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

1. Мета

Метою прийняття проєкту наказу є реалізація державної політики у сфері кібербезпеки, включаючи визначення та врегулювання обов'язкових до виконання операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури заходів з кіберзахисту власних об'єктів критичної інфраструктури та об'єктів кіберзахисту для досягнення конкретного цільового стану кібербезпеки.

2. Обґрунтування необхідності прийняття акта

Проєкт наказу розроблено Міністерством енергетики України відповідно до Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518.

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

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

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

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

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

3. Основні положення проєкту акта

Проєктом наказу пропонується:

затвердити Вимоги з кіберзахисту паливно-енергетичного сектору критичної інфраструктури;

встановити шість функцій обов'язкових до виконання операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури заходів з кіберзахисту власних об'єктів критичної інфраструктури – управління, ідентифікація, забезпечення захисту, виявлення, реагування та відновлення, які діляться на категорії та підкатегорії;

встановити форму Профілю кіберзахисту для оператора критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури;

встановити чотири рівні впровадження (зрілості) заходів з кіберзахисту, які оператори критичної інфраструктури забезпечують відповідно до категорій критичності об'єктів критичної інфраструктури.

4. Правові аспекти

У відповідній сфері суспільних відносин діють:

Закон України «Про основні засади забезпечення кібербезпеки в Україні»;

Закон України «Про захист інформації в інформаційно-комунікаційних системах»;

Закон України «Про критичну інфраструктуру»;

постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;

постанова Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури»;

постанова Кабінету Міністрів України від 29 грудня 2021 року № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту».

5. Фінансово-економічне обґрунтування

Реалізація проєкту наказу не потребуватиме фінансування із державного бюджету.

6. Позиція заінтересованих сторін

Проєкт наказу не потребує проведення публічних консультацій.

Проєкт наказу не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери, прав осіб з інвалідністю, функціонування і застосування української мови як державної, а також сфери наукової та науково-технічної діяльності.

7. Оцінка відповідності

Проєкт наказу не містить норм, які:

стосуються зобов'язань України у сфері європейської інтеграції;

стосуються прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод;

впливають на забезпечення рівних прав та можливостей жінок і чоловіків;

містять ризики вчинення корупційних правопорушень та правопорушень, пов'язаних з корупцією;

створюють підстави для дискримінації.

8. Прогноз результатів

Реалізація проєкту наказу не матиме негативного впливу на ринкове середовище, забезпечення захисту прав та інтересів суб'єктів господарювання, громадян і держави.

Прийняття проєкту наказу дозволить оновити та актуалізувати заходи з кіберзахисту об'єктів критичної інфраструктури для досягнення конкретного цільового стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

Міністр енергетики України **Світлана ГРИНЧУК**

«___» _____ 2025 року