ДЕРЖАВНА РЕГУЛЯТОРНА СЛУЖБА УКРАЇНИ

вул. Арсенальна, 9/11 м. Київ 01011, тел. (044) 254-56-73, факс (044) 254-43-93
E-mail: inform@dkrp.gov.ua, Web: http://www.drs.gov.ua, код ЄДРПОУ 39582357

від _____ №_____

на №_____від_____

Рішення №_____від_____2018 р.
про погодження проекту регуляторного акта

Державною регуляторною службою України відповідно до Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» розглянуто проекти постанов Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури» та «Про затвердження Порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури» (далі – проекти постанов), а також документи, що додаються до проектів постанов, подані листом Державної служби спеціального зв'язку та захисту інформації України від 16.07.2018 № 05/01-2200.

За результатами проведеного аналізу проектів постанов та відповідних аналізів регуляторного впливу на відповідність вимогам статей 4, 5, 8 і 9 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності», та керуючись частиною четвертою статті 21 цього Закону, Державною регуляторною службою України

вирішено:

погодити проекти постанов Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури» та «Про затвердження Порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури».

В.о. Голови **В.П. Загородній**

Державна регуляторна служба України
ВИХ №7740/0/20-18 від 03.08.2018

Коцовщей Олена Вологимирівна

сформувати протягом чотирьох місяців з дня набрання чинності цієї постанови секторальні (галузеві) переліки об'єктів критичної інформаційної інфраструктури, які відносяться до сфери їх управління та забезпечити їх ведення, а також забезпечити подання до Адміністрації Державної служби спеціального зв'язку та захисту інформації відомостей про об'єкти критичної інформаційної інфраструктури за встановленою формою та встановленим порядком;

організувати надання суб'єктами (операторами) критичної інформаційної інфраструктури відповідних секторів (галузей) економіки або сфер діяльності відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури згідно з Порядком внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування, затвердженим цією постановою.

4. Визнати такою, що втратила чинність, постанову Кабінету Міністрів України від 23 серпня 2016 року № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» (Офіційний вісник України, 2016, № 69 від 09.09.2016, ст.2332).

Прем'єр-міністр України **В. ГРОЙСМАН**

Л.О. Євдоченко

створення, модернізації або припинення функціонування об'єкта критичної інформаційної інфраструктури.

14. Уповноважені органи подають відомості про об'єкти критичної інформаційної інфраструктури до Адміністрації Держспецзв'язку у паперовому та електронному вигляді за формою згідно з додатком та здійснюють заходи щодо актуалізації відомостей, що містяться у Переліку, у разі:

зміни призначення об'єкта критичної інформаційної інфраструктури, виду інформації, яка обробляється ним, негативних наслідків до яких може призвести кібератака на об'єкт критичної інформаційної інфраструктури, відомостей про відповідальних осіб;

створення, модернізації або припинення функціонування об'єкта критичної інформаційної інфраструктури.

15. Кіберзахист об'єктів критичної інформаційної інфраструктури від кібератак забезпечується суб'єктами (операторами) критичної інформаційної інфраструктури відповідно до законодавства у сфері захисту інформації та кібербезпеки.

16. Керівник суб'єкта (оператора) критичної інформаційної інфраструктури або уповноважена ним особа невідкладно інформує урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузевий (відомчий) CERT) про інциденти кібербезпеки.

17. Відомості щодо кібербезпеки об'єктів критичної інформаційної інфраструктури, що містяться у Переліку та секторальних (галузевих) переліках об'єктів критичної інформаційної інфраструктури, є інформацією з обмеженим доступом. Обмін такою інформацією не повинен наносити іміджеві та фінансові збитки об'єктам критичної інфраструктури.

Л.О. Євдоченко

У разі підключення суб'єкта (оператора) критичної інформаційної інфраструктури до Національної телекомунікаційної мережі зазначені відомості можуть надаватися у вигляді електронних документів з виконанням вимог у сфері захисту інформації.

9. Відомості для внесення до Реєстру подаються суб'єктами (операторами) критичної інформаційної інфраструктури раз на рік (станом на 31 грудня року, що минув) до 1 лютого поточного року за формою, встановленою Адміністрацією Держспецзв'язку, або протягом місяця – у разі суттєвих змін відомостей про Систему, визначених у пункті 7, введення в експлуатацію нових або припинення функціонування Систем, внесених до Переліку об'єктів критичної інформаційної інфраструктури.

10. Захист інформації в Реєстрі забезпечується відповідно до законодавства у сфері захисту інформації та кібербезпеки.

11. Відомості, що містяться в інформаційному фонді Реєстру, є інформацією з обмеженим доступом.

12. Основні суб'єкти національної системи кібербезпеки забезпечуються цілодобовим безперешкодним доступом до інформаційного фонду Реєстру. Доступ до Реєстру надається каналами захищених електронних комунікацій авторизованим користувачам, які визначаються Адміністрацією Держспецзв'язку за погодженням з СБУ.

13. Інформація з Реєстру у разі потреби надається уповноваженому органу за його письмовим запитом з дотриманням вимог Законів України «Про захист персональних даних», «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», Кримінально-процесуального кодексу України та за наявності визначених законом підстав.

14. Керівник суб'єкта (оператора) критичної інфраструктури забезпечує подання відповідних відомостей для внесення до Реєстру та несе персональну відповідальність за своєчасність і достовірність наданих відомостей згідно із законодавством.

Л.О. Євдоченко

Проект

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2018 р. №

Київ

Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури

Відповідно до частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» Кабінет Міністрів України **постановляє:**

1. Затвердити такі, що додаються:

загальні вимоги з кіберзахисту об'єктів критичної інфраструктури, що додаються;

критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури.

2. Ця постанова набирає чинності з 1 січня 2019 року.

Прем'єр-міністр України **В. ГРОЙСМАН**

Л.О. Євдоченко

Рішення з обґрунтуванням щодо впровадження компенсуючих заходів або виключення окремих заходів з мінімального складу заходів із забезпечення кіберзахисту ОКІ оформлюється окремим документом за підписом власника та/або керівника ОКІ.

15. Міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування ОКІ, які відносяться до сфери їх управління. Такі вимоги з кіберзахисту погоджуються з Адміністрацією Держспецзв'язку.

Л.О. Євдоченко

обробки даних повинні бути вказані його зобов'язання щодо виконання тієї частини цих Загальних вимог, які він надає ОКІ.

Компоненти та інформація (дані) систем управління технологічними процесами ОКІ повинні бути розміщені тільки у власному центрі обробки даних.

50. З метою створення резервних копій своїх інформаційних ресурсів та їх оперативного відновлення у разі пошкодження або знищення, державні органи використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Держспецзв'язку. Порядок передачі, збереження і доступу до цих копій визначається Кабінетом Міністрів України.

51. Компоненти ОКІІ повинні знаходитись у приміщеннях, які унеможливлюють несанкціонований фізичний доступ до них сторонніх осіб.

Повинен бути забезпечений контрольований фізичний доступ до приміщень та/або комутаційних шаф, де знаходяться робочі станції, сервери, мережеві компоненти та комутаційні вузли структурованої кабельної системи ОКІІ.

52. Забороняється підключати робочі місця адміністраторів та операторів ОКІІ до інших інформаційно-телекомунікаційних систем.

53. Схеми (креслення) розміщення обладнання структурованої кабельної системи та кабельних каналів ОКІІ, схеми підключення обладнання, таблиці маркування кабелів структурованої кабельної системи та кабельних з'єднань зберігаються в актуальному стані.

Л.О. Євдоченко

створення, реконструкції, реорганізації або припинення функціонування об'єкта критичної інфраструктури;

зміни категорії об'єкта критичної інфраструктури.

15. Для визначення рівня вимог до захисту об'єктів критичної інфраструктури здійснюється категоризація об'єктів критичної інфраструктури відповідно до категорій, визначених Концепцією створення державної системи захисту критичної інфраструктури затвердженої розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р, а саме:

I категорія критичності – критично-важливі об'єкти;

II категорія критичності – життєво-важливі об'єкти;

III категорія критичності – важливі об'єкти;

IV категорія критичності – необхідні об'єкти.

16. Категоризація об'єктів критичної інфраструктури здійснюється з урахуванням:

існування викликів, ризиків і загроз, що можуть виникати щодо об'єктів критичної інфраструктури;

тяжкості можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода (здоров'ю населення; соціальній сфері; економіці; обороноздатності; іміджу країни);

масштабності негативних наслідків для держави (поширення на декілька секторів (галузей) економіки чи декілька регіонів країни);

тривалості ліквідації таких наслідків (тривалість впливу на функціонування економіки та суспільства, тривалість ліквідації наслідків та відновлення функціонування об'єкту, обсяг ресурсів необхідних для припинення негативного впливу імовірних загроз);

впливу на функціонування суміжних секторів критичної інфраструктури (ймовірність порушення функціонування інших секторів (галузей) критичної інфраструктури, виникнення каскадних ефектів).

17. Віднесення об'єктів до певної категорії критичності здійснюється уповноваженими органами.

18. Відомості про об'єкти критичної інфраструктури, які містяться у загальнодержавному і секторальних (галузевих) переліках об'єктів критичної інфраструктури, є інформацією з обмеженим доступом.

Л.О. Євдоченко