Аналіз регуляторного впливу
до проєкту наказу Міністерства енергетики України
«Про затвердження Вимог з кіберзахисту паливно-енергетичного сектору критичної інфраструктури»
(далі – проєкт наказу)

І. Визначення проблеми

Проєкт наказу розроблено Міністерством енергетики України з метою реалізації державної політики у сфері кібербезпеки, включаючи визначення та врегулювання обов'язкових до виконання операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури заходів з кіберзахисту власних об'єктів критичної інфраструктури та об'єктів кіберзахисту для досягнення конкретного цільового стану кібербезпеки.

Наказом Міністерства енергетики України від 15 грудня 2022 року № 417, зареєстрованим в Міністерстві юстиції України 08 лютого 2023 року за № 249/39305, затверджено Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури (далі – Вимоги). Вимоги було розроблено з урахуванням настанови для підвищення кібербезпеки критичної інфраструктури NIST Cybersecurity Framework (далі – NIST CSF) версії 1.1, виданої Національним інститутом стандартів та технології Сполучених Штатів Америки у 2018 році.

З моменту появи у 2014 році та оновлення до версії 1.1 у 2018, NIST CSF зазнав вагомих змін. У лютому 2024 року Національний інститут стандартів та технології Сполучених Штатів Америки представив нову версію стандарту NIST CSF 2.0. Фактично це перше значне оновлення за десятиліття, яким внесено суттєві доповнення та зміни.

Новий формат NIST CSF 2.0 передбачає уніфікацію функцій кібербезпеки так, щоб ними могли зручно користуватися для розвитку кібербезпеки організації різних галузей та розмірів.

Разом з тим, Законом України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» статтю 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» викладено в новій редакції. Так, комплексну систему захисту інформації (далі – КСЗІ) замінено на авторизовану систему з безпеки. Відповідно до пункту 5 Вимог, вони обов'язкові під час здійснення діяльності в тому числі з впровадження КСЗІ та на всіх етапах створення КСЗІ.

Впровадження проєкту наказу зумовлено необхідністю оновлення та актуалізації секторальних (галузевих) вимог з кіберзахисту паливно-енергетичного сектору критичної інфраструктури з урахуванням викликів у кіберпросторі, складності та багатовекторності кібератак на енергетичну галузь.

Під час визначення проблеми, яку передбачається розв'язати шляхом державного регулювання, встановлені основні групи, на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни	-	+
Держава	+	-
Суб'єкти господарювання	+	-
У тому числі суб'єкти малого підприємництва	-	+

Ця проблема не може бути вирішена за допомогою ринкових механізмів, оскільки визначення критеріїв і вимог безпеки, додержання яких обов'язкове у сфері кібербезпеки можливе лише за допомогою державного регулювання.

II. Цілі державного регулювання

1. **Підвищення рівня кібербезпеки паливно-енергетичного сектору критичної інфраструктури** шляхом запровадження єдиних обов'язкових до виконання вимог з кіберзахисту для операторів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури.
2. **Забезпечення безперервності та стабільності функціонування критичної інфраструктури** для збереження енергетичної безпеки держави та мінімізації ризиків кібербезпеки.
3. **Створення єдиної системи управління ризиками кібербезпеки** для об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури I–IV категорій критичності з урахуванням сучасних загроз та найкращих практик кіберзахисту.
4. **Запровадження стандартизованого підходу до моніторингу, реагування та відновлення** після інцидентів кібербезпеки для скорочення часу відновлення та зменшення наслідків кібератак.
5. **Підвищення компетенцій і обізнаності персоналу** операторів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури у сфері кібербезпеки, включаючи регулярне навчання та перевірку знань.
6. **Удосконалення взаємодії та обміну інформацією** між операторами критичної інфраструктури, постачальниками та державними органами для координації дій під час кіберінцидентів та кібератак.
7. **Формування єдиного підходу до планування та модернізації систем кіберзахисту** на основі аналізу поточного і цільового стану захищеності, а також пріоритизації заходів.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1. Залишення існуючої ситуації без змін.	Не актуальність механізму забезпечення кібербезпеки паливно-енергетичного сектору критичної інфраструктури призведе до збільшення ризиків порушення стабільного функціонування об'єктів критичної інфраструктури внаслідок кібератак.
Альтернатива 2. Прийняття проєкту наказу.	Прийняття проєкту наказу забезпечить досягнення вищезгаданих цілей державного регулювання повною мірою. Розроблення проєкту наказу з урахуванням положень сучасних міжнародних стандартів у сфері кібербезпеки забезпечить покращення стану кібербезпеки за допомогою визначення та врегулювання заходів кіберзахисту об'єктів

	критичної інфраструктури, протидії та пом’якшення наслідків потенційних кібератак.

2. Оцінка обраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. Залишення існуючої ситуації без змін.	Немає, оскільки чинні Вимоги не забезпечують підвищення рівня кібербезпеки паливно-енергетичного сектору критичної інфраструктури. Вимоги було розроблено з урахуванням настанови для підвищення кібербезпеки критичної інфраструктури NIST CSF версії 1.1, виданої Національним інститутом стандартів та технології Сполучених Штатів Америки у 2018 році. Вимоги не є актуальними, не відповідають наявним кіберзагрозам та не описують сучасні, дієві заходи з кіберзахисту. Альтернатива є неприйнятною, оскільки не забезпечує досягнення поставленої цілі.	Не актуальність нормативно-правової бази щодо практичної реалізації заходів кіберзахисту призводить до вразливості об’єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому стосовно впливу потенційних кібератак. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків внаслідок масштабних кібератак.
Альтернатива 2. Прийняття проєкту наказу.	Прийняття проєкту наказу, що містить сучасні вимоги з кіберзахисту забезпечить: - приведення у відповідність до вимог сучасних міжнародних стандартів у сфері кібербезпеки; - оновлення та актуалізація нормативно-правової бази для практичної реалізації заходів кіберзахисту, важливих для підвищення захищеності об’єктів критичної інфраструктури та паливно-енергетичного сектору в цілому. Це призведе до реалізації на об’єктах критичної	Додаткових витрат не потребує.

	інфраструктури ефективних заходів кіберзахисту від кібератак, підвищить безпеку об’єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому, суттєво зменшить імовірність виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.	

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. Залишення існуючої ситуації без змін.	Альтернатива є неприйнятною, оскільки чинні Вимоги не забезпечують підвищення рівня кібербезпеки паливно-енергетичного сектору критичної інфраструктури. Збереження існуючої ситуації збільшує ризик виникнення аварійних ситуацій та аварій (спричинених кібератаками) на об’єктах критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури з вкрай негативними наслідками для громадян.	Додаткових витрат не потребує.
Альтернатива 2. Прийняття проєкту наказу.	Матиме позитивний вплив на громадян. Громадяни матимуть підтвердження того, що держава розуміє необхідність захисту об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, в тому з урахуванням постійних комплексних,	Відсутні.

	багатовекторних кібератак.	

Оцінка впливу на сферу інтересів суб'єктів господарювання (операторів критичної інфраструктури) *

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання (одиниць)	63	100	-	-	163
Питома вага групи у загальній кількості, відсотків	38,6	61,4	-	-	100

* Відповідно до Переліку об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, затвердженого наказом Міністерства енергетики України від 07.09.2022 № 1-ДСК.

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Залишення існуючої ситуації без змін.	Немає, оскільки чинні Вимоги не забезпечують належного рівня кібербезпеки операторів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури та їх власних об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури. Отже, заходи кіберзахисту, що вживаються операторами критичної інфраструктури є недостатніми для ефективного реагування на сучасні кіберзагрози. Альтернатива є неприйнятною, оскільки не забезпечує досягнення поставленої цілі.	Негативний вплив на безпеку об'єктів критичної інфраструктури через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібератак. Виникнення аварійних ситуацій через кібератаки може призвести до значних матеріальних збитків. Виникнення аварій через кібератаки може призвести до забруднення навколишнього природного середовища, нанесення шкоди здоров'ю персоналу та населенню, значних витрат на ліквідацію наслідків аварії.
Альтернатива 2 Прийняття проєкту наказу.	Підвищення рівня кібербезпеки операторів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури завдяки	Потребую мінімальних необхідних витрат, пов'язаних із веденням обліку, підготовкою та поданням щорічної звітності до Міністерства енергетики

	реалізації актуальних заходів з кіберзахисту, важливих для безпеки об’єктів критичної інфраструктури. Зменшення імовірності виникнення аварійних ситуацій та аварій внаслідок кібератак. Забезпечення стабільної безпечної та економічно ефективної роботи об’єктів критичної інфраструктури.	України та витрат на оборотні активи (матеріали, канцелярські товари тощо).

Витрати на одного суб’єкта господарювання великого підприємництва і середнього підприємництва, які виникають внаслідок дії регуляторного акта (згідно з додатком 2 до Методики проведення аналізу впливу 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.	0,00	0,00
2	Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів), гривень.	0,00	0,00
3	Витрати, пов’язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень.	3000,00	5000,00
4	Витрати, пов’язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо), гривень.	0,00	0,00
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.	0,00	0,00
6	Витрати на оборотні активи (матеріали, канцелярські товари	200,00	1000,00

	тощо), гривень.		
7	Витрати, пов’язані із наймом додаткового персоналу, гривень.	0,00	0,00
8	Інше (уточнити), гривень.	0,00	0,00
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень.	3200,00	6000,00
10	Кількість суб’єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць.	163	163
11	Сумарні витрати суб’єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень.	521600,00	978000,00

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1. Залишення існуючої ситуації без змін.	Надвеликі витрати на ліквідацію наслідків аварій на об’єктах критичної інфраструктури.
Альтернатива 2. Прийняття проєкту наказу.	978000,00

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1. Залишення існуючої ситуації без змін.	1	Цілі прийняття регуляторного акта не можуть бути досягнуті (проблема продовжить існувати).
Альтернатива 2. Прийняття проєкту наказу.	4	Зазначений спосіб є найбільш доцільним та дасть змогу нормативно врегулювати питання щодо є впровадження операторами критичної інфраструктури визначених проєктом наказу заходів з кіберзахисту

		об’єктів критичної інфраструктури I–IV категорій критичності та об’єктів кіберзахисту.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1. Залишення існуючої ситуації без змін.	Немає, оскільки чинні Вимоги не забезпечують підвищення рівня кібербезпеки паливно-енергетичного сектору критичної інфраструктури. Проблема продовжить існувати.	Не актуальність нормативно-правової бази для практичної реалізації заходів з кіберзахисту призводить до вразливості об’єктів критичної інфраструктури до впливу потенційних кібератак. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків внаслідок кібератак. Негативний вплив на безпеку об’єктів критичної інфраструктури через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібератак, спрямованих на об’єкти критичної інфраструктури.	Альтернатива не забезпечує досягнення цілей регулювання. За відсутності вигод, кількість неврегульованих витрат залишається значною.
Альтернатива 2. Прийняття проєкту наказу.	Прийняття проєкту наказу, що містить сучасні вимоги до кіберзахисту об’єктів критичної інфраструктури забезпечить: - приведення у відповідність до вимог сучасних міжнародних стандартів; - оновлення	Мінімальні необхідні витрати, пов’язані із веденням обліку, підготовкою та поданням щорічної звітності до до Міністерства енергетики України та витрат на оборотні активи.	Альтернатива забезпечує досягнення цілей регулювання. За відсутності неврегульованих витрат, дозволяє досягнути максимальної кількості вигод.

	нормативно-правової бази для практичної реалізації заходів з кіберзахисту об'єктів критичної інфраструктури. Це призведе до досягнення конкретного цільового стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури, суттєво зменшить імовірність виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.		

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

Механізмами, що забезпечать розв'язання визначеної проблеми, є прийняття проєкту наказу, в якому будуть враховані сучасні міжнародні норми кібербезпеки.

Проєкт наказу затверджує Вимоги з кіберзахисту паливно-енергетичного сектору критичної інфраструктури; встановлює форму Профілю кіберзахисту для оператора критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, чотири рівні впровадження (зрілості) заходів з кіберзахисту, які оператори критичної інфраструктури забезпечують відповідно до категорій критичності об'єктів критичної інфраструктури, та шість функцій обов'язкових до виконання операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури заходів з кіберзахисту власних об'єктів критичної інфраструктури – управління, ідентифікація, забезпечення захисту, виявлення, реагування та відновлення, які діляться на категорії та підкатегорії.

Організаційні заходи, які необхідно здійснити Міністерству енергетики України для впровадження наказу «Про затвердження Вимог з кіберзахисту паливно-енергетичного сектору критичної інфраструктури»:

- направлення операторам критичної інфраструктури інформаційних листів щодо набрання чинності регуляторним актом;
- розміщення на сайті Міністерства енергетики України наказу «Про затвердження Вимог з кіберзахисту паливно-енергетичного сектору критичної інфраструктури».

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 проєкту наказу не потребуватиме додаткових бюджетних витрат і ресурсів на адміністрування регулювання органами виконавчої влади чи органами місцевого самоврядування.

Дія регуляторного акта не поширюється на суб'єктів малого та мікро підприємництва, тому розрахунок витрат на запровадження державного регулювання для суб'єктів малого підприємництва згідно з додатком 4 до Методики проведення аналізу впливу регуляторного акта (Тест малого підприємництва) не здійснювався.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Проєкт наказу набирає чинності з дня його офіційного опублікування.

Строк дії цього регуляторного акта не обмежується у часі, що надасть можливість розв'язати проблеми та досягти цілей державного регулювання.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності наказу є:

розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією наказу – не передбачається;

кількість суб'єктів господарювання, на яких поширюється дія наказу: 163 суб'єкти господарювання (оператори критичної інфраструктури), які підпадають під дію регулювання регуляторного акта;

розмір коштів і час, що витрачатимуться органами виконавчої влади, пов'язаними з виконанням вимог наказу – не змінюється (в межах робочого часу працівників та коштів, передбачених на фінансування заробітної плати для них);

рівень поінформованості суб'єктів господарювання з основних положень наказу – середній. Проєкт наказу розміщено на офіційному вебсайті Міністерства енергетики України www.mev.gov.ua, а після прийняття він буде розміщений на офіційному вебпорталі парламенту України www.zakon.rada.gov.ua;

кількість скарг/звернень громадян/суб'єктів господарювання, пов'язаних із дією наказу;

кількість погоджених документів;

кількість виявлених порушень, пов'язаних із дією наказу.

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

Базове відстеження результативності наказу буде здійснено через шість місяців після набрання чинності наказу (приблизно I квартал 2026 року) шляхом статистичного аналізу показників, але не більше року з дня набрання чинності цим актом.

Повторне відстеження буде здійснено через рік після здійснення заходів з базового відстеження, але не пізніше ніж через два роки (приблизно I квартал 2027 року), у результаті якого відбудеться порівняння показників базового та

повторного відстеження. У разі виявлення неврегульованих та проблемних питань шляхом аналізу якісних показників дії цього акта, такі питання буде врегульовано шляхом внесення відповідних змін.

Періодичне відстеження здійснюватиметься раз на три роки, починаючи з дня виконання заходів із повторного відстеження. Установлені кількісні та якісні значення показників результативності проєкту розпорядження порівнюватимуться зі значеннями аналогічних показників, що встановлені під час повторного відстеження.

Заходи з відстеження результативності дії проєкту розпорядження здійснюватиме Міністерство енергетики України.

Метод проведення відстеження результативності – статистичний. Вид даних, за допомогою яких здійснюватиметься відстеження результативності – статистичні дані.

Міністр енергетики України **Світлана ГРИНЧУК**

«___» _____ 2025 року