АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ

до проекту постанови Кабінету Міністрів України «Про затвердження Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту»

І. Визначення проблеми

Проект постанови розроблено Адміністрацією Держспецзв'язку на виконання підпункту 1.17 пункту 1 Плану організації підготовки проектів актів та виконання інших завдань, необхідних для реалізації Закону України від 27 березня 2025 р. № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» (далі – Закон № 4336-IX), доручення Кабінету Міністрів України від 08.05.2025 № 12422/1/1-25 до Закону № 4336-IX.

Згідно пунктом 4 статті 15 Закону України «Про основні засади забезпечення кібербезпеки України», Держспецзв'язку здійснює державний контроль за додержанням вимог законодавства у сфері кіберзахисту. У зв'язку зі змінами, передбаченими Законом України від 27 березня 2025 р. № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», на сьогодні спостерігається відсутність нормативно визначеної процедури державного контролю у сфері кіберзахисту, що ускладнює здійснення системного нагляду за виконанням вимог у цій сфері з боку держави, та перешкоджає ефективному реагуванню на порушення й ризики.

Наразі в Україні відсутній такий нормативно-правовий акт, який би врегульовував:

- загальні принципи державного контролю у сфері кіберзахисту, враховуючи цілі оцінювання стану кіберзахисту;
- форми контролю а також види перевірок в сфері кіберзахисту;
- підстави, процедури організації перевірки, обов'язки та права посадових осіб, що здійснюють перевірки;
- гармонізував процедури оцінювання стану кіберзахисту та звітність перед контролюючим органом;
- оформлення результатів перевірки із визначеним строком усунення виявлених порушень.

Це створює загрозу нерівномірного забезпечення рівня кіберзахисту серед органів державної влади, державних органів, органів місцевого самоврядування, підприємств, установ, організацій (крім систем та об'єктів банків) які є власниками або розпорядниками об'єктів оцінювання. Проєкт акта запроваджує

системний підхід до здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту.

Крім того, прийняття зазначеного Порядку дозволить реалізувати завдання держави щодо побудови національної системи кіберзахисту, наблизити практики контролю до стандартів Європейського Союзу, зокрема Директиви (ЄС) 2022/2555 (NIS2), та впровадити єдиний підхід до державного контролю (інспекційної діяльності) у сфері кіберзахисту.

Основні групи (підгрупи), на які впливає проблема:

Групи (підгрупи)	Так	Ні
Громадяни	-	+
Держава	+	-
Суб’єкти господарювання,	+	-
у тому числі суб’єкти малого підприємництва	-	+

Зазначена проблема не може бути розв’язана за допомогою ринкових механізмів, оскільки вона стосується безпеки державних інформаційних ресурсів.

Проблема не може бути розв’язана за допомогою чинних регуляторних актів, оскільки на сьогодні вона не урегульована жодними іншими нормативно-правовими актами.

II. Цілі державного регулювання

Основною ціллю державного регулювання є підвищення загального рівня кіберстійкості, повноти впровадження заходів кіберзахисту та захисту інформації в органах державної влади, державних органах, органах місцевого самоврядування, підприємствах, установах організаціях, які є власниками/розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури (крім систем та об’єктів банків) шляхом встановлення механізмів здійснення державного контролю у сфері кіберзахисту, що забезпечить належний рівень реалізації вимог законодавства щодо захисту інформації, у тому числі державних інформаційних ресурсів, інформації з обмеженим доступом, а також інформації, що обробляється в інформаційно-комунікаційних системах, в тому числі на об’єктах критичної

інфраструктури з урахуванням єдиного підходу до оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси, службова інформація, державна таємниця, а також функціонують об'єкти критичної інфраструктури, а також виконання норм абзацу другого пункту 29 та пункту 85 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», пункту 4 статті 15 Закону України «Про основні засади забезпечення кібербезпеки України».

Крім цього, цілями також є:

- забезпечення зворотного зв'язку між регулятором (Держспецзв'язку) та органами державної влади, державними органами, органами місцевого самоврядування, підприємствами, установами, організаціями, що є власниками або розпорядниками органах державної влади, державних органах, органах місцевого самоврядування, підприємствах, установах організаціях, які є власниками/розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури (крім систем та об'єктів банків) (далі - об'єктів оцінювання стану кіберзахисту) щодо відповідності їх систем вимогам безпеки;
- створення механізмів державного контролю в сфері кіберзахисту;
- виконання міжнародних зобов'язань України у сфері кібербезпеки відповідно до вимог Директиви (ЄС) 2022/2555 (NIS2).

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Прийняття регуляторного акта
Альтернатива 2	Залишення існуючої ситуації без змін

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Дозволить нормативно реалізувати системний підхід	Прийняття постанови не потребує додаткових

	до здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту; сформує прозорі та ефективні інструменти державного контролю у сфері кіберзахисту.	витрат з Державного бюджету України
Альтернатива 2	Немає, оскільки система державного контролю у сфері кіберзахисту не буде впроваджена, а старі нормативно-правові акти вже втратили чинність. Такий спосіб є неприйнятним. Це не забезпечить досягнення поставленої цілі регулювання та погіршить кіберстійкість і безпеку об'єктів оцінювання стану кіберзахисту	Немає

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	підвищення рівня довіри до державних цифрових сервісів; зменшення ризиків витоку персональних даних та збоїв у критичних послугах; посилення захисту прав на конфіденційність та цифрову безпеку.	Немає
Альтернатива 2	Немає	Немає

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	усі*	усі*	-	-	усі*
Питома вага групи у загальній кількості, відсотків	100%	100%	-	-	X

* У таблиці взято до уваги всі органи державної влади, державні органи, органи місцевого самоврядування, підприємства, установи організації (крім систем та об’єктів банків), які є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також щодо об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури (далі – об’єкти оцінювання), та підпадають під дію законодавства щодо проведення оцінювання стану кіберзахисту, а також враховано всіх операторів критичної інфраструктури, що на правах власності, оренди або на інших законних підставах здійснюють управління об’єктами критичної інфраструктури І категорії критичності. Водночас Закон України «Про критичну інфраструктуру», постанова Кабінету Міністрів України від 09.10.2020 № 1109 та Порядок ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього, затверджений постановою Кабінету Міністрів України від 28.04.2023 № 415, не містять вимог, відповідно до яких зазначених суб’єктів господарювання можна поділити на «великі», «середні», «малі» та «мікро». Однак, відповідно до пункту 1 частини другої статті 10 Закону України «Про критичну інфраструктуру» І категорія критичності – особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення.

У зв’язку з тим, що неможливо визначити питому вагу групи у загальній кількості суб’єктів господарювання, то питома вага обчислюється згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта, затвердженої постановою Кабінету Міністрів від 11 березня 2004 р. № 308 (далі – Методика).

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Прийняття регуляторного акта дозволить нормативно врегулювати питання щодо здійснення державного контролю в сфері кіберзахисту	Немає
Альтернатива 2	Залишення існуючої на цей момент ситуації без змін є неприйнятною, оскільки не забезпечить досягнення	Немає

	поставлених цілей регулювання	

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	-
Альтернатива 2	-

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення мети під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1	4	Максимальний бал, який доводить можливість максимального досягнення мети державного регулювання (проблема більше існувати не буде)
Альтернатива 2	1	Мінімальний бал, який доводить неможливість досягнення мети державного регулювання (проблема продовжить існувати)

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1	Прийняття регуляторного акту дозволить виконати норми 4 статті 15 Закону України «Про основні засади забезпечення кібербезпеки України», абзацу другого пункту 29 та пункту 85 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», а саме затвердити порядок здійснення державного контролю у сфері кіберзахисту, що забезпечить належний рівень реалізації вимог законодавства щодо кіберзахисту та захисту інформації, у тому числі державних інформаційних ресурсів, інформації з обмеженим доступом, а також інформації, що обробляється в інформаційно-комунікаційних системах, в тому числі на об'єктах критичної інфраструктури.	Немає	Максимальне досягнення мети державного регулювання

Альтернатива 2	Немає, оскільки проблема продовжить існувати	Немає	Неможливість досягнення мети державного регулювання

Рейтинг результативності	Аргументи щодо переваги обраної альтернативи/причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 1	Прийняття регуляторного акту є обґрунтованим та ефективним способом досягнення поставлених цілей	Зовнішніх ризиків немає
Альтернатива 2	Зазначений спосіб є неприйнятним, оскільки не відповідає поставленим цілям	Зовнішніх ризиків немає

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

Механізмом, який забезпечить розв'язання визначеної проблеми, є прийняття постанови та, як наслідок:

виконання норм 4 статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» та абзацу другого пункту 29 та пункту 85 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»;

встановлення порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту.

Для впровадження регуляторного акта необхідно вжити таких організаційних заходів, як забезпечення інформування органів державної влади, органів місцевого самоврядування, юридичних та фізичних осіб про вимоги регуляторного акта шляхом оприлюднення його на офіційному веб-сайті Держспецзв'язку та проведення Адміністрацією Держспецзв'язку інформаційно-роз'яснювальної роботи.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого

самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Реалізація регуляторного акту не потребує додаткових матеріальних, фінансових та інших ресурсів державного та місцевих бюджетів.

За результатами введення в дію запропонованого регуляторного акта не передбачається нанесення шкоди суб'єктам господарювання, тому механізм повної або часткової компенсації можливої шкоди у разі настання очікуваних наслідків дії акта не розроблявся.

М-Тест не проводився, оскільки для виконання вимог регуляторного акта у малих і мікросуб'єктів господарювання витрат не буде, окрім витрат на час, який потрібен суб'єктам господарювання на ознайомлення з вимогами нормативно-правового акта.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії регуляторного акта не обмежується у часі.

Зміна строку дії акта можлива в разі зміни законодавства, на вимогах якого базується проєкт регуляторного акта.

Регуляторний акт набирає чинності з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозовані показники результативності дії регуляторного акта:

1) частка об'єктів оцінювання стану кіберзахисту (інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси, службова інформація, державна таємниця, а також функціонують об'єкти критичної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, органи місцевого самоврядування, підприємства, установи організації (крім систем та об'єктів банків), щодо яких щорічно здійснено оцінювання поточного стану кіберзахисту задля виконання вимог державного контролю – 100% від загальної кількості об'єктів оцінювання;

2) частка суб'єктів оцінювання, які протягом року виконують зобов'язання щодо подання звітності суб'єктами контролю у встановленому форматі та строках – у % від загальної кількості або в абсолютній кількості;

3) Підвищення оцінки (виконаних та підтверджених заходів з кіберзахисту) у суб'єктів державного контролю (за результатами повторного оцінювання) – % покращення оцінки.

Розмір коштів і час, що витрачатимуться у зв'язку з виконанням вимог регуляторного акту: прийняття акту не потребує фінансових витрат.

Рівень поінформованості оцінюється як високий, оскільки суб’єкти господарювання будуть інформовані про положення регуляторного акту шляхом розміщення його на офіційному веб-сайті Держспецзв’язку з метою одержання пропозицій і зауважень.

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

Відстеження результативності цього регуляторного акту буде проводитися Адміністрацією Державної служби спеціального зв’язку та захисту інформації України за допомогою статистичного методу шляхом проведення:

базового відстеження – з дня набрання чинності регуляторним актом шляхом опрацювання пропозицій від фізичних та юридичних осіб;

повторного відстеження – через рік з дня набрання чинності;

періодичного відстеження – раз на рік, починаючи з дня виконання заходів з повторного відстеження, шляхом порівняння показників результативності з аналогічними показниками, що встановлені під час повторного відстеження.

Голова Державної служби спеціального
зв’язку та захисту інформації України Олександр ПОТІЙ

___ _____ 2025 р.

Додаток

до Аналізу регуляторного впливу

ВИТРАТИ
на одного суб’єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта за альтернативою 1

Порядковий номер	Витрати	За перший рік	За п’ять років
1	2	3	4
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	-	-
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень	-	-

10	Кількість суб’єктів господарювання середнього підприємництва, на яких буде поширено регулювання, одиниць	-	-
11	Сумарні витрати суб’єктів господарювання середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень	-	-

Розрахунок відповідних витрат на одного суб'єкта господарювання

Вид витрат	У перший рік	Періодичні (за рік)	Витрати за п'ять років
Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання / підвищення кваліфікації персоналу тощо	-	-	-

Вид витрат	Витрати на сплату податків та зборів (змінених/нововведених) (за рік)	Витрати за п'ять років
Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів)	-	-

Вид витрат	Витрати* на ведення обліку, підготовку та подання звітності (за рік)	Витрати на оплату штрафних санкцій за рік	Разом за рік	Витрати за п'ять років
Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам (витрати часу персоналу)	-	-	-	-

_____

* Вартість витрат, пов'язаних із підготовкою та поданням звітності державним органам, визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації).

Вид витрат	Витрати* на адміністрування заходів державного нагляду (контролю) (за рік)	Витрати на оплату штрафних санкцій та усунення виявлених порушень (за рік)	Разом за рік	Витрати за п'ять років
Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/приписів тощо)	-	-	-	-

_____

* Вартість витрат, пов'язаних з адмініструванням заходів державного нагляду (контролю), визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації.

Вид витрат	Витрати на проходження відповідних процедур (витрати часу, витрати на експертизи, тощо)	Витрати безпосередньо на дозволи, ліцензії, сертифікати, страхові поліси (за рік - стартовий)	Разом за рік (стартовий)	Витрати за п'ять років
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)	-	-	-	-

Вид витрат	За рік (стартовий)	Періодичні (за наступний рік)	Витрати за п'ять років
Витрати на оборотні активи (матеріали, канцелярські товари тощо)	-	-	-

Вид витрат	Витрати на оплату праці додатково найманого персоналу (за рік)	Витрати за п'ять років
Витрати, пов'язані із наймом додаткового персоналу	-	-