Аналіз регуляторного впливу
до проєкту наказу Міністерства енергетики України
«Про затвердження профілів безпеки системи
для паливно-енергетичного комплексу України»
(далі – проєкт наказу)

І. Визначення проблеми

Проєкт наказу розроблено Міністерством енергетики України з метою реалізації державної політики у сфері захисту інформації та кібербезпеки, передбачає врегулювання взаємопов'язаної сукупності заходів щодо захисту інформації для інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, у яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, а також для об'єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є державні підприємства, установи та організації у паливно-енергетичному комплексі України (далі – системи), з урахуванням мінімальних вимог (базових профілів), відповідних стандартів, політик безпеки та особливостей функціонування зазначених систем.

Проєкт наказу розроблено Міністерством енергетики України відповідно до статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах», Порядку розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 року № 712, Положення про Міністерство енергетики України, затвердженого постановою Кабінету Міністрів України від 17 червня 2020 року № 507 (далі – Положення).

Відповідно до пункту 1 Положення Міністерство енергетики України є головним органом у системі центральних органів виконавчої влади, який забезпечує формування та реалізує державну політику в електроенергетичному, ядерно-промисловому, вугільно-промисловому, торфодобувному, нафтогазовому та нафтогазопереробному комплексі (далі – паливно-енергетичний комплекс).

Законом України від 27 березня 2025 року № 4336-IX «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. Комплексну систему захисту інформації замінено на авторизовану систему безпеки. Органи державної влади та інші 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.

Розроблення проєкту наказу зумовлено необхідністю адаптації заходів захисту інформаційних систем до реальних кіберзагроз, з урахуванням викликів у кіберпросторі, складності та багатовекторності кібератак на паливно-енергетичний комплекс України (далі – ПЕК України).

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, дотримання яких є обов'язковим у сфері захисту інформації та кібербезпеки, можливе лише завдяки державному регулюванню.

II. Цілі державного регулювання

1. Підвищення рівня безпеки системи шляхом запровадження галузевих заходів захисту інформації в системах.
2. Забезпечення безперервності та стабільності функціонування систем для збереження енергетичної безпеки держави та мінімізації ризиків у сфері кібербезпеки.
3. Формування єдиного стандарту безпеки систем для їх власників або розпорядників, якими є державні підприємства, установи та організації ПЕК України, з урахуванням сучасних загроз та найкращих практик захисту інформації та кібербезпеки.
4. Створення гнучкого та адаптивного підходу до захисту інформації для ПЕК України, що ґрунтується на галузевих профілях безпеки систем.

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 захисту інформації в системі ПЕК України призведе до збільшення ризиків порушення стабільного функціонування системи внаслідок кібератак.
Альтернатива 2. Прийняття проєкту наказу.	Прийняття проєкту наказу забезпечить повне досягнення вищезазначених цілей державного регулювання повною мірою. Розроблення проєкту наказу з урахуванням положень сучасних міжнародних стандартів у сфері захисту інформації та кібербезпеки сприятиме підвищенню рівня безпеки системи шляхом визначення та врегулювання відповідних заходів захисту.

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 відсутні затверджені галузеві заходи захисту інформації, тому запропонована альтернатива є	Відсутність галузевої нормативно-правової бази щодо практичної реалізації заходів захисту інформації

	неприйнятною, оскільки не забезпечує досягнення поставленої мети.	призводить до підвищеної вразливості систем ПЕК України перед потенційними кібератаками. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків внаслідок масштабних кібератак.
Альтернатива 2. Прийняття проєкту наказу.	Прийняття проєкту наказу, що містить сучасні заходи кіберзахисту,забезпечить: приведення у відповідність до вимог сучасних міжнародних стандартів у сфері захисту інформації та кібербезпеки; створення галузевої нормативно-правової бази для практичної реалізації заходів, важливих для підвищення безпеки інформаційних систем. Це сприятиме впровадженню ефективних механізмів захисту від кібератак, підвищенню рівня безпеки систем та суттєвому зменшенню ймовірності виникнення аварійних ситуацій, що можуть мати негативні наслідки для держави, населення та навколишнього природного середовища.	Додаткових витрат не потребує.

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. Залишення існуючої ситуації без змін.	Альтернатива є неприйнятною, оскільки відсутні затверджені галузеві заходи кіберзахисту. Збереження існуючої ситуації збільшує ризик виникнення аварійних ситуацій та та масштабних кібератак, що можуть мати вкрай негативні наслідки для громадян, а також для державних підприємств, установ та	Додаткових витрат не потребує.

	організацій ПЕК України, які є власниками або розпорядниками відповідних систем.	
Альтернатива 2. Прийняття проєкту наказу.	Матиме позитивний вплив на громадян, адже вони отримають підтвердження, що держава усвідомлює необхідність забезпечення безпеки систем з урахуванням постійних комплексних та багатовекторних кібератак.	Відсутні.

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)	20	38	-	-	58
Питома вага групи у загальній кількості, відсотків	34,5%	65,5%	-	-	100%

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Залишення існуючої ситуації без змін.	Немає, оскільки відсутні затверджені галузеві заходи кіберзахисту. Отже, діючі заходи є недостатніми для ефективного реагування на сучасні кіберзагрози. Альтернатива неприйнятна, адже вона не забезпечує досягнення поставленої мети.	Негативний вплив на безпеку системи проявляється у ризику виникнення аварійних ситуацій та аварій внаслідок можливих кібератак. Такі події можуть призвести до: значних матеріальних збитків; забруднення навколишнього природного середовища; шкоди здоров'ю персоналу та населення; суттєвих витрат на ліквідацію наслідків аварії.
Альтернатива 2 Прийняття проєкту наказу.	Підвищення рівня безпеки системи завдяки впровадженню актуальних заходів кіберзахисту. Зменшення ймовірності виникнення аварійних ситуацій та аварій внаслідок	Потребує мінімальних необхідних витрат на оборотні активи (матеріали, канцелярські товари тощо).

	кібератак. Забезпечення стабільної, безпечної та економічно ефективної роботи системи.	

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, затвердженої постановою Кабінету Міністрів України від 11 березня 2004 року № 308).

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 підприємництва, на яких буде поширено регулювання, одиниць.	58	58
11	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень.	185600,00	348000,00

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1. Залишення існуючої ситуації без змін.	Надмірні витрати на ліквідацію наслідків аварій, спричинених можливими кібератаками.
Альтернатива 2. Прийняття проєкту наказу.	348000,00

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 проєкту наказу не можуть бути досягнуті (проблема продовжить існувати).
Альтернатива 2. Прийняття проєкту наказу.	4	Зазначений спосіб є найбільш доцільним та дозволить нормативно врегулювати питання підвищення рівня безпеки системи шляхом запровадження галузевих заходів кіберзахисту.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1.	Немає, оскільки відсутні	Відсутність галузевої	Альтернатива не

Залишення існуючої ситуації без змін.	затверджені галузеві заходи захисту інформаційних систем, томупроблема залишатиметься невирішеною.	нормативно-правової бази щодо практичної реалізації заходів захисту інформації призводить до підвищеної вразливості систем перед потенційними кібератаками. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків та негативно впливає на безпеку систем через можливість виникнення аварійних ситуацій або аварій, спричинених кібератаками.	забезпечує досягнення цілей регулювання. Через відсутність вигод обсяг неврегульованих витрат залишається значним.
Альтернатива 2. Прийняття проєкту наказу.	Прийняття проєкту наказу, що містить сучасні заходи кіберзахисту, забезпечить: приведення у відповідність до вимог сучасних міжнародних стандартів у сфері захисту інформації та кібербезпеки; створення галузевої нормативно-правової бази для практичної реалізації заходів, важливих для підвищення безпеки інформаційних систем. Це сприятиме впровадженню ефективних механізмів захисту від кібератак, підвищенню рівня безпеки систем та суттєвому зменшенню ймовірності виникнення аварійних ситуацій, що можуть мати негативні наслідки	Мінімально необхідні витрати на оборотні активи.	Альтернатива забезпечує реалізацію цілей регулювання та, за відсутності неврегульованих витрат, дозволяє отримати максимальні вигоди.

	для держави, населення та навколишнього природного середовища.		

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

Розв'язання визначеної проблемизабезпечить прийняття проєкту наказу, що врахує сучасні міжнародні норми захисту інформації та кібербезпеки.

Проєкт наказу затверджує Галузевий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація для паливно-енергетичного комплексу України та Галузевий профіль безпеки, де обробляється службова інформація для паливно-енергетичного комплексу України.

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

направлення державним підприємствам, установам та організаціям ПЕК України, які є власниками або розпорядниками системи, інформаційних листів щодо набрання чинності проєкту наказу;

розміщення на офіційному вебсайті Міністерства енергетики України проєкту наказу .

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 проєкту наказу не поширюється на суб'єктів малого та мікро підприємництва, тому розрахунок витрат (Тест малого підприємництва) на запровадження державного регулювання для суб'єктів малого підприємництва згідно з додатком 4 до Методики проведення аналізу впливу регуляторного акта, затвердженої постановою Кабінету Міністрів України від від 11 березня 2004 року № 308, не здійснювався.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Проєкт наказу набирає чинності з дня його офіційного опублікування.

Строк дії проєкту наказу 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 проєкту наказу, – не передбачається;

кількість суб’єктів господарювання, на яких поширюється дія проєкту наказу: 58 суб’єктів господарювання ПЕК України, які підпадають під дію регулювання проєкту наказу;

розмір коштів і час, що витрачатимуться органами виконавчої влади, на виконання вимог наказу, – не змінюється (у межах робочого часу працівників та коштів, передбачених на фінансування їхньої заробітної плати);

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

кількість скарг/звернень громадян тасуб’єктів господарювання, пов’язаних із дією проєкту наказу;

кількість погоджених документів;

кількість виявлених порушень, пов’язаних із дією проєкту наказу.

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

Стосовно проєкту наказу здійснюватиметься базове, повторне та періодичне відстеження його результативності у строки, встановлені статтею 10 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності»

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

Повторне відстеження проєкту наказу буде здійснено через рік після здійснення заходів з базового відстеження, але не пізніше ніж через два роки (приблизно І 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 проєкту наказу, такі питання будуть врегульовані шляхом внесення відповідних змін.

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

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

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

Перший віце-прем’єр-міністр України –
Міністр енергетики України **Денис ШМИГАЛЬ**

«___» _____ 2026 року