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», 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), постанові Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», 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 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури», 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.

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 захисту критичної інфраструктури, кібербезпеки та цифрового розвитку **Валерій СТРІГАНОВ**