оцінювання;
- висновки за контрольними точками відокремлено від оцінок ризику та вигод;
- спеціалізовані оцінки включаються за посиланням і узгоджуються в єдиному комплексному висновку;
- установа підтримує десять спроможностей контролю пропорційно впливу;
- публічні резюме та індивідуальні обґрунтування надаються з урахуванням законних винятків;
- моніторинг, повторне оцінювання, реагування на інциденти та вихід є обов'язковими елементами життєвого циклу;
- Файл цифрової публічної функції є офіційним адміністративним документом і зберігається відповідно.

DRAFT

III.5.4 Закупівлі мають забезпечувати механізми аудиту, документування, контролю змін, втручання, безперервності та виходу, яких потребують спроможності. Менші установи можуть використовувати спільну експертизу чи поєднувати ролі, розкриваючи конфлікти інтересів і зберігаючи незалежну критичну перевірку. Установі слід задокументувати, як вона фінансуватиме персонал, перевірки, участь і тестування, а не брати на себе обов'язки, виконати які не може.

III.5.5 Установі, що запровадила Стандарт, слід вести публічний реєстр, у якому для кожної оціненої функції зазначено відповідальну установу, дату оцінювання, застосовану версію Стандарту, ступінь перевірки, рішення, наступний перегляд і доступний шлях оскарження. Дворівнева структура оприлюднення може захищати чутливу інформацію, водночас підтримуючи підзвітність; будь-яке обмеження розкриття потребує законної мотивованої підстави й належного доступу для компетентних незалежних рецензентів.

III.5.6 DPLIA слід інтегрувати в чинне врядування, а не доручати окремому «етичному» підрозділу. Координаційна функція може бути в міністерстві юстиції, секретаріаті уряду, урядовій цифровій службі, вищому органі аудиту чи міжвідомчому підрозділі з перевірки відповідності; операційна відповідальність залишається за органом, що виконує функцію.

III.6 Участь і прозорість

III.6.1 Участь починається до того, як ухвалено суттєві рішення. У Файлі зазначається, кого вислухано, чий досвід не представлено, що змінилося в результаті та чому відхилено альтернативи. Публічні резюме допомагають виявляти проблеми; обґрунтування в конкретних справах і дієві шляхи подання скарг забезпечують засоби захисту. Прозорість діє на трьох рівнях — реєстру, системи та справи, — і запис у реєстрі сам по собі не замінює обґрунтування чи засобу захисту в конкретній справі.

III.7 Співвідношення з іншими інструментами

III.7.1 Публічний орган може виконати кожен галузевий обов'язок окремо, тоді як комплексна функція, якої вони разом стосуються, залишиться неоціненою. Стандарт покликаний усунути саме цю прогалину, а не конкурувати з інструментами, які надають йому докази. Його використовують разом із ними так.

Інструмент	Докази, які він надає	Що додає Стандарт
Рамкова конвенція Ради Європи про штучний інтелект і HUDERIA	Контекст, участь, вплив на права людини, демократію та верховенство права і заходи пом'якшення впродовж життєвого циклу системи ШІ.	Рівень конституційної законності та інституційного контролю: висновки за контрольними точками з урахуванням юрисдикції, спроможності контролю та підзвітне інституційне рішення, зокрема щодо компонентів, не пов'язаних зі ШІ.

DRAFT

Інструмент	Докази, які він надає	Що додає Стандарт
Оцінка впливу на основоположні права (FRIA) за Актом ЄС про штучний інтелект (ст. 27)	Групи, яких це стосується, конкретні шкоди, нагляд, врядування та скарги в межах її правової сфери.	Відповідальність і залежності в усій публічній функції. Стандарт не замінює FRIA.
Вимоги Акта ЄС про штучний інтелект до систем високого ризику	Докази щодо власних технічних і організаційних вимог до системи ШІ.	Оцінювання комплексної публічної функції, а не системи окремо.
Оцінка впливу на захист даних за GDPR (ст. 35)	Цілі обробки, необхідність, ризики, запобіжники та перегляд.	Інституційні повноваження, залежності поза обробкою даних, загальні засоби захисту, безперервність і вихід.
ISO/IEC 42001	Докази організаційного врядування ШІ.	Вони відповідають на різні питання. Сертифікація за 42001 є доречним доказом, але не доказом законності.
Управління ризиками кібербезпеки за NIS2	Стійкість мережевих та інформаційних систем.	Законність, права та підзвітність функції, яку підтримують ці системи.
Оцінка за Актом про інтероперабельну Європу	Правові, організаційні, семантичні й технічні наслідки для транскордонної інтероперабельності.	Чи може особа рівною мірою реалізувати право, коли системи обмінюються даними; комплексна відповідальність і безперервність.
Директива Канади про автоматизоване ухвалення рішень і AIA	Рівні впливу, юридичні консультації, тестування, перегляд і засоби захисту.	Докази щодо всієї функції там, де цифрове опосередкування виходить за інституційні чи системні межі Директиви.
NIST AI RMF	Добровільні докази та практики управління ризиками ШІ.	Застосовні публічно-правові обов'язки та їхні наслідки для інституційного рішення.

Таблиця III.4. Співвідношення з іншими інструментами.

III.7.2 Чинні інструменти вже підтримують інтеграцію: оцінка впливу на захист даних може охоплювати сукупність подібних операцій обробки, а FRIA за Актом ЄС про штучний інтелект прямо передбачає взаємодоповнюваність з такою оцінкою.

III.7.3 Широкий підхід HUDERIA до прав і верховенства права є змістовним джерелом сумісного аналізу, а її необов'язковий статус не применшує цінності методології. Канадська AIA уже передбачає перегляд упродовж життєвого циклу системи. DPLIA використовує такі напрацювання, а не претендує на аналіз життєвого циклу як на свій виключний внесок.

Частина IV — Ведення Стандарту та інструменти м’якого права

IV.1 Ведення і найменування

IV.1.1 Стандарт веде Інститут цифрового суспільства та публічного права майбутнього (далі — «Інститут») відповідно до Регламенту Інституту. До схвалення, описаного в IV.1.2, його називають «Стандарт цифрового публічного права „Влада над кодом“ Інституту», а до ухвалення додають слова «робочий проєкт для обговорення».

IV.1.2 Стандарт може називатися стандартом ЄОПП чи тимчасовим стандартом ЄОПП або описуватися як схвалений ЄОПП лише після його схвалення Виконавчим комітетом ЄОПП відповідно до Регламенту про стандарти ЄОПП. Схвалення не змінює тексту Стандарту.

IV.2 Публічне обговорення, ухвалення та зміни

IV.2.1 Ухвалення та зміни здійснюються відповідно до підпункту (f) пункту 3 статті IV Регламенту Інституту, згідно з яким стандарти та методології Інституту ухвалює Наукова рада за поданням Директора, і Рішення Наукової ради про порядок розроблення та ухвалення стандартів Інституту; застосовується також Регламент про стандарти ЄОПП. Згідно з цими положеннями:

- нова версія виноситься на публічне обговорення тривалістю щонайменше шістдесят (60) днів, будь-яка інша суттєва зміна — щонайменше тридцять (30) днів, і щодо кожного зауваження оприлюднюється рішення про його врахування;
- Стандарт і будь-які зміни до нього ухвалює Наукова рада за поданням Директора без участі членів, які мають у цьому інтерес, зокрема його авторів;
- кожна ухвалена версія має номер і дату та вноситься до публічного реєстру, який веде Інститут.

IV.2.2 Кожна зміна оприлюднюється разом з обґрунтуванням і переліком змінених вимог. У ній зазначається, як вона впливає на завершені й поточні оцінювання, та перехідні положення. У висновках за результатами оцінювання зазначається застосована версія Стандарту.

IV.2.3 Ведення Стандарту передбачає оприлюднення обов’язків, порядку участі, правил щодо конфлікту інтересів та історії версій. До нього залучаються органи публічної влади, фахівці з права та технологій, спільноти, яких це стосується, і незалежні дослідники.

IV.3 Інструменти м’якого права

IV.3.1 Стандарт впроваджується через інструменти м’якого права: керівні принципи; модельні положення договорів і модельні регуляторні положення; консультативні висновки Інституту; запити на зауваження; коментарі та тлумачні примітки; навчання й практичні посібники; заяви про сумісність з інструментами міжурядових організацій.

DRAFT

IV.4 Оцінювання, аудит і валідація відповідності

IV.4.1 Оцінювання, аудит і валідація відповідності, які здійснює Інститут чи які здійснюються на його замовлення, ґрунтуються на погодженій сфері, визначених критеріях і перевірюваних доказах. Інститут оформлює свої результати як висновки за Стандартом (III.4). Вони підтримують, але не замінюють рішення компетентної установи.

IV.4.2 Будь-яке публічне засвідчення результатів з ініціативи Інституту потребує окремого рішення Виконавчого комітету ЄОПП.

IV.5 Юридична сила та публічний статус

IV.5.1 Стандарт не має обов'язкової сили, доки компетентний орган не надасть йому юридичної сили власним актом (III.5). Ні Стандарт, ні висновок за результатами оцінювання не наділяють владними повноваженнями, не створюють презумпції законності і не надають Інституту чи будь-якому оцінювачеві особливого публічного статусу.

IV.6 Сертифікація персоналу

IV.6.1 Коли буде створено орган сертифікації компетентності осіб, сертифікація здійснюватиметься з дотриманням бар'єра неупередженості між навчанням, оцінюванням і сертифікацією, встановленим рішенням про створення цього органу.

DRAFT