АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
до проекту наказу Міністерства цифрової трансформації України «Про затвердження галузевих профілів безпеки систем, що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або операторам критичної інфраструктури»

I. Визначення проблеми

Відповідно до абзацу другого пункту 1 Положення про Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 року № 856, Мінцифри є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики, зокрема у сфері хмарних послуг.

Частина п’ята статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах» (далі – Закон) визначає, що органи державної влади, державні органи в межах своїх повноважень у відповідній сфері або галузі розробляють та за погодженням із Державною службою спеціального зв’язку та захисту інформації України затверджують галузеві профілі безпеки для відповідної сфери або галузі з урахуванням мінімальних вимог щодо заходів захисту (базового профілю безпеки), а також відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі.

Частиною шостою статті 10 Закону встановлено, що порядок затвердження цільових та галузевих профілів безпеки затверджується Кабінетом Міністрів України.

Відповідно до абзацу третього пункту 2 Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 року № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» (далі – Порядок авторизації), галузевий профіль безпеки системи — взаємопов’язана сукупність заходів щодо захисту інформації, визначених для системи органом державної влади, іншим державним органом у межах своїх повноважень у відповідній сфері або галузі з урахуванням мінімальних вимог щодо таких заходів із захисту (базового профілю), відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі, а також надання відповідних рекомендацій.

Абзацом четвертим пункту 2 Порядку авторизації визначено, що галузеві уповноважені органи – органи державної влади, інші державні органи, які в межах своїх повноважень у відповідній сфері або галузі затверджують галузевий профіль.

Механізм розроблення та затвердження галузевих профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем визначено Порядком розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженим постановою Кабінету Міністрів України від 18 червня 2025 року № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» (далі – Порядок розроблення).

Відповідно до абзацу першого пункту 4 Порядку розроблення галузевий профіль безпеки системи розробляється з урахуванням визначеного базового профілю безпеки системи для відповідної категорії систем залежно від інформації, що обробляється в них (відкрита інформація чи інформація з обмеженим доступом), відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі, а також надання відповідних рекомендацій, погоджується з Адміністрацією Держспецзв'язку та затверджується галузевим уповноваженим органом. Затверджений галузевий профіль безпеки системи протягом десяти днів з дати затвердження надсилається галузевим уповноваженим органом до Адміністрації Держспецзв'язку.

З огляду на зазначене та відповідно до частини п'ятої статті 10 Закону розроблено проект наказу Міністерства цифрової трансформації України «Про затвердження галузевих профілів безпеки систем, що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або операторам критичної інфраструктури» (далі – проект акта).

Проектом акта пропонується затвердити два окремі галузеві профілі безпеки, які враховують особливості захисту відкритої інформації та інформації з обмеженим доступом (конфіденційної та службової) відповідно до вимог законодавства.

Проект акта розроблено з урахуванням визначеного базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація, затвердженого наказом Адміністрації Держспецзв'язку від 30 червня 2025 року № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація» та базового профілю безпеки системи, де обробляється службова інформація, затвердженого наказом Адміністрації Держспецзв'язку від 02 липня 2025 року № 419 «Про затвердження базового профілю безпеки системи, де обробляється службова інформація».

Основні групи (підгрупи), на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни*	-	+
Держава	+	-

Суб’єкти господарювання,	+	-
у тому числі суб’єкти малого підприємництва*	-	+

Врегулювання зазначеного питання не може бути здійснено за допомогою ринкових механізмів, оскільки такі питання регулюються виключно нормативно-правовими актами.

Зазначена проблема не може бути розв’язана за допомогою діючих регуляторних актів через відсутність правового механізму у чинному законодавстві.

II. Цілі державного регулювання

Основними цілями державного регулювання є визначення диференційованих вимог безпеки щодо інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем (далі – системи), що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або критично важливим об’єктам інфраструктури залежно від категорії інформації, що в них обробляється (відкрита, конфіденційна або службова) та сукупності заходів з їх захисту.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Залишення існуючої ситуації без змін
Альтернатива 2	Прийняття наказу Міністерства цифрової трансформації України «Про затвердження галузевих профілів безпеки систем, що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або операторам критичної інфраструктури» (далі – наказ)

Інших альтернативних способів досягнення основної мети, ніж прийняття зазначеного регуляторного акта, не існує.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати

Альтернатива 1	Немає, оскільки залишення існуючої ситуації без змін не забезпечує виконання вимог частини п’ятої статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах» та, як наслідок, унеможливлює запровадження уніфікованих вимог до захисту державних даних і даних публічних користувачів/операторів критичної інфраструктури.	Немає, оскільки залишення існуючої ситуації без змін не передбачає додаткових витрат з державного та/або місцевих бюджетів, пов’язаних із впровадженням нового регуляторного акта.
Альтернатива 2	Прийняття наказу забезпечить системне підвищення національної безпеки через запровадження двох окремих галузевих профілів безпеки систем, що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або операторам критичної інфраструктури (далі – галузеві профілі), у яких обробляється відкрита та конфіденційна, а також службова інформація. Це уніфікує вимоги до захисту державних даних та мінімізує ризики кібератак на критичну інфраструктуру.	Реалізація проекту наказу не потребує додаткових коштів та не матиме прямого чи опосередкованого впливу на надходження та витрати державного та/або місцевого бюджетів. Фінансування видатків, необхідних для реалізації проекту наказу буде здійснюватися в межах бюджетних призначень, передбачених для функціонування відповідних центральних органів виконавчої влади Державним бюджетом України на відповідний бюджетний період та інших не заборонених законодавством джерел фінансування.

Оцінка впливу на сферу інтересів громадян

Оцінка впливу проекту акта на сферу інтересів громадян не здійснювалася, оскільки такий вплив відсутній.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	5	107	0	0	112
Питома вага групи у загальній кількості, відсотків	4.5%	95,5%	0%	0%	100%

Дані взято з офіційного сайту Державної служби статистики України в розділі «Кількість діючих суб'єктів великого, середнього, малого та мікропідприємництва за видами економічної діяльності за 2024 рік» (https://www.stat.gov.ua/). До уваги взято суб'єктів великого та середнього підприємництва з огляду на їхню фактичну участь та здатність забезпечити виконання високих регуляторних вимог у сфері надання хмарних послуг для державного сектору.

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає, оскільки відсутні єдині правила до захисту інформації в системах, що використовуються для надання хмарних послуг та/або послуг центру обробки даних.	Відсутні, оскільки залишення існуючої ситуації без змін не призводить до виникнення додаткових витрат для суб'єктів господарювання, пов'язаних із впровадженням чи виконанням положень нового регуляторного акта.
Альтернатива 2	Високі, оскільки затвердження галузевих профілів дозволить надавачам хмарних послуг та послуг центру обробки даних (далі – надавач) використовувати їх як уніфіковані основи для створення цільових профілів безпеки. Запровадження галузевих профілів забезпечить	Для суб'єктів господарювання витрати будуть пов'язані з ознайомленням з проектом акта і становитимуть 9 909,12 грн. на одного суб'єкта господарювання великого і середнього підприємництва.

	системний підхід до управління ризиками інформаційної безпеки у сфері хмарних послуг та сприятиме підвищенню рівня кібербезпеки шляхом зменшення вразливостей, мінімізації ризиків несанкціонованого доступу, кібератак та витоку даних.	Інші можливі витрати є індивідуальними та складно прогнозованими, оскільки залежать від: поточного рівня впровадження заходів з інформаційної безпеки; використання технічних рішень та організаційних політик управління безпекою інформації у кожного надавача.

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1 Сумарні витрати для суб'єктів господарювання великого і середнього підприємництва згідно з додатком 1 до АРВ (рядок 11 таблиці «Витрати на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта»)	0
Альтернатива 2 Сумарні витрати для суб'єктів господарювання великого і середнього підприємництва згідно з додатком 1 до АРВ (рядок 11 таблиці «Витрати на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта»)	1 109 821,44 грн

IV. Вибір найбільш оптимального альтернативного способу досягнення

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1	1	Мінімальний бал, який свідчить про неможливість досягнення мети державного регулювання

Альтернатива 2	4	Максимальний бал, який свідчить про можливість максимального досягнення мети державного регулювання

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1	Для держави: Немає, оскільки залишення існуючої ситуації без змін не забезпечує виконання вимог частини п’ятої статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах» та, як наслідок, унеможливлює запровадження уніфікованих вимог до захисту державних даних і даних публічних користувачів/операторів критичної інфраструктури. Для суб’єктів господарювання: Немає, оскільки відсутні єдині правила до захисту інформації в системах, що використовуються для надання хмарни	Для держави: Немає, оскільки залишення існуючої ситуації без змін не передбачає додаткових витрат з державного та/або місцевих бюджетів, пов’язаних із впровадженням нового регуляторного акта. Для суб’єктів господарювання: відсутні, оскільки залишення існуючої ситуації без змін не призводить до виникнення додаткових витрат для суб’єктів	Найменш ефективний у розв’язанні існуючої проблеми

	послуг та/або послуг центру обробки даних.	господарювання, пов’язаних із впровадженням чи виконанням положень нового регуляторного акта.	
Альтернатива 2	Для держави: Прийняття наказу забезпечить системне підвищення національної безпеки через запровадження двох окремих галузевих, у яких обробляється відкрита та конфіденційна, а також службова інформація. Це уніфікує вимоги до захисту державних даних та мінімізує ризики кібератак на критичну інфраструктуру.	Для держави: реалізація проекту наказу не потребує додаткових коштів та не матиме прямого чи опосередкованого впливу на надходження та витрати державного та/або місцевого бюджетів. Фінансування видатків, необхідних для реалізації проекту наказу буде здійснюватися в межах бюджетних призначень, передбачених для функціонування відповідних центральних органів виконавчої влади Державним бюджетом України на відповідний бюджетний період та інших не	Найбільш ефективний у розв’язанні існуючої проблеми

	Для суб’єктів господарювання: Високі, оскільки затвердження галузевих профілів дозволить надавачам хмарних послуг та послуг центру обробки даних (далі – надавач) використовувати їх як уніфіковані основи для створення цільових профілів безпеки. Запровадження галузевих профілів забезпечить системний підхід до управління ризиками інформаційної безпеки у сфері хмарних послуг та сприятиме підвищенню рівня кібербезпеки шляхом зменшення вразливостей, мінімізації ризиків несанкціонованого доступу,	заборонених законодавством джерел фінансування. Для суб’єктів господарювання витрати будуть пов’язані з ознайомленням з проектом акта і становитимуть 9 909,12 грн. на одного суб'єкта господарювання великого і середнього підприємництва. Інші можливі витрати є індивідуальними та складно прогнозованими, оскільки залежать від: поточного рівня впровадження заходів з інформаційної безпеки; використання технічних рішень та організаційних політик управління безпекою інформації у кожного надавача.	

	кібератак та витоку даних.		

Рейтинг	Аргументи щодо переваги обраної альтернативи/причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 1	Зазначений спосіб є неприйнятним, оскільки не забезпечується виконання вимог Закону	Х
Альтернатива 2	Зазначений спосіб забезпечує досягнення мети державного регулювання, а саме: досягнення цілей державного регулювання відповідно до вимог чинного законодавства.	На дію проекту акта можуть вплинути такі економічні та політичні фактори: економічна криза, військові дії, зміни в чинному законодавстві.

V. Механізми та заходи, які забезпечать розв’язання визначеної проблеми

Основним механізмом, що забезпечить розв’язання визначеної проблеми, є прийняття проекту акту.

Прийняття проекту акту дозволить встановити чіткі та уніфіковані вимоги безпеки до систем, що використовуються для надання хмарних послуг та/або послуг центрів обробки даних публічним користувачам та/або операторам критично важливої інфраструктури. Галузеві профілі визначають комплекс організаційних, технічних і процедурних заходів, спрямованих на захист інформації, що обробляється в таких системах, включно з відкритими, конфіденційними та службовими даними.

Запровадження галузевих профілів забезпечить системний підхід до управління ризиками інформаційної безпеки у сфері хмарних послуг та підвищення рівня національної та кібербезпеки шляхом зменшення вразливостей і мінімізації ризиків несанкціонованого доступу, кібератак та витоку даних.

Заходи, які повинні здійснити органи влади для впровадження проекту акта, передбачають інформування суб’єктів господарювання про вимоги регуляторного акта шляхом його оприлюднення у засобах масової інформації та розміщення на офіційному вебпорталі Верховної Ради України.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні впроваджувати або виконувати ці вимоги

Реалізація проекту акта не потребує додаткових коштів та не матиме прямого чи опосередкованого впливу на надходження та витрати державного та/або місцевого бюджетів.

Фінансування видатків, необхідних для реалізації проекту постанови буде здійснюватися в межах бюджетних призначень, передбачених для функціонування відповідних центральних органів виконавчої влади Державним бюджетом України на відповідний бюджетний період та інших не заборонених законодавством джерел фінансування.

Проведено розрахунок витрат на одного суб'єкта великого та середнього підприємництва згідно з додатком 1.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії регуляторного акта є необмеженим, оскільки акти законодавства, на виконання яких розроблено акт, мають необмежений строк дії.

Регуляторний акт набирає чинності з дня його офіційного опублікування.

Зміна строку дії проекту акта можлива у разі прийняття змін до нього, прийняття змін до нормативно-правових актів, що мають вищу юридичну силу, які стосуються цієї сфери регулювання, або визнання зазначених актів такими, що втратили чинність.

VIII. Визначення показників результативності дії регуляторного акта

Кількість суб'єктів господарювання та/або фізичних осіб, на які поширюватиметься дія акта, – дія акта поширюється на 112 надавачів послуг.

Розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта (грн.), – не прогнозується.

Розмір коштів і час, що витрачатимуться суб'єктами господарювання у зв'язку із виконанням вимог регуляторного акта.

На ознайомлення з наказом, за попередніми розрахунками, одному суб'єкту господарювання доведеться витратити:

час – приблизно 24 години робочого часу,

кошти – 66 060,00 грн в середньому на місяць на одного суб'єкта господарювання, що становить 412,88 грн за 1 год.

Для суб'єктів господарювання, які надають відповідні послуги, прямі фінансові витрати є складно прогнозованими та залежать від індивідуального рівня впровадження заходів безпеки, наявних технічних рішень і організаційних політик.

У зв'язку з цим:

для суб'єктів, які вже мають впроваджені заходи з безпеки системи, витрати на виконання вимог галузевого профілю будуть відсутні;

для суб'єктів, які впровадили такі заходи частково, можливі додаткові витрати, пов'язані з оновленням політик безпеки або технічних налаштувань, але їхній обсяг не є системним і не може бути об'єктивно оцінений без конкретних даних кожного надавача.

Рівень поінформованості суб'єктів господарювання – достатній. Після прийняття регуляторного акта він буде розміщений офіційному вебпорталі Верховної Ради України.

Показники результативності дії регуляторного акта становлять:

- кількість центральних органів виконавчої влади, що використовують хмарні послуги та/бо послуги центру обробки даних (за 1 рік 57 центральних органів виконавчої влади, що використовують хмарні послуги та/бо послуги центру обробки даних, за 5 років - 86 центральних органів виконавчої влади, що використовують хмарні послуги та/бо послуги центру обробки даних, це прогнозні дані-припущення);

- кількість звернень заінтересованих сторін щодо необхідності внесення змін до проекту акта;

- кількість скарг суб'єктів господарювання щодо реалізації акта.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Відповідно до законодавства здійснюється базове, повторне та періодичне відстеження результативності регуляторного акта у строки, встановлені статтею 10 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Базове відстеження результативності регуляторного акта буде здійснено через 6 місяців після набрання чинності цим регуляторним актом, але не більше року з дня набрання ним чинності (орієнтовно у четвертому кварталі 2026 року).

Повторне відстеження здійснюватиметься через рік після проведення заходів з базового відстеження, але не пізніше двох років з дня набрання чинності цим актом (орієнтовно у четвертому кварталі 2027 року).

Періодичне відстеження результативності буде здійснюватися один раз на кожні три роки, починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Метод проведення відстеження результативності – статистичний.

Вид даних, за допомогою яких здійснюватиметься відстеження результативності, – статистичні.

У разі надходження пропозицій та зауважень щодо вирішення неврегульованих або проблемних питань буде розглянуто необхідність внесення відповідних змін.

Відстеження результативності регуляторного акта буде здійснюватися Міністерством цифрової трансформації України протягом усього строку його дії.

Заступник Міністра цифрової трансформації України з питань європейської інтеграції **Олександр БОРНЯКОВ**

«___» _____ 2026 р.

Додаток 1
до Аналізу регуляторного впливу

ВИТРАТИ
на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо, гривень	-	-
2	Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів), гривень	-	-
3	Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень	-	-
4	Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо), гривень	-	-
5	Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень	-	-
6	Витрати на оборотні активи матеріали, канцелярські товари тощо), гривень	-	-
7	Витрати, пов'язані із наймом додаткового персоналу, гривень	-	-
8	Інше (уточнити), гривень. Витрати пов'язані з ознайомленням з положеннями акта. Припускаємо, що для отримання зазначеної інформації необхідно витратити 24 год. робочого часу.	9 909,12 грн.*	-
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень	9 909,12 грн.	

10	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць	112	112

11	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень	1 109 821,44 грн.	

*Вартість витрат, визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації за 1 годину, що розрахована за формулою: заробітна плата спеціаліста – 66 060,00 грн в середньому на місяць, що становить 412,88 грн за 1 год (66 060 грн/160 год). Інформація про середньомісячну заробітну плату штатних працівників за видом діяльності "Інформація та телекомунікації" взята із сайту Держстату: https://stat.gov.ua/explorer?md5=2aa704c105fb87251039dbddb9ca89ac