МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

м. Київ

Про внесення змін до Плану діяльності Міністерства енергетики України з підготовки проектів регуляторних актів на 2024 рік

Відповідно до Закону України «Про засади державної регуляторної політики у сфері господарської діяльності»; постанови Кабінету Міністрів України від 17 червня 2020 року № 507 «Про затвердження Положення про Міністерство енергетики України»; Положення про державну реєстрацію нормативно-правових актів міністерств, інших органів виконавчої влади, затвердженого постановою Кабінету Міністрів України від 28 грудня 1992 року № 731,

НАКАЗУЮ:

1. Затвердити зміни до Плану діяльності Міністерства енергетики України з підготовки проектів регуляторних актів на 2024 рік, затвердженого наказом Міністерства енергетики України від 08 грудня 2023 року № 377 (зі змінами), що додаються.

2. Контроль за виконанням цього наказу залишаю за собою.

Міністр **Герман ГАЛУЩЕНКО**

ЗАТВЕРДЖЕНО

Наказ Міністерства енергетики України
_____ № _____

Зміни
до Плану діяльності Міністерства енергетики України
з підготовки проектів регуляторних актів на 2024 рік

Доповнити план позиціями такого змісту:

№ з/п	Назва проекту регуляторного акта	Обґрунтування необхідності прийняття регуляторного акта	Центральні органи виконавчої влади, структурні підрозділи, що розроблятимуть регуляторний акт	Термін виконання
26.	Постанова Кабінету Міністрів України «Про затвердження Технічного регламенту природного газу»	Впровадження в Україні механізмів технічного регулювання якості природного газу, що відповідатимуть європейським і міжнародним стандартам, та створять умови для усунення технічних бар'єрів у торгівлі, забезпечать можливість незалежного контролю та оцінки відповідності природного газу призначеного для споживачів	Директорат нафтогазового комплексу та розвитку ринків нафти, природного газу та нафтопродуктів	III квартал 2024 року

27.	Наказ Міністерства енергетики України «Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури»	Визначення напрямів вдосконалення і розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту з урахуванням реальних і потенційних загроз у кіберпросторі	Управління захисту критичної інфраструктури, кібербезпеки та цифрового розвитку	III квартал 2024 року

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** **_____**

Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури

Відповідно до статей 5 та 8 Закону України «Про основні засади забезпечення кібербезпеки України», пункту 8 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, з метою реалізації державної політики захисту об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури
НАКАЗУЮ:

1. Затвердити Порядок проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури, що додається.

2. Управлінню кібербезпеки та цифрового розвитку забезпечити координацію заходів щодо організації проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

3. Управлінню кібербезпеки та цифрового розвитку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

4. Цей наказ набирає чинності з дня його офіційного опублікування.

5. Контроль за виконанням цього наказу покласти на заступника Міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації АНДАРАКА Романа.

Міністр **Герман ГАЛУЩЕНКО**

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** **_____**

Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури

Відповідно до статей 5 та 8 Закону України «Про основні засади забезпечення кібербезпеки України», пункту 8 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, з метою реалізації державної політики захисту об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури
НАКАЗУЮ:

1. Затвердити Порядок проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури, що додається.

2. Управлінню кібербезпеки та цифрового розвитку забезпечити координацію заходів щодо організації проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

3. Управлінню кібербезпеки та цифрового розвитку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

4. Цей наказ набирає чинності з дня його офіційного опублікування.

5. Контроль за виконанням цього наказу покласти на заступника Міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації АНДАРАКА Романа.

Міністр **Герман ГАЛУЩЕНКО**

Міністерство енергетики України

Міністерство енергетики України

Повідомлення про оприлюднення проєкту наказу Міністерства енергетики України «Про затвердження Порядку огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури»

**Повідомлення про оприлюднення
проєкту наказу Міністерства енергетики України
«Про затвердження Порядку огляду стану кібербезпеки
паливно-енергетичного сектору критичної інфраструктури»**

Проєкт акта розроблений Міністерством енергетики України з метою реалізації державної політики захисту об’єктів критичної інфраструктури паливно-енергетичного сектора критичної інфраструктури, включаючи 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.

Зауваження та пропозиції слід надсилати на адреси:

Міністерство енергетики України, 01601 м. Київ, вул. Хрещатик, 30;

e-mail: volodymyr.otroda@mev.gov.ua

Державна регуляторна служба України, 01011 м. Київ, вул. Арсенальна, 9/11;

e-mail: inform@dkrp.gov.ua

Проєкт регуляторного акта та аналіз регуляторного впливу оприлюднені шляхом розміщення на офіційному веб-сайті Міненерго в мережі інтернет https://www.mev.gov.ua/.

Зауваження та пропозиції від фізичних та юридичних осіб, їх об’єднань приймаються протягом місяця з дати оприлюднення в письмовому або електронному вигляді.

Документи:
1. Проєкт наказу;
2. Порядок;
3. Пояснювальна записка;
4. Аналіз регуляторного впливу.

Док… працьовані:
1. П… – доопрацьований;

UB
Міністерство енергетики України
№26/1.1-10.2-17632 від 19.07.2024
КЕП: Галущенко Г. В. 19.07.2024 17:36
3ED5083160DBC59B040000007CDD0600BFB5FF00
Сертифікат дійсний з 01.05.2023 17:01 до 01.05.2025 17:01

Проєкт наказу	126.5 КБ
Порядок	2.17 МБ
Пояснювальна записка	140.99 КБ
Аналіз регуляторного впливу	214 КБ
Проєкт наказу - доопрацьований;	133.81 КБ
Аналіз регуляторного впливу - доопрацьований;	282.67 КБ

Дата публікації 18 березня 2024, 16:19

Категорія Повідомлення про оприлюднення

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
_____2024 року № _____

Порядок
проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури

1. Цей Порядок визначає організаційні засади проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

2. У цьому Порядку терміни вживаються у таких значеннях:

огляд – спільне з операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – оператор критичної інфраструктури) дослідження інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, систем електронних комунікацій, систем управління технологічними процесами (далі – системи), об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – об'єкт критичної інфраструктури) шляхом проведення інтерв'ю, дослідження та аналізу документації, принципів роботи, впроваджених засобів та заходів з кіберзахисту;

оцінювання стану кібербезпеки – процес вивчення результатів застосування заходів з кіберзахисту систем, об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури (далі – заходи з кіберзахисту) для визначення стану захищеності об'єктів огляду та ефективності вжитих заходів.

Інші терміни вживаються у значеннях, наведених у Законах України «Про критичну інфраструктуру», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», постанові Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373, Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (далі – Загальні вимоги до кіберзахисту), Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, затвердженому постановою Кабінету Міністрів України від 11 листопада 2020 року № 1176, Положенні про організаційно-технічну

модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, Вимогах з кібербезпеки паливно-енергетичного сектору критичної інфраструктури, затверджених наказом Міністерства енергетики України від 15 грудня 2022 року № 417, зареєстрованого в Міністерстві юстиції України 08 лютого 2023 року за № 249/39305 (далі – Вимоги з кібербезпеки).

3. Об'єктами огляду є системи, об'єкти критичної інформаційної інфраструктури, державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури.

Суб'єктами огляду є підрозділи або посадові особи з інформаційної безпеки, кібербезпеки, кіберзахисту операторів критичної інфраструктури, об'єктів критичної інфраструктури та/або підрозділи або посадові особи операторів критичної інфраструктури, об'єктів критичної інфраструктури на які покладено завдання із забезпечення заходів з кіберзахисту.

4. Огляд проводиться з метою:

виявлення реальних і потенційних кіберзагроз для запобігання їм і їх нейтралізації;

оцінювання стану кібербезпеки операторів критичної інфраструктури та об'єктів критичної інфраструктури;

аналізу стану готовності суб'єктів огляду до ефективного та оперативного реагування на кіберзагрози, запобігання кіберінцидентам, виявлення та захисту від кібератак, ліквідації їх наслідків, відновлення сталості та надійності функціонування систем;

аналізу стану виконання Загальних вимог до кіберзахисту, Вимог з кібербезпеки, Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року № 601, та інших вимог чинного законодавства України у сфері захисту інформації та кібербезпеки.

5. За результатами огляду визначається поточний стан та напрями вдосконалення і розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту з урахуванням реальних і потенційних загроз у кіберпросторі.

6. Завданнями огляду є:

оцінювання стану кібербезпеки;

формування пропозицій щодо удосконалення чинного законодавства України у сфері захисту інформації та кібербезпеки, конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури;

визначення напрямів розвитку у сфері захисту інформації та кібербезпеки паливно-енергетичного сектору критичної інфраструктури;

формування пропозицій щодо вдосконалення суб'єктами огляду заходів з кіберзахисту;

планування заходів щодо забезпечення кіберстійкості операторів критичної інфраструктури та об'єктів критичної інфраструктури.

7. Проведення огляду ґрунтується на таких принципах:

централізоване управління процесом проведення огляду;

об'єктивність, що передбачає проведення огляду на основі вихідних даних, які відображають реальний стан справ у сфері захисту інформації та кібербезпеки;

системність здійснення заходів з проведення огляду та колегіальність під час прийняття рішень щодо його результатів.

8. Огляд проводиться на підставі результатів аналізу:

стану дотримання суб'єктами огляду вимог чинного законодавства України у сфері захисту інформації та кібербезпеки;

інформації щодо стану кібербезпеки операторів критичної інфраструктури, об'єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому;

застосування заходів з кіберзахисту;

проведених незалежних аудитів інформаційної безпеки на об'єктах критичної інфраструктури згідно з вимогами чинного законодавства України у сфері захисту інформації та кібербезпеки.

9. Загальне керівництво оглядом здійснює Міненерго.

10. Для здійснення заходів з проведення огляду Міненерго утворює та затверджує склад робочої групи з питань проведення огляду (далі – Робоча група).

До складу Робочої групи залучаються представники операторів критичної інфраструктури, Служби безпеки України, Адміністрації Держспецзв'язку.

У разі потреби до складу Робочої групи можуть залучатися представники інших органів державної влади, установ та організацій різних форм власності.

11. За рішенням Робочої групи утворюється група/підгрупа з огляду в кількості не менш як 2 осіб (далі – підгрупа з огляду) до складу якої входять представники Міненерго.

12. Керівники операторів критичної інфраструктури, об'єктів критичної інфраструктури зобов'язані сприяти роботі підгрупи з огляду шляхом надання фізичного доступу до об'єктів огляду, контрольованого доступу до відповідної інформації та систем.

13. Під час огляду досліджуються:

1) стан впровадження загальної політики інформаційної безпеки;

2) відповідність поточного профілю кіберзахисту існуючому стану кіберзахисту;

3) стан виконання плану кіберзахисту;

4) ідентифікація та автентифікація користувачів та адміністраторів;

5) реєстрація подій компонентами інформаційної інфраструктури та реагування на них;

6) стан впровадженого процесу невідкладного інформування про комп'ютерні надзвичайні події, кібератаки та потенційні кіберризики;

7) забезпечення мережевого захисту компонентів та інформаційних ресурсів;

8) забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів;

9) умови використання змінних (зовнішніх) пристроїв та носіїв інформації;

10) умови використання програмного та апаратного забезпечення;

11) умови розміщення компонентів інформаційної інфраструктури (у тому числі умови фізичного розміщення);

12) рівень обізнаності персоналу з питань попередження і реагування на кіберзагрози та кіберінциденти, відновлення після кібератак;

13) наявність кількох незалежних приєднань Ethernet/мобільний, спроможність автоматично перемикатись між каналами без втрати якості зв'язку.

14. За результатами огляду підгрупою з огляду готуються звіти, що надсилаються операторам критичної інфраструктури та Міненерго.

У звітах зазначаються:

дані про поточний стан кібербезпеки операторів критичної інфраструктури та об'єктів критичної інфраструктури;

дані про стан застосування заходів з кіберзахисту;

порушення (у разі наявності) вимог чинного законодавства України у сфері захисту інформації та кібербезпеки;

пропозиції щодо підвищення рівня кіберзахисту.

15. Від дня отримання звітів, у разі виявлення порушення вимог чинного законодавства України у сфері захисту інформації та кібербезпеки під час огляду, оператори критичної інфраструктури не пізніше 15 календарних днів надсилають до Міненерго плани заходів щодо усунення недоліків та поточні профілі кіберзахисту.

16. Оператори критичної інфраструктури не пізніше 30 календарних днів від дня отримання звітів надсилають до Міненерго звіти про виконання планів заходів щодо усунення недоліків, виявлених під час огляду, та цільові профілі кіберзахисту.

17. Міненерго, 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 щодо стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури та не пізніше 20 грудня поточного року надсилає Адміністрації Держспецзв'язку та Службі безпеки України.

У річному звіті зазначаються:

оцінка поточного стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури;

опис виявлених реальних та потенційних кіберзагроз паливно-енергетичного сектору критичної інфраструктури;

пропозиції щодо заходів забезпечення кіберстійкості паливно-енергетичного сектору критичної інфраструктури;

пропозиції щодо удосконалення чинного законодавства України у сфері захисту інформації та кібербезпеки.

Начальник Управління кібербезпеки та цифрового розвитку **Валерій СТРІГАНОВ**

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
_____2024 року № _____

Порядок
проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури

1. Цей Порядок визначає організаційні засади проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

2. У цьому Порядку терміни вживаються у таких значеннях:

огляд – спільне з операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – оператор критичної інфраструктури) дослідження інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, систем електронних комунікацій, систем управління технологічними процесами (далі – системи), об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – об'єкт критичної інфраструктури) шляхом проведення інтерв'ю, дослідження та аналізу документації, принципів роботи, впроваджених засобів та заходів з кіберзахисту;

оцінювання стану кібербезпеки – процес вивчення результатів застосування заходів з кіберзахисту систем, об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури (далі – заходи з кіберзахисту) для визначення стану захищеності об'єктів огляду та ефективності вжитих заходів.

Інші терміни вживаються у значеннях, наведених у Законах України «Про критичну інфраструктуру», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», постанові Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373, Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (далі – Загальні вимоги до кіберзахисту), Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, затвердженому постановою Кабінету Міністрів України від 11 листопада 2020 року № 1176, Положенні про організаційно-технічну

модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, Вимогах з кібербезпеки паливно-енергетичного сектору критичної інфраструктури, затверджених наказом Міністерства енергетики України від 15 грудня 2022 року № 417, зареєстрованого в Міністерстві юстиції України 08 лютого 2023 року за № 249/39305 (далі – Вимоги з кібербезпеки).

3. Об'єктами огляду є системи, об'єкти критичної інформаційної інфраструктури, державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури.

Суб'єктами огляду є підрозділи або посадові особи з інформаційної безпеки, кібербезпеки, кіберзахисту операторів критичної інфраструктури, об'єктів критичної інфраструктури та/або підрозділи або посадові особи операторів критичної інфраструктури, об'єктів критичної інфраструктури на які покладено завдання із забезпечення заходів з кіберзахисту.

4. Огляд проводиться з метою:

виявлення реальних і потенційних кіберзагроз для запобігання їм і їх нейтралізації;

оцінювання стану кібербезпеки операторів критичної інфраструктури та об'єктів критичної інфраструктури;

аналізу стану готовності суб'єктів огляду до ефективного та оперативного реагування на кіберзагрози, запобігання кіберінцидентам, виявлення та захисту від кібератак, ліквідації їх наслідків, відновлення сталості та надійності функціонування систем;

аналізу стану виконання Загальних вимог до кіберзахисту, Вимог з кібербезпеки, Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року № 601, та інших вимог чинного законодавства України у сфері захисту інформації та кібербезпеки.

5. За результатами огляду визначається поточний стан та напрями вдосконалення і розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту з урахуванням реальних і потенційних загроз у кіберпросторі.

6. Завданнями огляду є:

оцінювання стану кібербезпеки;

формування пропозицій щодо удосконалення чинного законодавства України у сфері захисту інформації та кібербезпеки, конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури;

визначення напрямів розвитку у сфері захисту інформації та кібербезпеки паливно-енергетичного сектору критичної інфраструктури;

формування пропозицій щодо вдосконалення суб'єктами огляду заходів з кіберзахисту;

планування заходів щодо забезпечення кіберстійкості операторів критичної інфраструктури та об'єктів критичної інфраструктури.

7. Проведення огляду ґрунтується на таких принципах:

централізоване управління процесом проведення огляду;

об'єктивність, що передбачає проведення огляду на основі вихідних даних, які відображають реальний стан справ у сфері захисту інформації та кібербезпеки;

системність здійснення заходів з проведення огляду та колегіальність під час прийняття рішень щодо його результатів.

8. Огляд проводиться на підставі результатів аналізу:

стану дотримання суб'єктами огляду вимог чинного законодавства України у сфері захисту інформації та кібербезпеки;

інформації щодо стану кібербезпеки операторів критичної інфраструктури, об'єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому;

застосування заходів з кіберзахисту;

проведених незалежних аудитів інформаційної безпеки на об'єктах критичної інфраструктури згідно з вимогами чинного законодавства України у сфері захисту інформації та кібербезпеки.

9. Загальне керівництво оглядом здійснює Міненерго.

10. Для здійснення заходів з проведення огляду Міненерго утворює та затверджує склад робочої групи з питань проведення огляду (далі – Робоча група).

До складу Робочої групи залучаються представники операторів критичної інфраструктури, Служби безпеки України, Адміністрації Держспецзв'язку.

У разі потреби до складу Робочої групи можуть залучатися представники інших органів державної влади, установ та організацій різних форм власності.

11. За рішенням Робочої групи утворюється група/підгрупа з огляду в кількості не менш як 2 осіб (далі – підгрупа з огляду) до складу якої входять представники Міненерго.

12. Керівники операторів критичної інфраструктури, об'єктів критичної інфраструктури зобов'язані сприяти роботі підгрупи з огляду шляхом надання фізичного доступу до об'єктів огляду, контрольованого доступу до відповідної інформації та систем.

13. Під час огляду досліджуються:

1) стан впровадження загальної політики інформаційної безпеки;

2) відповідність поточного профілю кіберзахисту існуючому стану кіберзахисту;

3) стан виконання плану кіберзахисту;

4) ідентифікація та автентифікація користувачів та адміністраторів;

5) реєстрація подій компонентами інформаційної інфраструктури та реагування на них;

6) стан впровадженого процесу невідкладного інформування про комп'ютерні надзвичайні події, кібератаки та потенційні кіберризики;

7) забезпечення мережевого захисту компонентів та інформаційних ресурсів;

8) забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів;

9) умови використання змінних (зовнішніх) пристроїв та носіїв інформації;

10) умови використання програмного та апаратного забезпечення;

11) умови розміщення компонентів інформаційної інфраструктури (у тому числі умови фізичного розміщення);

12) рівень обізнаності персоналу з питань попередження і реагування на кіберзагрози та кіберінциденти, відновлення після кібератак;

13) наявність кількох незалежних приєднань Ethernet/мобільний, спроможність автоматично перемикатись між каналами без втрати якості зв'язку.

14. За результатами огляду підгрупою з огляду готуються звіти, що надсилаються операторам критичної інфраструктури та Міненерго.

У звітах зазначаються:

дані про поточний стан кібербезпеки операторів критичної інфраструктури та об'єктів критичної інфраструктури;

дані про стан застосування заходів з кіберзахисту;

порушення (у разі наявності) вимог чинного законодавства України у сфері захисту інформації та кібербезпеки;

пропозиції щодо підвищення рівня кіберзахисту.

15. Від дня отримання звітів, у разі виявлення порушення вимог чинного законодавства України у сфері захисту інформації та кібербезпеки під час огляду, оператори критичної інфраструктури не пізніше 15 календарних днів надсилають до Міненерго плани заходів щодо усунення недоліків та поточні профілі кіберзахисту.

16. Оператори критичної інфраструктури не пізніше 30 календарних днів від дня отримання звітів надсилають до Міненерго звіти про виконання планів заходів щодо усунення недоліків, виявлених під час огляду, та цільові профілі кіберзахисту.

17. Міненерго, 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 щодо стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури та не пізніше 20 грудня поточного року надсилає Адміністрації Держспецзв'язку та Службі безпеки України.

У річному звіті зазначаються:

оцінка поточного стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури;

опис виявлених реальних та потенційних кіберзагроз паливно-енергетичного сектору критичної інфраструктури;

пропозиції щодо заходів забезпечення кіберстійкості паливно-енергетичного сектору критичної інфраструктури;

пропозиції щодо удосконалення чинного законодавства України у сфері захисту інформації та кібербезпеки.

Начальник Управління кібербезпеки та цифрового розвитку **Валерій СТРІГАНОВ**

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ
(Міненерго)
вул. Хрещатик, 30, м. Київ, 01601, тел.: (044) 531-36-93; 206-38-45
E-mail: kanc@mev.gov.ua, сайт: https://www.mev.gov.ua, ідентифікаційний код 37552996

_____ На № _____

Державна регуляторна служба України

Щодо погодження проєкту наказу

Міністерство енергетики України надсилає для погодження проєкт наказу «Про затвердження Порядку огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури» (далі – проєкт наказу).

Звертаємо увагу, що рішенням Державної регуляторної служби від 14 лютого 2023 року № 64 проєкт наказу був погоджений без зауважень. Однак, відповідно до вимог абзацу другого пункту 66 Типової інструкції з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади, затвердженої постановою Кабінету Міністрів України від 17 січня 2018 року № 55, проєкт наказу потребує повторного погодження.

На підставі вищезазначеного просимо розглянути та погодити зазначений проєкт наказу.

Додатки: 1. Проєкт наказу на 6 арк.
2. Аналіз регуляторного впливу до проєкту наказу на 11 арк.
3. Повідомлення про оприлюднення проєкту наказу на 2 арк.
4. Копія наказу від 11 березня 2024 року № 104 «Про внесення змін до Плану діяльності Міністерства енергетики України з підготовки проектів регуляторних актів на 2024 рік» на 3 арк.

Міністр **Герман ГАЛУЩЕНКО**

Володимир Отрода +380508030265

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
_____2024 року № _____

Порядок
проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури

1. Цей Порядок визначає організаційні засади проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

2. У цьому Порядку терміни вживаються у таких значеннях:

огляд – спільне з операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – оператор критичної інфраструктури) дослідження інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, систем електронних комунікацій, систем управління технологічними процесами (далі – системи), об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – об'єкт критичної інфраструктури) шляхом проведення інтерв'ю, дослідження та аналізу документації, принципів роботи, впроваджених засобів та заходів з кіберзахисту;

оцінювання стану кібербезпеки – процес вивчення результатів застосування заходів з кіберзахисту систем, об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури (далі – заходи з кіберзахисту) для визначення стану захищеності об'єктів огляду та ефективності вжитих заходів.

Інші терміни вживаються у значеннях, наведених у Законах України «Про критичну інфраструктуру», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», постанові Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373, Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (далі – Загальні вимоги до кіберзахисту), Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, затвердженому постановою Кабінету Міністрів України від 11 листопада 2020 року № 1176, Положенні про організаційно-технічну

модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, Вимогах з кібербезпеки паливно-енергетичного сектору критичної інфраструктури, затверджених наказом Міністерства енергетики України від 15 грудня 2022 року № 417, зареєстрованого в Міністерстві юстиції України 08 лютого 2023 року за № 249/39305 (далі – Вимоги з кібербезпеки).

3. Об'єктами огляду є системи, об'єкти критичної інформаційної інфраструктури, державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури.

Суб'єктами огляду є підрозділи або посадові особи з інформаційної безпеки, кібербезпеки, кіберзахисту операторів критичної інфраструктури, об'єктів критичної інфраструктури та/або підрозділи або посадові особи операторів критичної інфраструктури, об'єктів критичної інфраструктури на які покладено завдання із забезпечення заходів з кіберзахисту.

4. Огляд проводиться з метою:

виявлення реальних і потенційних кіберзагроз для запобігання їм і їх нейтралізації;

оцінювання стану кібербезпеки операторів критичної інфраструктури та об'єктів критичної інфраструктури;

аналізу стану готовності суб'єктів огляду до ефективного та оперативного реагування на кіберзагрози, запобігання кіберінцидентам, виявлення та захисту від кібератак, ліквідації їх наслідків, відновлення сталості та надійності функціонування систем;

аналізу стану виконання Загальних вимог до кіберзахисту, Вимог з кібербезпеки, Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року № 601, та інших вимог чинного законодавства України у сфері захисту інформації та кібербезпеки.

5. За результатами огляду визначається поточний стан та напрями вдосконалення і розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту з урахуванням реальних і потенційних загроз у кіберпросторі.

6. Завданнями огляду є:

оцінювання стану кібербезпеки;

формування пропозицій щодо удосконалення чинного законодавства України у сфері захисту інформації та кібербезпеки, конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури;

визначення напрямів розвитку у сфері захисту інформації та кібербезпеки паливно-енергетичного сектору критичної інфраструктури;

формування пропозицій щодо вдосконалення суб'єктами огляду заходів з кіберзахисту;

планування заходів щодо забезпечення кіберстійкості операторів критичної інфраструктури та об'єктів критичної інфраструктури.

7. Проведення огляду ґрунтується на таких принципах:

централізоване управління процесом проведення огляду;

об'єктивність, що передбачає проведення огляду на основі вихідних даних, які відображають реальний стан справ у сфері захисту інформації та кібербезпеки;

системність здійснення заходів з проведення огляду та колегіальність під час прийняття рішень щодо його результатів.

8. Огляд проводиться на підставі результатів аналізу:

стану дотримання суб'єктами огляду вимог чинного законодавства України у сфері захисту інформації та кібербезпеки;

інформації щодо стану кібербезпеки операторів критичної інфраструктури, об'єктів критичної інфраструктури та паливно-енергетичного сектору критичної інфраструктури в цілому;

застосування заходів з кіберзахисту;

проведених незалежних аудитів інформаційної безпеки на об'єктах критичної інфраструктури згідно з вимогами чинного законодавства України у сфері захисту інформації та кібербезпеки.

9. Загальне керівництво оглядом здійснює Міненерго.

10. Для здійснення заходів з проведення огляду Міненерго утворює та затверджує склад робочої групи з питань проведення огляду (далі – Робоча група).

До складу Робочої групи залучаються представники операторів критичної інфраструктури, Служби безпеки України, Адміністрації Держспецзв'язку.

У разі потреби до складу Робочої групи можуть залучатися представники інших органів державної влади, установ та організацій різних форм власності.

11. За рішенням Робочої групи утворюється група/підгрупа з огляду в кількості не менш як 2 осіб (далі – підгрупа з огляду) до складу якої входять представники Міненерго.

12. Керівники операторів критичної інфраструктури, об'єктів критичної інфраструктури зобов'язані сприяти роботі підгрупи з огляду шляхом надання фізичного доступу до об'єктів огляду, контрольованого доступу до відповідної інформації та систем.

13. Під час огляду досліджуються:

1) стан впровадження загальної політики інформаційної безпеки;

2) відповідність поточного профілю кіберзахисту існуючому стану кіберзахисту;

3) стан виконання плану кіберзахисту;

4) ідентифікація та автентифікація користувачів та адміністраторів;

5) реєстрація подій компонентами інформаційної інфраструктури та реагування на них;

6) стан впровадженого процесу невідкладного інформування про комп'ютерні надзвичайні події, кібератаки та потенційні кіберризики;

7) забезпечення мережевого захисту компонентів та інформаційних ресурсів;

8) забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів;

9) умови використання змінних (зовнішніх) пристроїв та носіїв інформації;

10) умови використання програмного та апаратного забезпечення;

11) умови розміщення компонентів інформаційної інфраструктури (у тому числі умови фізичного розміщення);

12) рівень обізнаності персоналу з питань попередження і реагування на кіберзагрози та кіберінциденти, відновлення після кібератак;

13) наявність кількох незалежних приєднань Ethernet/мобільний, спроможність автоматично перемикатись між каналами без втрати якості зв'язку.

14. За результатами огляду підгрупою з огляду готуються звіти, що надсилаються операторам критичної інфраструктури та Міненерго.

У звітах зазначаються:

дані про поточний стан кібербезпеки операторів критичної інфраструктури та об'єктів критичної інфраструктури;

дані про стан застосування заходів з кіберзахисту;

порушення (у разі наявності) вимог чинного законодавства України у сфері захисту інформації та кібербезпеки;

пропозиції щодо підвищення рівня кіберзахисту.

15. Від дня отримання звітів, у разі виявлення порушення вимог чинного законодавства України у сфері захисту інформації та кібербезпеки під час огляду, оператори критичної інфраструктури не пізніше 15 календарних днів надсилають до Міненерго плани заходів щодо усунення недоліків та поточні профілі кіберзахисту.

16. Оператори критичної інфраструктури не пізніше 30 календарних днів від дня отримання звітів надсилають до Міненерго звіти про виконання планів заходів щодо усунення недоліків, виявлених під час огляду, та цільові профілі кіберзахисту.

17. Міненерго, 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 щодо стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури та не пізніше 20 грудня поточного року надсилає Адміністрації Держспецзв'язку та Службі безпеки України.

У річному звіті зазначаються:

оцінка поточного стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури;

опис виявлених реальних та потенційних кіберзагроз паливно-енергетичного сектору критичної інфраструктури;

пропозиції щодо заходів забезпечення кіберстійкості паливно-енергетичного сектору критичної інфраструктури;

пропозиції щодо удосконалення чинного законодавства України у сфері захисту інформації та кібербезпеки.

Начальник Управління кібербезпеки та цифрового розвитку **Валерій СТРІГАНОВ**

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

І. Визначення проблеми

Проєкт наказу Міністерства енергетики України «Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури» (далі – проєкт 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 (в редакції постанови Кабінету Міністрів України від 16 січня 2024 року № 48), 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 протиборства, 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 структури 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.	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 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 проєкту наказу.	Прийняття проєкту 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 проєкту 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 х 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 проєкту 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 проєкту наказу.	4	Прийняття проєкту 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 неврегульованих 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 проєкту наказу.	Прийняття проєкту 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.

Проєктом 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

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** **_____**

Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури

Відповідно до статей 5 та 8 Закону України «Про основні засади забезпечення кібербезпеки України», пункту 8 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, з метою реалізації державної політики захисту об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури
НАКАЗУЮ:

1. Затвердити Порядок проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури, що додається.

2. Управлінню кібербезпеки та цифрового розвитку забезпечити координацію заходів щодо організації проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

3. Управлінню кібербезпеки та цифрового розвитку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

4. Цей наказ набирає чинності з дня його офіційного опублікування.

5. Контроль за виконанням цього наказу покласти на заступника Міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації АНДАРАКА Романа.

Міністр **Герман ГАЛУЩЕНКО**

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

І. Визначення проблеми

Проєкт наказу Міністерства енергетики України «Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури» (далі – проєкт 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 (в редакції постанови Кабінету Міністрів України від 16 січня 2024 року № 48), 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 протиборства, 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 структури 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.	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 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 проєкту наказу.	Прийняття проєкту 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 проєкту 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 х 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 проєкту 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 проєкту наказу.	4	Прийняття проєкту 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 неврегульованих 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 проєкту наказу.	Прийняття проєкту 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.

Проєктом 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

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

І. Визначення проблеми

Проєкт наказу Міністерства енергетики України «Про затвердження Порядку проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури» (далі – проєкт 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 (в редакції постанови Кабінету Міністрів України від 16 січня 2024 року № 48), 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 протиборства, 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.	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 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 проєкту наказу.	Прийняття проєкту 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 проєкту 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 х 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 проєкту 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 проєкту наказу.	4	Прийняття проєкту 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 неврегульованих 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 проєкту наказу.	Прийняття проєкту 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.

Проєктом 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

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ
(Міненерго)
вул. Хрещатик, 30, м. Київ, 01601, тел.: (044) 531-36-93; 206-38-45
E-mail: kanc@mev.gov.ua, сайт: https://www.mev.gov.ua, ідентифікаційний код 37552996

_____ На № _____

Державна регуляторна служба України

Щодо погодження проєкту наказу

Міністерство енергетики України надсилає для погодження проєкт наказу «Про затвердження Порядку огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури» (далі – проєкт наказу).

Звертаємо увагу, що рішенням Державної регуляторної служби від 14 лютого 2023 року № 64 проєкт наказу був погоджений без зауважень. Однак, відповідно до вимог абзацу другого пункту 66 Типової інструкції з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади, затвердженої постановою Кабінету Міністрів України від 17 січня 2018 року № 55, проєкт наказу потребує повторного погодження.

На підставі вищезазначеного просимо розглянути та погодити зазначений проєкт наказу.

Додатки: 1. Проєкт наказу на 6 арк.
2. Аналіз регуляторного впливу до проєкту наказу на 11 арк.
3. Повідомлення про оприлюднення проєкту наказу на 2 арк.
4. Копія наказу від 11 березня 2024 року № 104 «Про внесення змін до Плану діяльності Міністерства енергетики України з підготовки проектів регуляторних актів на 2024 рік» на 3 арк.

Міністр **Герман ГАЛУЩЕНКО**

Володимир Отрода +380508030265