Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

25.05.2018 № 05/02-1643

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

Щодо погодження проекту
постанови КМУ

Направляємо на погодження проект постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування», розроблений Адміністрацією Державної служби спеціального зв'язку та захисту інформації України на виконання вимог частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України».

Просимо погодити зазначений проект згідно з положеннями статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Додатки: 1. Проект постанови Кабінету Міністрів України на 10 арк., тільки на адресу.
2. Пояснювальна записка до проекту постанови Кабінету Міністрів України на 4 арк., тільки на адресу.
3. Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України на 11 арк., тільки на адресу.
4. Повідомлення про оприлюднення проекту нормативно-правового акта на 1 арк., тільки на адресу.

Голова Служби Л.О. Євдоченко

Виконавець: Заверюха К.
281-93-34

0.31

Проект

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2018 р. №

Київ

Про затвердження
порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування

Відповідно до абзацу першого частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» Кабінет Міністрів України **постановляє**:

1. Затвердити такі, що додаються:

Порядок формування переліку об'єктів критичної інформаційної інфраструктури;

Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

2. Адміністрації Державної служби спеціального зв'язку та захисту інформації:

сформувати перелік об'єктів критичної інформаційної інфраструктури та забезпечити його ведення;

утворити державний реєстр об'єктів критичної інформаційної інфраструктури та забезпечити його функціонування.

3. Міністерствам та іншим центральним органам виконавчої влади:

розробити протягом трьох місяців з дня набрання чинності цієї постанови галузеві критерії значущості об'єктів критичної інформаційної інфраструктури;

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

організувати надання суб'єктами критичної інформаційної інфраструктури відповідних галузей 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

Затверджено
постановою Кабінету Міністрів України
від 2018 р. № _____

ПОРЯДОК
формування переліку об'єктів критичної інформаційної інфраструктури

1. Цей Порядок визначає механізм формування переліку об'єктів критичної інформаційної інфраструктури України (далі – Перелік), а також основні засади організації діяльності суб'єктів забезпечення кібербезпеки критичної інфраструктури при його формуванні.

2. Терміни, що вживаються у цьому Порядку, мають таке значення:

суб'єкт критичної інформаційної інфраструктури – державний орган, підприємство, установа та організація, юридична та (або) фізична особа, якому (якій) на правах власності, оренди або на інших законних підставах належать інформаційні та інформаційно-телекомунікаційні системи, системи управління технологічними процесами, що функціонують задля забезпечення функціонування об'єктів критичної інфраструктури у штатному режимі у відповідній галузі або сфері;

уповноважений орган – державний орган, орган місцевого самоврядування, орган управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронні органи, у власності чи розпорядженні якого (яких) є об'єкт критичної інфраструктури, та/або до сфери управління яких належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта.

Інші терміни вживаються у значеннях, наведених у Законах України «Про інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України».

3. До Переліку включаються об'єкти критичної інформаційної інфраструктури об'єктів критичної інфраструктури, які: провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами потенційно небезпечних технологій і виробництв.

4. Визначення необхідності включення об'єкта критичної інформаційної інфраструктури до Переліку здійснюється з урахуванням категорії:

значущості об'єкта критичної інформаційної інфраструктури для правоохоронної сфери, національної безпеки і оборони України;

економічної значущості, яка виражається оцінкою можливого нанесення втрат (збитків) суб'єкту (суб'єктам) критичної інформаційної інфраструктури, економіці та фінансовому сектору України;

соціальній значущості, яка виражається оцінкою можливого заподіяння майнової шкоди, нанесення шкоди життю і здоров'ю людей, припинення або порушення функціонування об'єктів забезпечення життєдіяльності населення і суспільства, транспортної інфраструктури, телекомунікаційних мереж, максимальному часу відсутності доступу до адміністративних послуг для їх отримувачів;

екологічної значущості, яка виражається оцінкою рівня впливу на оточуюче середовище;

політичного значущості, яка виражається оцінкою можливого нанесення втрат Україні у внутрішній і зовнішній політиці.

5. Критерієм включення об'єкта критичної інформаційної інфраструктури до Переліку є порушення сталого функціонування об'єкта критичної інформаційної інфраструктури через здійснені на них кібератаки та кіберінциденти, що може спричинити:

виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н1);

негативний вплив на стан енергетичної безпеки держави (регіону) (Н2);

негативний вплив на стан економічної безпеки держави (Н3);

негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н4);

негативний вплив на систему управління державою (Н5);

негативний вплив на суспільно-політичну ситуацію в державі (Н6);

негативний вплив на імідж держави (Н7);

порушення сталого функціонування фінансової системи держави (Н8);

порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н9);

порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав (Н10).

6. Правила категоріювання об'єктів критичної інформаційної інфраструктури, а також переліки і показники критеріїв віднесення до об'єктів критичної інформаційної інфраструктури інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, які забезпечують управлінські, технологічні, виробничі, фінансово-економічні, інші процеси в рамках виконання функцій (повноважень) або здійснення видів діяльності суб'єктів критичної інфраструктури встановлюються Кабінетом Міністрів України.

7. Включені до Переліку об'єкти критичної інформаційної інфраструктури є критичною інформаційною інфраструктурою та захищаються від кібератак у першу чергу (пріоритетно).

8. Відомості про об'єкт критичної інформаційної інфраструктури для внесення до Переліку подаються уповноваженими органами до Адміністрації Держспецзв'язку у паперовому та електронному вигляді за формою згідно з додатком.

9. Відомості про об'єкти критичної інформаційної інфраструктури вносяться до державного реєстру об'єктів критичної інформаційної інфраструктури.

10. Перелік об'єктів критичної інформаційної інфраструктури формується на базі галузевих переліків об'єктів критичної інформаційної інфраструктури.

11. Галузеві переліки об'єктів критичної інформаційної інфраструктури формуються та ведуться уповноваженим органом, який забезпечує формування і реалізацію державної політики у відповідній галузі або сфері діяльності та відповідно до законодавства у сфері захисту критичної інфраструктури визначає об'єкти критичної інфраструктури, що знаходяться у його власності чи розпорядженні.

12. Галузеві переліки об'єктів критичної інформаційної інфраструктури формуються на підставі відомостей, отриманих від суб'єктів критичної інформаційної інфраструктури відповідних галузей або сфер діяльності.

13. Пропозиції щодо внесення об'єкта критичної інформаційної інфраструктури до галузевого переліку об'єктів критичної інформаційної інфраструктури готуються суб'єктом критичної інформаційної інфраструктури.

14. Галузеві критерії віднесення об'єкта критичної інформаційної інфраструктури до галузевого переліку об'єктів критичної інформаційної інфраструктури розробляються та затверджуються уповноваженим органом з урахуванням критеріїв, викладених у пункті 5 цього Порядку.

15. Для формування галузевого переліку об'єктів критичної інформаційної інфраструктури суб'єкти критичної інформаційної інфраструктури збирають та подають до уповноваженого органу відомості:

щодо призначення і архітектури об'єкта критичної інформаційної інфраструктури, наявність доступу до телекомунікаційних мереж;

вид інформації, яка обробляється об'єктом критичної інформаційної інфраструктури, сервіси з управління, контролю або моніторингу, які здійснюються об'єктом критичної інформаційної інфраструктури;

відомості щодо взаємодії об'єкта критичної інформаційної інфраструктури з іншими об'єктами критичної інформаційної інфраструктури та (або) щодо залежності функціонування об'єкта критичної інформаційної інфраструктури від інших таких об'єктів;

загрози безпеці інформації щодо об'єкта критичної інформаційної інфраструктури, наявні відомості, у т.ч. статистичні щодо кіберінцидентів, які мали місце на об'єкті критичної інфраструктури.

16. Суб'єкти критичної інформаційної інфраструктури здійснюють заходи щодо актуалізації відомостей, що містяться у галузевих переліках об'єктів критичної інформаційної інфраструктури, у разі:

зміни відомостей, визначених у пункті 15 цього Порядку;

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

зміни категорії значущості об'єкта критичної інформаційної інфраструктури.

17. Уповноважені органи подають відомості про об'єкт критичної інформаційної інфраструктури до Адміністрації Держспецзв'язку 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;

зміни категорії значущості об'єкта критичної інформаційної інфраструктури.

18. Кіберзахист об'єктів критичної інформаційної інфраструктури від кібератак забезпечується суб'єктом критичної інформаційної інфраструктури відповідно до законодавства у сфері захисту інформації та кібербезпеки.

19. Власник та/або керівник суб'єкта критичної інформаційної інфраструктури невідкладно інформує урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузевий CERT) про інциденти кібербезпеки та організовує проведення незалежного аудиту інформаційної безпеки на таких об'єктах критичної інформаційної інфраструктури.

20. Інформація щодо кібербезпеки об'єктів критичної інформаційної інфраструктури, що містяться у Переліку, є інформацією з обмеженим доступом. Обмін такою інформацією не повинен наносити іміджеві та фінансові збитки об'єктам критичної інфраструктури.

Л.О. Євдоченко

Додаток
до Порядку формування переліку
об'єктів критичної інформаційної
інфраструктури

Відомості про об'єкт критичної інформаційної інфраструктури

_____
(найменування уповноваженого органу)

для внесення до переліку об'єктів критичної інформаційної інфраструктури

Порядковий номер	Назва (призначення) об'єкта критичної інформаційної інфраструктури, форма власності	Найменування власника (розпорядника) об'єкта критично інформаційної інфраструктури	Вид інформації, що обробляється на об'єкті крити чної інформаційної інфраструктури (відкрита, конфіденційна, службова, технологічна)	Негативні наслідки, до яких може призвести кібератака на об'єкт критичної інформаційної інфраструктури *	Дані про осіб (адміністраторів безпеки), відповідальних за функціонування об'єкта критичної інформаційної інфрастурктури (прізвище, ім'я, по батькові, номер телефону, адреса електронної пошти тощо)	Примітка

_____ _____ _____
(найменування посади керівника уповноваженого органу) (підпис) (ініціали та прізвище)

___ _____ 20__ р.

*Зазначаються умовні позначення негативних наслідків згідно з пунктом 5 Порядку формування переліку об'єктів критичної інформаційної інфраструктури.

Затверджено
постановою Кабінету Міністрів України
від 2018 р. № _____

ПОРЯДОК
внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування

1. Цей Порядок визначає механізми внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури (далі – Реєстр), його формування та забезпечення функціонування.

2. Терміни, що вживаються у цьому Порядку, мають таке значення:

Реєстр – автоматизована система накопичення, обліку, обробки і зберігання відомостей про комунікаційні, інформаційні, інформаційно-телекомунікаційні системи та системи управління технологічними процесами (далі – Системи) об'єктів критичної інфраструктури, які внесені до переліку об'єктів критичної інформаційної інфраструктури;

суб'єкт критичної інформаційної інфраструктури – державний орган, підприємство, установа та організація, юридична та (або) фізична особа, якому (якій) на правах власності, оренди або на інших законних підставах належать інформаційні та інформаційно-телекомунікаційні системи, системи управління технологічними процесами, що функціонують задля забезпечення функціонування об'єктів критичної інфраструктури у штатному режимі у відповідній галузі або сфері.

Інші терміни вживаються у значеннях, наведених у Законах України «Про інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України».

3. Розпорядником Реєстру є Адміністрація Держспецзв'язку, яка:

здійснює заходи з адміністрування Реєстру;

встановлює організаційні та методичні засади функціонування Реєстру, а також забезпечує його функціонування;

встановлює форми подання відомостей до Реєстру, а також визначає порядок доступу до інформаційного фонду Реєстру;

на підставі отриманих відомостей забезпечує формування та оновлення інформаційного фонду Реєстру;

вживає необхідних заходів для захисту відомостей інформаційного фонду Реєстру;

виконує інші роботи, пов'язані з функціонуванням Реєстру.

4. Реєстр формується з метою:

запровадження та ведення у повному обсязі єдиної системи обліку відомостей про Системи, які внесені до переліку об'єктів критичної інформаційної інфраструктури;

проведення аналізу вразливостей (загроз) стану кіберзахисту Систем та надання методичної допомоги суб'єктам, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, а також кіберзахисту Систем.

5. До складу Реєстру входять: інформаційний фонд, комп'ютерне обладнання, електронні носії інформації, програмне забезпечення, експлуатаційна документація.

6. Інформаційний фонд Реєстру містить відомості, що надаються суб'єктами, Системи яких внесені до Переліку об'єктів критичної інформаційної інфраструктури.

7. Відомості про Систему, які подаються для формування Реєстру, містять інформацію про:

її повну та скорочену назву, або призначення;

повне найменування суб'єкта, що є власником (розпорядником) Системи;

технічне завдання на створення Системи;

режим доступу до державних електронних інформаційних ресурсів (відкрита інформація або інформація з обмеженим доступом), які обробляються або плануються для оброблення в Системі;

місцезнаходження Системи та/або її елементів (підсистем);

підключення Системи до мережі Інтернет, інших глобальних мереж передачі даних та(або) до інших Систем, які не входять до її складу;

назви та моделі комутаційного обладнання, яке використовується в Системі, його кількісні показники та країна виробника;

назви та версії операційних систем, які використовуються в Системі, кількість комп'ютерної техніки, у якій встановлені ці операційних систем;

назви та версії програмного забезпечення, яке використовується в Системі, з відображенням кількості одиниць комп'ютерної техніки, де воно встановлено, та країни виробника;

сервери, які входять до складу Системи, у разі, коли вона має фізичне з'єднання з мережею Інтернет, іншими глобальними мережами передачі даних;

відповідальну особу та/або підрозділ, відповідальні за стан захисту інформації у Системі, у тому числі про тих, на яких покладено функції служби захисту інформації;

проведення та результати державної експертизи комплексної системи захисту інформації Системи;

спроби вчинення та (або) вчинені несанкціоновані дії щодо інформаційних ресурсів у Системі.

8. Відомості для внесення до Реєстру подаються суб'єктами критичної інформаційної інфраструктури до Адміністрації Держспецзв'язку в електронному вигляді на оптичних носіях типу CD-R із супровідним листом за підписом керівника суб'єкту, Системи якого внесені до Переліку об'єктів критичної інформаційної інфраструктури.

У разі підключення суб'єкта критичної інформаційної інфраструктури до Національної телекомунікаційної мережі зазначені відомості надаються з додержанням вимог чинного законодавства в електронному вигляді, завізовані електронно-цифровим підписом керівника суб'єкта критичної інфраструктури.

9. Відомості для внесення до Реєстру подаються суб'єктами 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 зміни в Системі, введення в експлуатацію нових або припинення функціонування Систем, внесених до Переліку об'єктів критичної інформаційної інфраструктури.

10. Інформація, яка міститься в інформаційному фонді Реєстру, є державним електронним інформаційним ресурсом.

Інформація, що міститься в інформаційному фонді Реєстру, є інформацією з обмеженим доступом.

11. Власник та/або керівник суб'єкта критичної інфраструктури забезпечує подання відповідних відомостей для внесення до Реєстру та несе персональну відповідальність за достовірність наданих відомостей згідно із законодавством.

Л.О. Євдоченко

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування»

1. Обґрунтування необхідності прийняття акта

Проект постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування» (далі – проект Постанови) підготовлено Адміністрацією Державної служби спеціальної зв'язку та захисту інформації України на виконання частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України».

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії ним та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, у тому числі шляхом порушення штатних режимів роботи систем управління технологічними процесами на об'єктах критичної інфраструктури.

Аналіз кіберзагроз свідчить, що кібератаки на системи управління технологічними процесами об'єктів критичної інфраструктури держави таких галузей, як енергетика, хімічна промисловість, авіаційний та залізничний транспорт може призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави.

Розбудова цілісної системи кіберезпеки вимагає чіткого окреслення об'єкта діяльності у сфері кібербезпеки, передусім шляхом визначення переліку тих об'єктів критичної інформаційної інфраструктури, щодо яких пріоритетно мають здійснюватись заходи з кіберзахисту, а також заходи з аудиту інформаційної безпеки, інформаційного обміну про інциденти кібербезпеки.

На сьогодні перелік інформаційно-телекомунікаційних систем об'єктів критично інфраструктури держави формується відповідно до постанови Кабінету Міністрів України №563 від 23.08.2016 «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критично інфраструктури держави».

Водночас набуття чинності Законом України «Про основні засади забезпечення кібербезпеки України» вимагає включення до переліку об'єктів критичної інформаційної інфраструктури держави (далі – Перелік) систем управління технологічними процесами, що не мають виходу каналами електрозв'язку за межі контрольованої зони, але кібератака на які може призвести до негативних наслідків, зазначених у пункті 5 Порядку формування переліку об'єктів критичної інформаційної інфраструктури (далі – Порядок).

Крім того, забезпечення кіберзахисту об'єктів критичної інфраструктури в сучасних умовах інформаційних війн вимагає особливої уваги до усіх критично важливих об'єктів інфраструктури незалежно від форми власності з огляду на те значення яке вони мають для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, а погіршення їх функціонування може заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Тобто питання формування Переліку та підтримки його в актуальному стані є одним з першочергових кроків на шляху створення загальнодержавної системи захисту об'єктів критичної інфраструктури.

При цьому, забезпечення належного функціонування Переліку вимагає створення автоматизованої системи накопичення, обліку, обробки і зберігання відомостей про ті об'єкти критичної інформаційної інфраструктури, які внесені до Переліку – державного реєстру об'єктів критичної інформаційної інфраструктури (далі – Реєстр).

2. Мета і шляхи її досягнення

Метою проекту Постанови є удосконалення порядку формування Переліку та визначення механізм формування та забезпечення функціонування Реєстру.

Одним з шляхів удосконалення існуючого порядку формування Переліку є залучення до його формування не тільки суб'єктів критичної інформаційної інфраструктури будь-якої форми власності, але й уповноважених органів, які через ведення галузевих (секторальних) переліків отримують можливість координувати та контролювати заходи з кіберзахисту на об'єктах критичної інфраструктури, щодо яких вони здійснюють владні повноваження.

Крім того, Порядком встановлюється необхідність розробки галузевих критеріїв віднесення об'єкта критичної інформаційної інфраструктури до галузевого Переліку, що створить умови для чіткого окреслення секторальних об'єктів діяльності у сфері кібербезпеки, і, як наслідок – посилення кіберзахисту об'єктів критичної інфраструктури з урахуванням галузевих особливостей.

Зважаючи на важливість створення виваженого механізму формування Переліку для подальшого впровадження відповідних загрозам заходів з кіберзахисту об'єктів критичної інфраструктури з урахуванням принципів застосування Закону України «Про основні засади забезпечення кібербезпеки України», Порядком встановлюється вимога щодо розробки правил категоріювання об'єктів критичної інформаційної інфраструктури, а також показників критеріїв їх значущості. Ці правила, показники і критерії мають бути розроблені на підставах законодавства у сфері захисту об'єктів критичної інфраструктури.

Визначення механізм формування та забезпечення функціонування Реєстру дасть змогу запровадити єдину систему обліку відомостей про об'єкти

критичної інформаційної інфраструктури, які внесені до переліку об'єктів критичної інформаційної інфраструктури, а також організувати проведення аналізу вразливостей (загроз) стану їх кіберзахисту.

3. Правові аспекти

Основними нормативно-правовими актами у сфері регулювання проекту Постанови є:

Конституція України;

Закон України «Про основні засади забезпечення кібербезпеки України»;

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

Закон України «Про телекомунікації»;

Закон України «Про інформацію»;

Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96;

Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введене в дію Указом Президента України від 13 лютого 2017 року № 32;

Постанова Кабінету Міністрів України від 23 серпня 2016 року № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

4. Фінансово-економічне обґрунтування

Витрати з державного бюджету України на створення Реєстру становитимуть 500 тис. грн. Зазначена сума бюджетних коштів закладена у бюджетному запиті Держспецзв'язку на 2019 рік.

5. Позиція заінтересованих органів

Проект Постанови потребує погодження з Міністерством фінансів України, Міністерством економічного розвитку і торгівлі України, Міністерством внутрішніх справ України, Міністерством оборони України, Службою безпеки України, Державним агентством з питань електронного урядування України, Міністерством екології та природних ресурсів України, Міністерством енергетики та вугільної промисловості України, Міністерством закордонних справ України, Міністерством інфраструктури України, Міністерством регіонального розвитку, будівництва та житлово-комунального господарства України, Міністерством соціальної політики України, Міністерством юстиції України, Державною казначейською службою України, Державною міграційною службою України, Державною службою України з надзвичайних ситуацій, Державною службою фінансового моніторингу України, Державною фіскальною службою України, Адміністрацією Державної прикордонної служби України, Пенсійним фондом України та Службою зовнішньої розвідки України.

6. Регіональний аспект

Проект Постанови не стосується питання розвитку адміністративно-територіальних одиниць.

6^{-1}. Запобігання дискримінації

Проект Постанови не містить положень, які мають ознаки дискримінації. Громадська антидискримінаційна експертиза не проводилась.

7. Запобігання корупції

У проекті Постанови немає правил і процедур, що можуть містити ризики вчинення корупційних правопорушень.

8. Громадське обговорення

Проект Постанови висвітлено на офіційному веб-сайті Держспецзвязку з метою проведення громадського обговорення.

8-1. Розгляд Науковим комітетом Національної ради України з питань розвитку науки і технологій

Проект постанови не стосується сфери наукової та науково-технічної діяльності.

9. Позиція соціальних партнерів

Проект Постанови не стосується соціально-трудової сфери.

10. Оцінка регуляторного впливу

Відповідно до Закону України "Про засади державної регуляторної політики у сфері господарської діяльності" проект Постанови є регуляторним актом.

10^{-1}. Вплив реалізації акта на ринок праці

Реалізація Постанови не впливатиме на ринок праці.

11. Прогноз результатів

Прийняття проекту Постанови дозволить посилити заходи щодо кіберзахисту об'єктів критичної інфраструктури держави шляхом першочергового (пріоритетного) захисту включених до Переліку об'єктів критичної інформаційної інфраструктури від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, у тому числі й шляхом забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури як основного елемента системи обліку відомостей про такі об'єкти.

Голова Державної служби спеціального зв'язку та захисту інформації України Леонід Євдоченко

«18» 05 2018 року

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту Постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування»

І. Визначення проблеми

Проект постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування» (далі – проект Постанови) підготовлено Адміністрацією Державної служби спеціальної зв'язку та захисту інформації України на виконання вимог частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України».

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії ним та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, у тому числі шляхом порушення штатних режимів роботи систем управління технологічними процесами на об'єктах критичної інфраструктури.

Аналіз кіберзагроз свідчить, що кібератаки на комунікаційні системи та системи управління технологічними процесами об'єктів критичної інфраструктури держави таких галузей, як енергетика, хімічна промисловість та інші може призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави.

Розбудова цілісної системи кібербезпеки вимагає чіткого окреслення об'єктів кібербезпеки, передусім шляхом визначення переліку тих об'єктів критичної інформаційної інфраструктури, щодо яких пріоритетно мають здійснюватись заходи з кіберзахисту, а також заходи з аудиту інформаційної безпеки.

На сьогодні, перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави формується відповідно до постанови Кабінету Міністрів України №563 від 23.08.2016 «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

Водночас набуття чинності Законом України «Про основні засади забезпечення кібербезпеки України» вимагає включення до переліку об'єктів критичної інформаційної інфраструктури держави (далі – Перелік) систем управління технологічними процесами, що не мають виходу каналами електрозв'язку за межі контрольованої зони, але кібератака на які може призвести до негативних наслідків, зазначених у пункті 5 Порядку формування переліку об'єктів критичної інформаційної інфраструктури (далі – Порядок).

Крім того, забезпечення кіберзахисту об'єктів критичної інфраструктури в сучасних умовах інформаційних війн вимагає особливої уваги до усіх критично

важливих об'єктів інфраструктури незалежно від форми власності з огляду на те значення, яке вони мають для економіки та промисловості, суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, а погіршення їх функціонування може заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Тобто питання формування Переліку та підтримки його в актуальному стані є одним з першочергових кроків на шляху створення загальнодержавної системи захисту об'єктів критичної інфраструктури.

При цьому, забезпечення належного функціонування Переліку вимагає створення автоматизованої системи накопичення, обліку, обробки і зберігання відомостей про ті об'єкти критичної інформаційної інфраструктури, які внесені до Переліку – державного реєстру об'єктів критичної інформаційної інфраструктури (далі – Реєстр).

Основні групи (підгрупи), на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни		+
Держава	+	
Суб'єкти господарювання	+	
у тому числі суб'єкти малого підприємства		+

Проблема не може бути розв'язана за допомогою ринкових механізмів, оскільки відсутній механізм залучення до формування Переліку не тільки суб'єктів критичної інформаційної інфраструктури будь-якої форми власності, але й уповноважених органів, які через ведення галузевих (секторальних) переліків отримують можливість координувати та контролювати заходи з кіберзахисту на об'єктах критичної інфраструктури, щодо яких вони здійснюють владні повноваження.

Проблема не може бути розв'язана за допомогою діючих регуляторних актів, оскільки на сьогодні такі нормативно-правові акти відсутні.

II. Цілі державного регулювання

Основною ціллю проекту Постанови є удосконалення порядку формування Переліку та визначення механізму формування та забезпечення функціонування Реєстру.

Одним з шляхів удосконалення існуючого порядку формування Переліку є залучення до його формування не тільки суб'єктів критичної інформаційної інфраструктури будь-якої форми власності, але й уповноважених органів, які через ведення галузевих (секторальних) переліків отримують можливість координувати та контролювати заходи з кіберзахисту на об'єктах критичної інфраструктури, щодо яких вони здійснюють владні повноваження, або які належать до сфери їх управління (перебувають в управлінні).

Крім того, Порядком встановлюється необхідність розробки галузевих критеріїв віднесення об'єкта критичної інформаційної інфраструктури до

галузевого Переліку, що створить умови для чіткого окреслення об'єктів діяльності у сфері кібербезпеки відповідних галузей, і, як наслідок – посилення кіберзахисту об'єктів критичної інфраструктури з урахуванням галузевих особливостей.

Зважаючи на важливість створення ефективного механізму формування Переліку, для подальшого впровадження заходів з кіберзахисту об'єктів критичної інфраструктури, з урахуванням принципів застосування Закону України «Про основні засади забезпечення кібербезпеки України», Порядком встановлюється вимога щодо розробки правил категоріювання об'єктів критичної інформаційної інфраструктури, а також показників критеріїв їх значущості. Ці правила, показники і критерії мають бути розроблені на підставах законодавства у сфері захисту об'єктів критичної інфраструктури.

Визначення механізму формування та забезпечення функціонування Реєстру дасть змогу запровадити єдину систему обліку відомостей про об'єкти критичної інформаційної інфраструктури, які внесені до переліку об'єктів критичної інформаційної інфраструктури, а також організувати проведення аналізу вразливостей (загроз) стану їх кіберзахисту.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Збереження чинного стану законодавства з цього питання та, як наслідок, неповнота охоплення об'єктів критичної інформаційної інфраструктури у зв'язку з тим, що норми, викладенні в постанові Кабінету Міністрів України від від 23.08.2016 № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», не в повному обсязі відповідають нормам Закону України «Про основні засади забезпечення кібербезпеки України» та не дозволяють в повній мірі охопити всі об'єкти критичної інформаційної інфраструктури
Альтернатива 2	Прийняття проекту Постанови
Альтернатива 3	Внесення змін до чинного законодавства, які передбачать введення норм щодо віднесення до об'єктів критичної інформаційної інфраструктури всіх суб'єктів господарювання та, як наслідок, надмірне наповнення Переліку

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні,	Додаткових витрат

	оскільки такий підхід призведе до некоректної визначеності першочерговості (пріоритетності) об'єктів критичної інформаційної інфраструктури, які мають захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, а також створить перешкоди для створення та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури як основного елемента системи обліку відомостей про такі об'єкти, як наслідок – зашкодить проведенню аналізу загроз (вразливостей) стану кіберзахисту об'єктів критичної інформаційної інфраструктури	не потребує
Альтернатива 2	Високі, оскільки прийняття Постанови дозволить визначити об'єкти критичної інформаційної інфраструктури, які мають першочергово (пріоритетно) захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, у тому числі й шляхом забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури як основного елемента системи обліку відомостей про такі об'єкти	Витрати з державного бюджету України на створення Реєстру становитимуть 500 тис. грн. Зазначена сума бюджетних коштів закладена у бюджетному запиті Держспецзв'язку на 2019 рік.
Альтернатива 3	Відсутні оскільки такий підхід призведе до надмірної кількості об'єктів критичної інформаційної інфраструктури та не дозволить коректно визначити першочерговість (пріоритетність) об'єктів критичної інформаційної інфраструктури, які мають захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки	Додаткових витрат не потребує

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні,	Додаткових витрат

	оскільки такий підхід призведе до некоректної визначеності першочерговості (пріоритетності) об'єктів критичної інформаційної інфраструктури, які мають захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, зокрема тих, що мають вплив на здоров'я та безпеку громадян	не потребує
Альтернатива 2	Високі, оскільки прийняття проекту Постанови дозволить визначити об'єкти критичної інформаційної інфраструктури, які мають першочергово (пріоритетно) захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, зокрема тих, що мають вплив на здоров'я та безпеку громадян	Додаткових витрат не потребує
Альтернатива 3	Відсутні, оскільки такий підхід призведе до надмірної кількості об'єктів критичної інформаційної інфраструктури та не дозволить коректно визначити першочерговість (пріоритетність) об'єктів критичної інформаційної інфраструктури, які мають захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, зокрема тих, що мають вплив на здоров'я та безпеку громадян	Додаткових витрат не потребує

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	На поточний час оцінити кількість великих та середніх суб'єктів господарювання, що підпадають під дію регулювання неможливо, оскільки з прийняттям проекту Постанови буде задіяний галузевий (секторальний) підхід до віднесення об'єктів до об'єктів критичної		Дія регуляторного акта не буде розповсюджуватися на малі та мікро суб'єктів господарювання		–

	інформаційної інфраструктури		
Питома вага групи у загальній кількості, відсотків	Питома вага великих та середніх суб'єктів господарювання у загальній кількості може бути визначена тільки після віднесення об'єктів до об'єктів критичної інформаційної інфраструктури, 100	0	100 %

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні, оскільки такий підхід призведе до некоректної визначеності першочерговості (пріоритетності) об'єктів критичної інформаційної інфраструктури, які мають захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки	Додаткових витрат не потребує
Альтернатива 2	Високі, оскільки прийняття проекту Постанови дозволить визначити об'єкти критичної інформаційної інфраструктури, які мають першочергово (пріоритетно) захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки	Додаткових витрат не потребує
Альтернатива 3	Відсутні, оскільки такий підхід призведе до надмірної кількості об'єктів критичної інформаційної інфраструктури та не дозволить коректно визначити першочерговість (пріоритетність) об'єктів критичної інформаційної інфраструктури, які мають захищатися від кібератак відповідно до законодавства у сфері захисту інформації та	Додаткових витрат не потребує

	кібербезпеки	

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	Додаткових витрат не потребує
Альтернатива 2	Додаткових витрат не потребує
Альтернатива 3	Додаткових витрат не потребує

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Вибір оптимального альтернативного способу здійснюється з урахуванням системи бальної оцінки ступеня досягнення визначених цілей.

Вартість балів визначається за чотирибальною системою оцінки ступеня досягнення визначених цілей, де:

4 – цілі прийняття регуляторного акта, які можуть бути досягнуті повною мірою (проблема більше існувати не буде);

3 – цілі прийняття регуляторного акта, які можуть бути досягнуті майже повною мірою (усі важливі аспекти проблеми існувати не будуть);

2 – цілі прийняття регуляторного акта, які можуть бути досягнуті частково (проблема значно зменшиться, деякі важливі та критичні аспекти проблеми залишаться невирішеними);

1 – цілі прийняття регуляторного акта, які не можуть бути досягнуті (проблема продовжує існувати).

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1	1	Цілі прийняття регуляторного акта не можуть бути досягнуті (проблема продовжує існувати)
Альтернатива 2	4	Цілі прийняття регуляторного акта можуть бути досягнені повною мірою (проблема більше існувати не буде)
Альтернатива 3	2	Цілі прийняття регуляторного акта, які можуть бути досягнуті частково (проблема значно зменшиться, деякі важливі та критичні аспекти проблеми залишаться невирішеними)

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у

			рейтингу
Альтернатива 1	Відсутні	Додаткових витрат не потребує	Проблема продовжує існувати
Альтернатива 2	Посилення заходів щодо кіберзахисту об'єктів критичної інфраструктури шляхом першочергового (пріоритетного) захисту включених до Переліку об'єктів критичної інформаційної інфраструктури від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, у тому числі й шляхом забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури як основного елемента системи обліку відомостей про такі об'єкти	Витрати з державного бюджету України на створення Реєстру становитимуть 500 тис. грн. Зазначена сума бюджетних коштів закладена у бюджетному запиті Держспецзв'язку на 2019 рік.	Проблема більше існувати не буде
Альтернатива 3	Відсутні	Додаткових витрат не потребує	Проблема значно зменшиться, деякі важливі та критичні аспекти проблеми залишаться невирішеними

V. Механізми та заходи, які забезпечать розв'язання визначеної проблеми

Механізмом, який забезпечить розв'язання визначеної проблеми, є прийняття регуляторного акта.

Адміністрацією Держспецзв'язку підготовлено проект Постанови, яким пропонується затвердити Порядок формування переліку об'єктів критичної інформаційної інфраструктури та Порядок внесення об'єктів критичної

інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

Порядок формування переліку об'єктів критичної інформаційної інфраструктури визначає:

– механізм формування переліку об'єктів критичної інформаційної інфраструктури України;

– категорії, згідно з якими об'єктів критичної інформаційної інфраструктури включаються до Переліку;

– критерії включення об'єкта критичної інформаційної інфраструктури до Переліку;

– порядок створення та ведення галузевих переліків об'єктів критичної інформаційної інфраструктури;

– перелік відомостей, що збираються та подаються уповноваженому органу суб'єктами критичної інформаційної інфраструктури для формування галузевого переліку об'єктів критичної інформаційної інфраструктури.

Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування визначає:

– механізми внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування;

– повноваження розпорядника Реєстру;

– мету формування Реєстру та його склад;

– перелік відомостей про об'єкти критичної інформаційної інфраструктури, що подаються для формування Реєстру;

– терміни подання суб'єктами критичної інформаційної інфраструктури відомостей для внесення до Реєстру.

Для досягнення цієї цілі проектом постанови передбачається:

– затвердити Порядок формування переліку об'єктів критичної інформаційної інфраструктури;

– затвердити Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування;

– 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».

Заходи, що пропонуються для розв'язання проблеми:

– погодити проект Постанови з Міністерством фінансів України, Міністерством економічного розвитку і торгівлі України, Міністерством внутрішніх справ України, Міністерством оборони України, Службою безпеки України, Державним агентством з питань електронного урядування України, Міністерством екології та природних ресурсів України, Міністерством енергетики та вугільної промисловості України, Міністерством закордонних справ України, Міністерством інфраструктури України, Міністерством регіонального розвитку,

будівництва та житлово-комунального господарства України, Міністерством соціальної політики України, Державною казначейською службою України, Державною міграційною службою України, Державною службою України з надзвичайних ситуацій, Державною службою фінансового моніторингу України, Державною фіскальною службою України, Адміністрацією Державної прикордонної служби України, Пенсійним фондом України та Службою зовнішньої розвідки України;

– направити проект Постанови на правову експертизу до Міністерства юстиції України;

– забезпечити інформування громадськості про вимоги регуляторного акта шляхом його оприлюднення на офіційному веб-сайті Держспецзв'язку;

– забезпечити інформування суб'єктів господарювання, на сферу дії яких поширюватиметься регуляторний акт, про вимоги регуляторного акта шляхом проведення семінарів.

Реалізація положень проекту Постанови:

Дозволить визначити об'єкти критичної інформаційної інфраструктури, які мають першочергово (пріоритетно) захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, у тому числі й шляхом забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури як основного елемента системи обліку відомостей про такі об'єкти.

Дії суб'єктів господарювання – ознайомитися з регуляторним актом та дотримуватися його вимог.

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

Впровадження положень проекту Постанови дозволить посилити заходи щодо кіберзахисту об'єктів критичної інфраструктури держави шляхом першочергового (пріоритетного) захисту включених до Переліку об'єктів критичної інформаційної інфраструктури від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки, у тому числі й шляхом забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури як основного елемента системи обліку відомостей про такі об'єкти.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується.

Строк набрання чинності регуляторного акта настає з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності проекту Постанови, як регуляторного акта є:

– кількість об'єктів критичної інформаційної інфраструктури, внесених до Переліку;

– кількість об'єктів критичної інформаційної інфраструктури, включених до Реєстру;

– кількість сформованих галузевих переліків об'єктів критичної інформаційної інфраструктури;

– кількість здійснених заходів щодо актуалізації відомостей, що містяться у Переліку.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Адміністрація Держспецзв'язку буде здійснювати базове, повторне та періодичні відстеження результативності регуляторного акта у строки, встановлені статтею 10 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Проведення відстеження результативності регуляторного акта буде здійснюватися шляхом збирання статистичних даних відповідно до вищезазначених показників та аналізу звернень заінтересованих осіб щодо необхідності перегляду нормативно-правового акту з метою внесення до нього змін.

Базове відстеження результативності регуляторного акта буде здійснюватися через один рік, після набрання чинності цього регуляторного акта шляхом збирання статистичних даних, одержання пропозицій до нього, їх аналізу.

Повторне відстеження результативності регуляторного акта буде здійснюватись не пізніше двох років з дня набрання чинності цим актом, шляхом аналізу статистичних даних.

Періодичні відстеження результативності регуляторного акта будуть здійснюватись шляхом аналізу статистичних даних раз на кожні три роки починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Голова Державної служби спеціального
зв'язку та захисту інформації України Леонід Євдоченко
«18» 05 2018 року

Повідомлення про оприлюднення проекту постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування»

1. Стислий виклад змісту проекту акта

Проект постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування» підготовлено Адміністрацією Державної служби спеціальної зв'язку та захисту інформації України на виконання вимог частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України».

Документ визначає порядок формування переліку об'єктів критичної інформаційної інфраструктури та порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

2. Адреси для зауважень та пропозицій до проекту акта

Пропозиції та зауваження до проекту постанови просимо надсилати протягом місяця з дати його оприлюднення на адреси:

- Адміністрації Державної служби спеціального зв'язку та захисту інформації України:

поштова: вул. Солом'янська, 13, м. Київ, 03110; тел. (044) 281-93-05;

електронна: cyber@dsszzi.gov.ua;

- Державної регуляторної служби України:

поштова: вул. Арсенальна, 9/11, м. Київ, 01011; тел. (044) 254-56-73,

факс (044) 254-43-93;

електронна: inform@dkrp.gov.ua

3. Обраний спосіб оприлюднення проекту акта

Проект акта та аналіз його регуляторного впливу розміщено на веб-сайті Держспецзв'язку (електронна адреса: www.dsszzi.gov.ua) у підрозділі «Повідомлення про оприлюднення та проекти» розділу «Регуляторна діяльність».

4. Строк, протягом якого приймаються зауваження та пропозиції

Зауваження та пропозиції до проекту акта приймаються протягом місяця з дати його оприлюднення.

Голова Державної служби спеціального
зв'язку та захисту інформації України Леонід Євдоченко

«18» травня 2018 р.