МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** _____

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

Відповідно до Закону України «Про критичну інфраструктуру», Закону України «Про основні засади забезпечення кібербезпеки України», постанов Кабінету Міністрів України від 29 грудня 2021 року № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту» та від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», з урахуванням доручення Прем'єр-міністра України Дениса ШМИГАЛЯ від 27 жовтня 2021 року № 49142/1/1-21, з метою реалізації державної політики захисту об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури

НАКАЗУЮ:

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

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

3. Управлінню цифрового розвитку та кібербезпеки 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 САФАРОВА Фаріда.

Міністр **Герман ГАЛУЩЕНКО**

37552996 - Міністерство енергетики України
КЕП (Підписання): Галущенко Г. В. 26.12.2022 19:24
3ED5083160DBC59B0400 00007CDD0600E0AE7A00
Сертифікат дійсний з 29.04.2022 10:07 до 29.04.2023 10:07

37552996 - Міністерство енергетики України
КЕП (Підписання): Галущенко Г. В. 29.08.2022 16:11
3ED5083160DBC59B0400 00007CDD0600E0AE7A00
Сертифікат дійсний з 29.04.2022 10:07 до 29.04.2023 10:07

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
_____ № _____

Порядок
огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури

1. Цей Порядок визначає організаційні засади проведення огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури (далі – огляд).

2. У цьому Порядку терміни вживаються у такому значенні:

1) огляд – спільне з оператором критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – оператор критичної інфраструктури) дослідження інформаційної інфраструктури об'єкта 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;

2) оцінювання стану кібербезпеки - процес вивчення результатів застосування засобів і заходів 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», постановах Кабінету Міністрів України від 29 грудня 2021 року № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту», від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури».

3. Об'єктами огляду є оператори критичної інфраструктури, об'єкти критичної інфраструктури.

Суб'єктами огляду є команди реагування на комп'ютерні надзвичайні події (інциденти комп'ютерної безпеки), підрозділи кіберзахисту та кібербезпеки оператора критичної інфраструктури, об'єкта критичної інфраструктури.

4. Огляд проводиться з метою оцінювання стану кібербезпеки операторів критичної інфраструктури, об'єктів критичної інфраструктури та готовності суб'єктів огляду до ефективного і оперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак і кіберінцидентів, ліквідації їх наслідків, відновлення функціонування операторів критичної інфраструктури, об'єктів критичної інфраструктури, а також з метою перевірки виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів

України від 19 червня 2019 року № 518, та інших нормативно-правових актів у сферах кібербезпеки та кіберзахисту.

5. За результатами огляду визначаються 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:

проведення аналізу стану кіберзахисту операторів критичної інфраструктури, об'єктів критичної інфраструктури;

розробка конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування паливно-енергетичного сектору критичної інфраструктури;

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.

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 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 вимог законодавства у сфері кібербезпеки об'єктів огляду;

аудиту кібербезпеки операторів критичної інфраструктури, об'єктів критичної інфраструктури;

аналізу інформації щодо стану кібербезпеки об'єктів огляду, отриманої за результатами огляду;

аналізу проведених аудитів інформаційної безпеки об'єктів критичної інфраструктури.

9. Загальне керівництво оглядом здійснює Міненерго.

10. Для здійснення заходів з проведення огляду Міненерго утворює робочу групу з питань проведення огляду (далі - Робоча група).

11. Огляд проводиться групою/підгрупою з огляду з числа членів Робочої групи в кількості не менше 3 осіб.

Огляд проводиться відповідно до складеного Робочою групою та затвердженого Міненерго плану оглядів на поточний рік.

План оглядів на поточний рік в десятиденний термін з дня його затвердження доводиться до відома керівникам об'єктів огляду засобами електронного документообігу, електронного або поштового зв'язку.

Керівники об'єктів огляду зобов'язані сприяти роботі групі/підгрупі з огляду шляхом надання фізичного доступу до об'єктів огляду, контрольованого доступу до відповідної інформації та інформаційних систем.

12. Під час огляду на об'єкті досліджуються:

1) впроваджені політики інформаційної безпеки та ступінь їх виконання;

2) процес оцінки та управління ризиками;

3) управління доступом користувачів та адміністраторів;

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;

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) умов розміщення компонентів інформаційної інфраструктури (в тому числі умови фізичного розміщення);

12) рівень обізнаності персоналу з питань інформаційної безпеки;

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

13. За результатами огляду групою/підгрупою з огляду готуються відповідні звіт та рекомендації, які надаються Міненерго та суб'єкту огляду.

14. Суб'єкт огляду в десятиденний термін з дня отримання звіту та рекомендацій надає Міненерго план заходів щодо усунення недоліків, виявлених під час огляду, та в тридцятиденний термін – звіт про виконання зазначеного плану заходів щодо усунення недоліків, виявлених під час огляду.

15. Міненерго, за результатами узагальнення звітів про виконання плану заходів щодо усунення недоліків, виявлених під час огляду за рік складає відповідний звіт стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури та в десятиденний термін з дня його укладання надає Адміністрації Держспецзв'язку.

Начальник управління
цифрового розвитку та кібербезпеки **Роман КРАВІДЗ**