

Аналіз регуляторного впливу
до проекту наказу Міністерства енергетики України
«Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури»

I. Визначення проблеми

Проект наказу Міністерства енергетики України «Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури» (далі – проект наказу) розроблено з метою реалізації державної політики захисту об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – об'єкти критичної інфраструктури).

Згідно з Переліком секторів критичної інфраструктури, затвердженим постановою Кабінету Міністрів України від 09 жовтня 2020 року № 1109, Міністерство енергетики України визначено секторальним органом у сфері захисту критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури.

Одним з основних чинників, що створює небезпеку об'єктам критичної інфраструктури є кіберзагрози та кібератаки.

Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протистояння, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно об'єктів критичної інформаційної інфраструктури об'єктів критичної інфраструктури (далі – об'єкти критичної інформаційної інфраструктури).

24 лютого 2022 року Російська Федерація розпочала військову агресію проти України. У зв'язку з цим, відповідно до Указу Президента України від 24 лютого 2022 року № 64/2022 в Україні введено воєнний стан, строк дії якого продовжено.

Починаючи з лютого 2022 року постійно відбуваються масштабні цільові кібератаки на об'єкти критичної інфраструктури. Задум зловмисників передбачав виведення з ладу високовольтних електричних підстанцій, комп'ютерів користувачів, серверів, автоматизованих робочих місць, серверного обладнання, активного мережевого обладнання.

Така ситуація зумовила необхідність покращення стану кібербезпеки, підвищення захищеності інформаційних ресурсів та інформаційно-комунікаційних систем об'єктів критичної інфраструктури та паливно-енергетичного сектору в цілому, до рівня, який забезпечує функціонування єдиного секторального (галузевого) безпечного інтегрованого інформаційного та комунікаційного середовища.

Відповідно до пункту 1 частини четвертої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є міністерства та інші центральні органи виконавчої влади.

Згідно з абзацом сьомим пункту 8 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, під час функціонування організаційно-керуючої інфраструктури кіберзахисту суб'єкти забезпечення кібербезпеки організовують і

проводять огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Зважаючи на це, з урахуванням доручення Прем'єр-міністра України Дениса ШМИГАЛЯ від 27 жовтня 2021 року № 49142/1/1-21 було прийнято рішення щодо розроблення Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

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	+	-

Ця проблема не може бути вирішена за допомогою ринкових механізмів, оскільки визначення організаційних засад проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури можливе лише за допомогою державного регулювання.

II. Цілі державного регулювання

Основною ціллю проєкту наказу є отримання об'єктивної інформації щодо оцінки рівня кібербезпеки та визначення напрямів вдосконалення і розвитку системи кібербезпеки об'єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому в частині кіберзахисту.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1 Залишення існуючої ситуації без змін.	Залишення існуючої ситуації без змін. Відсутність об'єктивної інформації щодо оцінки рівня кібербезпеки об'єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому призведе до збільшення ризиків порушення стабільного функціонування об'єктів критичної інфраструктури внаслідок кібератак.
Альтернатива 2 Прийняття проєкту наказу.	Прийняття проєкту наказу. Прийняття проєкту наказу забезпечить досягнення вищезгаданих цілей державного регулювання повною мірою.

2. Оцінка обраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Залишення існуючої ситуації без змін.	Відсутні.	Відсутність нормативно-правової бази щодо визначення порядку проведення оцінювання та звітування операторів критичної

		інфраструктури, об'єктів критичної інфраструктури стосовно стану забезпечення кібербезпеки. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків внаслідок масштабних кібератак.
Альтернатива 2 Прийняття проекту наказу.	Прийняття проекту наказу забезпечить: - проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури; - складання відповідного звіту стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури. Це дозволить об'єктивно оцінити реальний стан кібербезпеки паливно-енергетичного сектору критичної інфраструктури з урахуванням реальних і потенційних загроз у кіберпросторі та визначити напрями вдосконалення і розвитку системи кібербезпеки, що своєю чергою, забезпечить можливість суттєвого зменшення імовірності виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.	Відсутні.

Оцінка впливу на громадян не проводилась, оскільки положення проекту наказу на них не поширюються.

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)	69	65	-	-	134
Питома вага групи у загальній кількості, відсотків	51,1	48,9	-	-	100

* Відповідно до Переліку об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, затвердженого наказом Міністерства енергетики України від 07 вересня 2022 року № 1-ДСК (зі змінами).

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Залишення існуючої ситуації без змін.	Відсутні.	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, заподіяння шкоди здоров'ю персоналу та населенню, значних витрат на ліквідацію наслідків аварії.
Альтернатива 2 Прийняття проєкту наказу.	Покращення стану кібербезпеки завдяки реалізації рекомендацій з удосконалення кібербезпеки, у тому числі щодо усунення недоліків, виявлених під час проведення огляду. Зменшення імовірності виникнення аварійних ситуацій та аварій внаслідок кібератак. Забезпечення стабільно безпечної та економічно ефективної роботи об'єктів критичної інфраструктури.	Відсутні.

Витрати на одного суб'єкта господарювання великого підприємництва і середнього підприємництва, які виникають внаслідок дії проєкту наказу (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 тощо), гривень.	200,00	1000,00
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	134	134

	підприємництва, на яких буде поширено регулювання, одиниць.		
11	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 x рядок 10), гривень.	428800,00	804000,00

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 проекту наказу.	804000,00

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 регулювання не можуть бути досягнуті (проблема продовжить існувати).
Альтернатива 2 Прийняття проекту наказу.	4	Прийняття проекту наказу забезпечить повною мірою досягнення поставлених цілей.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1 Залишення існуючої ситуації без змін.	Відсутні.	Відсутність нормативно-правової бази стосовно практичної реалізації заходів щодо проведення оцінювання та звітування операторів критичної інфраструктури, об'єктів критичної інфраструктури про стан забезпечення	Альтернатива не забезпечує досягнення цілей регулювання. За відсутності вигод, кількість нерегульованих витрат залишається значною.

		кібербезпеки, що своєю чергою, призведе до відсутності об'єктивної інформації щодо оцінки рівня кібербезпеки об'єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому і, як наслідок, до вразливості об'єктів критичної інфраструктури у кіберпросторі. 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 інформаційної інфраструктури, важливих для безпеки об'єктів критичної інфраструктури.	
Альтернатива 2 Прийняття проекту наказу.	Прийняття проекту наказу забезпечить: проведення аналізу стану кіберзахисту операторів критичної інфраструктури, об'єктів критичної інфраструктури; проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної	Відсутні.	Альтернатива забезпечує досягнення цілей регулювання. За відсутності витрат, дозволяє досягнути максимальної кількості вигод.

	інфраструктури в цілому; отримання об'єктивної та повної оцінки рівня кібербезпеки об'єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому; формування пропозицій щодо вдосконалення законодавства у сфері кібербезпеки, кіберзахисту та визначення напрямів розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту; формування пропозицій щодо вдосконалення суб'єктами огляду заходів з кіберзахисту; планування заходів щодо забезпечення кіберстійкості операторів критичної інфраструктури, об'єктів критичної інфраструктури. Це призведе до визначення напрямів вдосконалення і розвитку системи кібербезпеки об'єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в		
--	---	--	--

	цілому, що 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.

Проектом наказу пропонується:

затвердити Порядок проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури;

визначити об'єкти та суб'єкти огляду;

установити, що загальне керівництво оглядом здійснює Міністерство енергетики України;

визначити критерії дослідження стану кібербезпеки;

установити, що Міністерство енергетики України, за результатами узагальнення звітів операторів критичної інфраструктури про виконання планів заходів щодо усунення недоліків, виявлених під час огляду, поточних та цільових профілів кіберзахисту, складає річний звіт стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури та не пізніше 20 грудня поточного року надсилає Адміністрації Державної служби спеціального зв'язку та захисту інформації України та Службі безпеки України.

Організаційні заходи, які необхідно здійснити Міністерству енергетики України для впровадження проєкту наказу:

направлення операторам критичної інфраструктури інформаційних листів щодо набрання чинності наказу;

розміщення на офіційному вебсайті Міністерства енергетики України www.mev.gov.ua наказу;

утворення робочої групи з питань проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури;

проведення дослідження інформаційної інфраструктури об'єктів критичної інфраструктури;

підготовка звітів за результатами проведення оглядів стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури, що надсилаються операторам критичної інфраструктури та Міністерству енергетики України;

за результатами узагальнення звітів операторів критичної інфраструктури про виконання планів заходів щодо усунення недоліків, виявлених під час огляду, поточних та цільових профілів кіберзахисту, Міністерство енергетики України складає річний звіт стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури та не пізніше 20 грудня поточного року надсилає Адміністрації

Адміністрації Державної служби спеціального зв'язку та захисту інформації України та Службі безпеки України з метою інформування щодо оцінки поточного стану кібербезпеки, реальних та потенційних кіберзагроз, пропозиції стосовно заходів забезпечення кіберстійкості паливно-енергетичного сектору критичної інфраструктури, а також удосконалення чинного законодавства України у сфері захисту інформації та кібербезпеки.

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.

М-тест не проводився оскільки малі суб'єкти господарювання не зазнають витрат на впровадження проєкту наказу.

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: 134 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 здійснюється після набрання ним чинності, але не пізніше дня, з якого починається проведення повторного відстеження результативності наказу.

Повторне відстеження результативності наказу здійснюється через 1 рік з дня набрання ним чинності.

Періодичні відстеження результативності наказу здійснюються раз на кожні три роки починаючи з дня закінчення заходів з повторного відстеження його результативності.

Міністр енергетики України

Герман ГАЛУЩЕНКО

«___» _____ 2024 року