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

26.11.19 № 05/03-1075

Державна регуляторна служба України

вул. Арсенальна, 9/11, м. Київ, 01011

Щодо погодження проєктів
постанов КМУ

Надсилаємо на повторне погодження проєкти постанов Кабінету Міністрів України «Про затвердження порядків з питань 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» та «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури» (далі – проєкти постанов), розроблені Адміністрацією Держспецзв'язку на виконання вимог частини третьої статті 4 та частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України».

Відповідно до абзацу третього пункту 2 § 40 Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 18 серпня 2007 року № 950 (далі – Регламент), проєкти постанов були повернуті на адресу Адміністрації Держспецзв'язку як головного розробника.

Проєкти постанов розроблено з урахуванням вимог законодавства ЄС, зокрема Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 06.07.2019 «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» та Директиви Ради 2008/114/ЄС від 8.12.2008 «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту», та узгоджені з текстом проєкту Закону України «Про критичну інфраструктуру та її захист».

У проєктах постанов враховано результати наукових досліджень з питань кіберзахисту критичної інфраструктури, які проводилися на замовлення Адміністрації Держспецзв'язку у 2019 році.

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

Додатки:

1. Проєкт постанови Кабінету Міністрів України «Про затвердження порядків з питань 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» на 12 арк.
2. Проєкт постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури» на 41 арк.
3. Пояснювальна записка до проєкту постанови Кабінету Міністрів України «Про затвердження порядків з питань 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» на 5 арк.
4. Пояснювальна записка до проєкту постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури» на 5 арк.
5. Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України «Про затвердження порядків з питань 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» на 13 арк.
6. Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури» на 12 арк.
7. Повідомлення про оприлюднення проектів нормативно-правових актів на 2 арк.

Голова Служби Валентин ПЕТРОВ

Вик. Дубок В.А. 281-87-44

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2019 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;

створити державний реєстр об'єктів критичної інформаційної інфраструктури та забезпечити його функціонування;

встановити форму подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури.

3. Міністерствам та іншим центральним органам виконавчої влади:

протягом шести місяців з дня визначення органів державної влади, відповідальних за сектори (підсектори) критичної інфраструктури, сформувати секторальні переліки об'єктів критичної інформаційної інфраструктури, що належать до сфери їх управління, забезпечити їх ведення та надання до

Адміністрації Державної служби спеціального зв'язку та захисту інформації відомостей про об'єкти критичної інформаційної інфраструктури у порядку та за формою, що встановлені цією постановою.

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

Прем'єр-міністр України **О. ГОНЧАРУК**

Валентин ПЕТРОВ

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2019 р. №

ПОРЯДОК
формування переліку об'єктів критичної інформаційної інфраструктури

1. Цей Порядок визначає механізм формування переліку об'єктів критичної інформаційної інфраструктури (далі – Національний перелік), а також основні завдання суб'єктів забезпечення кібербезпеки під час його формування.

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

безпека об'єкта критичної інфраструктури – стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи, а також можливість надання ним основних послуг;

власник та/або керівник об'єкта критичної інфраструктури (далі – оператор основних послуг) – державний орган, підприємство, установа, організація, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належать об'єкти критичної інфраструктури та який/яка відповідає за їх поточне функціонування;

життєво важливі послуги та функції (далі – основні послуги) – послуги та функції, які надаються органами державної влади, установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану, національної безпеки і обороноздатності;

захист об'єктів критичної інформаційної інфраструктури – організаційні, нормативно-правові, інженерно-технічні та інші заходи, спрямовані на забезпечення безпеки об'єктів критичної інформаційної інфраструктури;

ідентифікація об'єкта критичної інформаційної інфраструктури – процедура віднесення об'єкта інформаційної інфраструктури до об'єктів критичної інформаційної інфраструктури;

критична інформаційна інфраструктура — сукупність об'єктів критичної інформаційної інфраструктури;

критична інфраструктура – сукупність об'єктів критичної інфраструктури;

сектор (підсектор) критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до одного сектору (підсектору) економіки та/або мають спільну функціональну спрямованість;

уповноважений орган державної влади, відповідальний за сектор (підсектор) критичної інфраструктури (далі – уповноважений орган) – центральний орган виконавчої влади, інший державний орган, який забезпечує формування та/або реалізацію державної політики в одній чи декількох сферах.

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

3. Оператор основних послуг проводить ідентифікацію об'єктів критичної інформаційної інфраструктури, що забезпечують функціонування об'єкта критичної інфраструктури та надання ним основних послуг.

4. Ідентифікація об'єктів критичної інформаційної інфраструктури проводиться у такому порядку:

4.1. Оператор основних послуг проводить інвентаризацію всіх об'єктів інформаційної інфраструктури (інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, автоматизованих систем управління технологічними процесами тощо), що експлуатуються на об'єкті критичної інфраструктури.

4.2. Оператор основних послуг визначає, які із цих об'єктів інформаційної інфраструктури необхідні для забезпечення безперервного та стійкого функціонування об'єкта критичної інфраструктури з точки зору надання ним основних послуг, та проводить оцінку їх критичності.

5. Для оцінки критичності об'єкта інформаційної інфраструктури оператор основних послуг використовує такі три критерії:

необхідність об'єкта інформаційної інфраструктури для стійкого та безперервного функціонування об'єкта критичної інфраструктури та надання ним основних послуг;

кібератака або кіберінцидент (інцидент з інформаційної безпеки) на об'єкті інформаційної інфраструктури істотно впливає на безперервність та стійкість надання об'єктом критичної інфраструктури основних послуг;

у разі порушення безперервності та стійкості надання основних послуг об'єктом інформаційної інфраструктури немає альтернативного об'єкта (способу) для їх надання.

Об'єкти інформаційної інфраструктури, що відповідають всім трьом критеріям, визначаються оператором основних послуг як об'єкти критичної інформаційної інфраструктури. При цьому категорія критичності об'єкта

критичної інформаційної інфраструктури встановлюється за категорією критичності об'єкта критичної інфраструктури.

6. Оператор основних послуг подає відомості про об'єкти критичної інформаційної інфраструктури до уповноваженого органу, який на їх основі формує секторальний перелік об'єктів критичної інформаційної інфраструктури. Відомості подаються у паперовому та електронному вигляді за формою згідно з додатком до цього Порядку.

До секторального переліку подаються відомості про об'єкти критичної інформаційної інфраструктури тих об'єктів критичної інфраструктури, що внесені до національного переліку об'єктів критичної інфраструктури та належать до I, II, III та IV категорій критичності.

7. Оператор основних послуг вживає заходів щодо актуалізації відомостей про об'єкти критичної інформаційної інфраструктури, що містяться у секторальному переліку об'єктів критичної інформаційної інфраструктури, у разі:

суттєвої зміни відомостей, зазначених у додатку до цього Порядку;

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

8. Уповноважений орган розглядає надані відомості щодо об'єктів критичної інформаційної інфраструктури та у разі потреби надає зауваження та рекомендації стосовно коректності та/або повноти наданих відомостей, а також встановлює терміни їх перегляду операторами основних послуг.

9. Уповноважений орган на підставі відомостей про об'єкти критичної інформаційної інфраструктури, що перебувають у його власності чи розпорядженні, та відомостей, отриманих від операторів основних послуг його сектору (підсектору), формує та веде секторальний перелік об'єктів критичної інформаційної інфраструктури.

10. Уповноважений орган оновлює секторальний перелік об'єктів критичної інформаційної інфраструктури кожні два роки або у разі змін суттєвих змін, що відбулися у критичній інформаційній інфраструктурі (створення, модернізація, припинення функціонування об'єкта критичної інформаційної інфраструктури).

11. Відомості про об'єкти критичної інформаційної інфраструктури I та II категорії критичності свого сектору (підсектору) критичної інфраструктури уповноважений орган подає до Адміністрації Держспецзв'язку у паперовому та електронному вигляді за формою згідно з додатком до цього Порядку та вживає заходів щодо актуалізації відомостей про об'єкти свого сектору (підсектору), що містяться у переліку, у разі:

суттєвої зміни відомостей, зазначених у додатку до цього Порядку;

створення, модернізації або припинення функціонування об'єкта I та II категорії критичності.

12. Після внесення об'єкта критичної інформаційної інфраструктури до секторального переліку уповноважений орган повідомляє про це оператора основних послуг для проведення ним паспортизації об'єкта критичної інформаційної інфраструктури.

13. Паспорт на об'єкт критичної інформаційної інфраструктури є складовою частиною паспорта об'єкта критичної інфраструктури.

14. Національний перелік об'єктів критичної інформаційної інфраструктури формується на базі відомостей, отриманих із секторальних переліків об'єктів критичної інформаційної інфраструктури. До Національного переліку об'єктів критичної інфраструктури вносяться об'єкти критичної інформаційної інфраструктури I та II категорій критичності.

15. Адміністрація Держспецзв'язку має право запитувати в уповноваженого органу або в операторів основних послуг додаткову інформацію стосовно наданих відомостей про об'єкти інформаційної інфраструктури, що внесені до секторального переліку об'єктів критичної інформаційної інфраструктури.

16. Внесений до Національного переліку об'єкт критичної інформаційної інфраструктури захищається від кібератак першочергово (пріоритетно).

17. Відомості про об'єкти критичної інформаційної інфраструктури, включені до Національного переліку, вносяться до державного реєстру об'єктів критичної інформаційної інфраструктури.

18. Відомості щодо об'єктів критичної інформаційної інфраструктури, що містяться у Національному переліку та секторальних переліках об'єктів критичної інформаційної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства у сфері захисту інформації та державної таємниці.

Валентин ПЕТРОВ

Додаток
до Порядку формування переліку об'єктів
критичної інформаційної інфраструктури

ВІДОМОСТІ
про об'єкт критичної інформаційної інфраструктури

_____

(найменування об'єкта)

для внесення до Національного переліку об'єктів критичної інформаційної інфраструктури

Необхідні відомості	Надана інформація	Примітка
Повна назва юридичної особи, у власності (розпорядженні) якої знаходиться об'єкт критичної інформаційної інфраструктури, її юридична та фактична адреса, форма власності, П.І.Б. керівника		
Повна назва об'єкта критичної інфраструктури, до складу якого входить об'єкт критичної інформаційної інфраструктури, його призначення, сектор та підсектор, до якого він входить, перелік основних послуг, які він надає, категорія критичності		
Повна назва об'єкта критичної інформаційної інфраструктури, його призначення, перелік основних послуг, надання яких він забезпечує, категорія критичності		
Вид інформації за порядком доступу, яка обробляється або планується для оброблення на об'єкті критичної інформаційної інфраструктури		
Адреса місця фізичного розташування об'єкта критичної інформаційної інфраструктури		
Наявність підключення об'єкта критичної інформаційної інфраструктури до Інтернету, інших інформаційно-телекомунікаційних систем, які не входять до його складу		
Повна назва юридичної особи провайдера (провайдерів) телекомунікацій, що надає (надають) послуги з доступу до Інтернету для об'єкта критичної інформаційної інфраструктури, її (їх) юридична та фактична адреси		
Наявність взаємодії об'єкта критичної інформаційної інфраструктури з іншими об'єктами критичної інформаційної інфраструктури та/або залежності		

функціонування об'єкта критичної інформаційної інфраструктури від інших таких об'єктів		
Наявність атестата відповідності комплексної системи захисту інформації об'єкта критичної інформаційної інфраструктури або результатів незалежного аудиту інформаційної безпеки об'єкта критичної інформаційної інфраструктури		
Особи та/або підрозділ, відповідальні за стан захисту інформації (забезпечення інформаційної безпеки) та кіберзахисту об'єкта критичної інформаційної інфраструктури, у тому числі ті, на яких покладено функції служби захисту інформації (П.І.Б., номер телефону, адреса електронної пошти)		
Наявні відомості, у тому числі статистичні, щодо кіберінцидентів, які мали місце на об'єкті критичної інфраструктури		

(найменування посади керівника об'єкта критичної інфраструктури – до пункту 6, 7 Порядку найменування посади керівника уповноваженого органу сектору (підсектору) критичної інфраструктури – до пункту 11 Порядку)	(підпис)	(прізвище, ім'я, по-батькові)

___ _____ 20__ р.

Валентин ПЕТРОВ

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2019 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 механізм 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:

безпека об'єкта критичної інфраструктури – стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи, а також можливість надання ним основних послуг;

власник та/або керівник об'єкта критичної інфраструктури (далі – оператор основних послуг) – державний орган, підприємство, установа, організація, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належать об'єкти критичної інфраструктури та який/яка відповідає за їх поточне функціонування;

життєво важливі послуги та функції (далі – основні послуги) – послуги та функції, які надаються органами державної влади, установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України;

захист об'єктів критичної інформаційної інфраструктури – організаційні, нормативно-правові, інженерно-технічні та інші заходи, спрямовані на забезпечення безпеки об'єктів критичної інформаційної інфраструктури;

ідентифікація об'єкта критичної інформаційної інфраструктури – процедура віднесення об'єкта інформаційної інфраструктури до об'єктів критичної інформаційної інфраструктури;

критична інформаційна інфраструктура — сукупність об'єктів критичної інформаційної інфраструктури;

критична інфраструктура – сукупність об'єктів критичної інфраструктури;

сектор (підсектор) критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до одного сектору (підсектору) економіки та/або мають спільну функціональну спрямованість;

уповноважений орган державної влади відповідальний за сектор (підсектор) критичної інфраструктури (далі – уповноважений орган) – центральний орган виконавчої влади, інший державний орган, який забезпечує формування та/або реалізацію державної політики в одній чи декількох галузях економіки або сферах життєдіяльності суспільства і держави.

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

3. Реєстр формується з метою ведення обліку об'єктів критичної інформаційної інфраструктури об'єктів критичної інфраструктури.

4. Реєстр являє собою інформаційно-телекомунікаційну систему, в якій обробляються та зберігаються відомості про об'єкти критичної інформаційної інфраструктури об'єктів критичної інфраструктури (далі – відомості Реєстру).

5. Розпорядником інформаційно-телекомунікаційної системи Реєстру та володільцем інформації (відомостей), що міститься у Реєстрі, є Адміністрація Держспецзв'язку, яка:

вживає заходів зі створення та адміністрування Реєстру;

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

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

на підставі отриманих відомостей забезпечує формування та оновлення відомостей Реєстру;

забезпечує захист відомостей Реєстру відповідно до вимог законодавства у сфері захисту інформації та державної таємниці;

проводить інші заходи щодо забезпечення функціонування Реєстру.

6. Відомості, які подаються до Реєстру, містять таку інформацію:

повна назва юридичної особи, у власності (розпорядженні) якої знаходиться об'єкт критичної інформаційної інфраструктури, її юридична та фактична адреса, форма власності, П.І.Б. керівника;

повна назва об'єкта критичної інфраструктури, до складу якого входить об'єкт критичної інформаційної інфраструктури, його призначення, сектор та підсектор, до якого він входить, перелік основних послуг, які він надає, категорія критичності;

повна назва об'єкта критичної інформаційної інфраструктури, його призначення, перелік основних послуг, надання яких він забезпечує, категорія критичності;

уповноважений орган сектору (підсектору) критичної інфраструктури, до якого належить об'єкт критичної інфраструктури;

вид інформації за порядком доступу, яка обробляється або планується для оброблення на об'єкті критичної інформаційної інфраструктури;

адреса місця фізичного розташування об'єкта критичної інформаційної інфраструктури;

наявність підключення об'єкта критичної інформаційної інфраструктури до Інтернету, інших інформаційно-телекомунікаційних систем, які не входять до його складу;

повна назва юридичної особи провайдера (провайдерів) телекомунікацій, що надає (надають) послуги з доступу до Інтернету для об'єкта критичної інформаційної інфраструктури, її (їх) юридична та фактична адреси;

наявність 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;

наявність атестата відповідності комплексної системи захисту інформації об'єкта критичної інформаційної інфраструктури або результатів незалежного аудиту інформаційної безпеки об'єкта критичної інформаційної інфраструктури;

особи та/або підрозділ, відповідальні за стан захисту інформації (забезпечення інформаційної безпеки) та кіберзахисту об'єкта критичної інформаційної інфраструктури, у тому числі ті, на яких покладено функції служби захисту інформації;

наявні відомості, у тому числі статистичні, щодо кібератак, які мали місце на об'єкті критичної інфраструктури;

відомості щодо виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 (Офіційний вісник України, 2019 р., № 50, стор. 53), на об'єкті критичної інформаційної інфраструктури.

7. Відомості до Реєстру подаються операторами основних послуг до Адміністрації Держспецзв'язку в електронному вигляді, підписані кваліфікованим електронним підписом керівника об'єкта критичної інфраструктури, на електронних носіях із супровідним листом за підписом керівника об'єкта критичної інфраструктури.

Відомості до Реєстру подаються один 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 об'єкт критичної інформаційної інфраструктури, визначених у пункті 5 цього Порядку, введення в експлуатацію нового або припинення функціонування об'єкта критичної інформаційної інфраструктури.

До Реєстру подаються відомості про об'єкти критичної інформаційної інфраструктури I та II категорій критичності, які внесені до Національного переліку об'єктів критичної інформаційної інфраструктури.

8. Відомості Реєстру є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства у сфері захисту інформації та державної таємниці.

9. Доступ до Реєстру може надаватися зовнішнім авторизованим користувачам за наявності визначених законом підстав з дотриманням вимог законодавства у сфері захисту інформації та державної таємниці. Порядок доступу до інформації Реєстру зовнішніх авторизованих користувачів визначає Адміністрація Держспецзв'язку.

10. Відомості Реєстру можуть надаватися уповноваженому органу за його письмовим запитом у частині сфери його управління.

11. Оператор основних послуг забезпечує подання відомостей до Реєстру та несе відповідальність за несвоєчасність і недостовірність наданих відомостей згідно із законом.

Валентин ПЕТРОВ

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту 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. Резюме

Проєкт 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 – проєкт Постанови) удосконалить порядок формування переліку об'єктів критичної інформаційної інфраструктури та визначить механізм формування та функціонування реєстру об'єктів критичної інформаційної інфраструктури

Прийняття проєкту 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.

2. Проблема, яка потребує розв'язання

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії їм 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 проводитися заходи з кіберзахисту, а також заходи з аудиту інформаційної безпеки.

На сьогодні перелік інформаційно-телекомунікаційних систем об'єктів критично інфраструктури держави формується відповідно до постанови

Кабінету Міністрів України від 23.08.2016 № 563 «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 внесення до переліку об'єктів критичної інформаційної інфраструктури держави (далі – Перелік) систем управління технологічними процесами, кібератака на які може призвести до негативних наслідків.

Крім того, забезпечення кіберзахисту об'єктів критичної інфраструктури в сучасних умовах підвищення кіберзагроз 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).

3. Суть проєкту акта

Проєкт Постанови визначає механізм формування переліку об'єктів критичної інформаційної інфраструктури, основні засади організації діяльності суб'єктів забезпечення кібербезпеки під час його формування, а також механізм внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

Проєкти постанов розроблено з урахуванням вимог законодавства ЄС, зокрема Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 06.07.2019 «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» та Директиви Ради 2008/114/ЄС від 08.12.2008 «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту», та узгоджені з текстом проєкту Закону України «Про критичну інфраструктуру та її захист». Треба також зазначити, що термінологія, яка використовується в проєкті Постанови, максимально наближена до термінології зазначених документів ЄС.

Проєкт Постанови надає можливість операторам основних послуг провести ідентифікацію об'єктів критичної інформаційної інфраструктури, що

забезпечують функціонування об'єкта критичної інфраструктури та надання ним основних послуг, та їх категоризацію. Для оцінки критичності об'єкта інформаційної інфраструктури оператором основних послуг використовуються три критерії.

Об'єкти інформаційної інфраструктури, що відповідають всім трьом критеріям, визначаються оператором основних послуг як об'єкти критичної інформаційної інфраструктури. При цьому категорія критичності об'єкта критичної інформаційної інфраструктури встановлюється за категорією критичності об'єкта критичної інфраструктури.

Визначений проєктом Постанови механізм формування Переліку об'єктів критичної інформаційної інфраструктури та механізм формування та забезпечення функціонування Реєстру цих об'єктів дасть змогу запровадити єдину систему обліку відомостей про об'єкти критичної інформаційної інфраструктури держави.

Одним зі шляхів удосконалення існуючого порядку формування Переліку є залучення до його формування не тільки власників та/або керівників критичної інформаційної інфраструктури, але й уповноважених органів, які через ведення секторальних переліків отримують можливість координувати та контролювати заходи з кіберзахисту на об'єктах критичної інфраструктури, які знаходяться в сфері їх управління.

У проєкті Постанови враховані результати наукових досліджень з питань кіберзахисту критичної інфраструктури, які проводилися на замовлення Адміністрації Держспецзв'язку у 2019 році.

4. Вплив на бюджет

Реалізація проекту Постанови не потребує додаткового фінансування з Державного бюджету України.

5. Позиція заінтересованих сторін

Проєкт Постанови не матиме впливу на ключові інтереси заінтересованих сторін та не потребує проведення консультацій із заінтересованими сторонами.

Проєкт Постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку.

Проєкт Постанови не стосується питань соціально-трудової сфери та сфери наукової та науково-технічної діяльності.

6. Прогноз впливу

Проєкт Постанови є регуляторним актом. Державна регуляторна служба України за результатами проведення аналізу регуляторного впливу проєкту Постанови 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 зазначеного Закону прийняла рішення погодити проєкт Постанови. Проєкт Постанови потребує повторного аналізу Державною регуляторною службою України.

Проєкт Постанови не стосується питання розвитку адміністративно-територіальних одиниць.

Проєкт Постанови не спрямовано безпосередньо на регулювання трудових відносин, а тому реалізація його положень не вплине на ринок праці.

Проєкт Постанови не стосується питань громадського здоров'я, екології та навколишнього середовища, інших сфер суспільних відносин.

7. Позиція заінтересованих органів

Проєкт Постанови потребує повторного погодження з Міністерством цифрової трансформації України, Міністерством фінансів України, Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством внутрішніх справ України, Міністерством оборони України, Міністерством енергетики та захисту довкілля України, Міністерством інфраструктури України, Міністерством розвитку громад та території України, Службою безпеки України, Державною службою України з надзвичайних ситуацій, Національною поліцією, та Адміністрацією Державної прикордонної служби України, з урахуванням абзацу третього пункту 2 § 40 Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 18 серпня 2007 року № 950.

Проєкт Постанови вже надсилався на погодження до Міністерства фінансів України, Міністерства економічного розвитку і торгівлі України, Служби безпеки України, Міністерства внутрішніх справ України, Міністерства енергетики та вугільної промисловості України, Міністерства інфраструктури України, Міністерства оборони України, Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України, Міністерства екології та природних ресурсів України, Державної служби України з надзвичайних ситуацій, Національної поліції України, Державного агентства водних ресурсів України, Адміністрації Державної прикордонної служби України.

Міністерство фінансів України, Міністерство економічного розвитку і торгівлі України, Міністерство внутрішніх справ України, Міністерство інфраструктури України, Міністерство оборони України, Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України, Адміністрація Державної прикордонної служби України, Державна регуляторна служба України погодили без зауважень.

Міністерство енергетики та вугільної промисловості України погоджено із зауваженнями, які враховано частково.

Служба безпеки України, Міністерство екології та природних ресурсів України – погоджено із зауваженнями, які не враховано.

Міністерством юстиції України проведено правову експертизу та погоджено проєкт Постанови із зауваженнями, які було враховано. Проєкт Постанови потребує повторного проведення правової експертизи Міністерством юстиції України.

8. Підстава розроблення проєкту акта

Правовими підставами розроблення проєкту Постанови є вимоги частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» та завдання, передбачене Планом організації підготовки проєктів актів, необхідних для забезпечення реалізації Закону України від 05 жовтня 2017 р. № 2163–VIII «Про основні засади забезпечення кібербезпеки України».

Основними нормативно-правовими актами у сфері регулювання проєкту 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», 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».

Голова Державної служби спеціального зв'язку та захисту інформації України Валентин ПЕТРОВ

«22» 11 2019 року

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту 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. Резюме

Проєкт 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 – проєкт Постанови) удосконалить порядок формування переліку об'єктів критичної інформаційної інфраструктури та визначить механізм формування та функціонування реєстру об'єктів критичної інформаційної інфраструктури

Прийняття проєкту 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.

2. Проблема, яка потребує розв'язання

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії їм 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 проводитися заходи з кіберзахисту, а також заходи з аудиту інформаційної безпеки.

На сьогодні перелік інформаційно-телекомунікаційних систем об'єктів критично інфраструктури держави формується відповідно до постанови

Кабінету Міністрів України від 23.08.2016 № 563 «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 внесення до переліку об'єктів критичної інформаційної інфраструктури держави (далі – Перелік) систем управління технологічними процесами, кібератака на які може призвести до негативних наслідків.

Крім того, забезпечення кіберзахисту об'єктів критичної інфраструктури в сучасних умовах підвищення кіберзагроз 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).

3. Суть проєкту акта

Проєкт Постанови визначає механізм формування переліку об'єктів критичної інформаційної інфраструктури, основні засади організації діяльності суб'єктів забезпечення кібербезпеки під час його формування, а також механізм внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

Проєкти постанов розроблено з урахуванням вимог законодавства ЄС, зокрема Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 06.07.2019 «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» та Директиви Ради 2008/114/ЄС від 08.12.2008 «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту», та узгоджені з текстом проєкту Закону України «Про критичну інфраструктуру та її захист». Треба також зазначити, що термінологія, яка використовується в проєкті Постанови, максимально наближена до термінології зазначених документів ЄС.

Проєкт Постанови надає можливість операторам основних послуг провести ідентифікацію об'єктів критичної інформаційної інфраструктури, що

забезпечують функціонування об'єкта критичної інфраструктури та надання ним основних послуг, та їх категоризацію. Для оцінки критичності об'єкта інформаційної інфраструктури оператором основних послуг використовуються три критерії.

Об'єкти інформаційної інфраструктури, що відповідають всім трьом критеріям, визначаються оператором основних послуг як об'єкти критичної інформаційної інфраструктури. При цьому категорія критичності об'єкта критичної інформаційної інфраструктури встановлюється за категорією критичності об'єкта критичної інфраструктури.

Визначений проєктом Постанови механізм формування Переліку об'єктів критичної інформаційної інфраструктури та механізм формування та забезпечення функціонування Реєстру цих об'єктів дасть змогу запровадити єдину систему обліку відомостей про об'єкти критичної інформаційної інфраструктури держави.

Одним зі шляхів удосконалення існуючого порядку формування Переліку є залучення до його формування не тільки власників та/або керівників критичної інформаційної інфраструктури, але й уповноважених органів, які через ведення секторальних переліків отримують можливість координувати та контролювати заходи з кіберзахисту на об'єктах критичної інфраструктури, які знаходяться в сфері їх управління.

У проєкті Постанови враховані результати наукових досліджень з питань кіберзахисту критичної інфраструктури, які проводилися на замовлення Адміністрації Держспецзв'язку у 2019 році.

4. Вплив на бюджет

Реалізація проекту Постанови не потребує додаткового фінансування з Державного бюджету України.

5. Позиція заінтересованих сторін

Проєкт Постанови не матиме впливу на ключові інтереси заінтересованих сторін та не потребує проведення консультацій із заінтересованими сторонами.

Проєкт Постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку.

Проєкт Постанови не стосується питань соціально-трудової сфери та сфери наукової та науково-технічної діяльності.

6. Прогноз впливу

Проєкт Постанови є регуляторним актом. Державна регуляторна служба України за результатами проведення аналізу регуляторного впливу проєкту Постанови 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 зазначеного Закону прийняла рішення погодити проєкт Постанови. Проєкт Постанови потребує повторного аналізу Державною регуляторною службою України.

Проєкт Постанови не стосується питання розвитку адміністративно-територіальних одиниць.

Проєкт Постанови не спрямовано безпосередньо на регулювання трудових відносин, а тому реалізація його положень не вплине на ринок праці.

Проєкт Постанови не стосується питань громадського здоров'я, екології та навколишнього середовища, інших сфер суспільних відносин.

7. Позиція заінтересованих органів

Проєкт Постанови потребує повторного погодження з Міністерством цифрової трансформації України, Міністерством фінансів України, Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством внутрішніх справ України, Міністерством оборони України, Міністерством енергетики та захисту довкілля України, Міністерством інфраструктури України, Міністерством розвитку громад та території України, Службою безпеки України, Державною службою України з надзвичайних ситуацій, Національною поліцією, та Адміністрацією Державної прикордонної служби України, з урахуванням абзацу третього пункту 2 § 40 Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 18 серпня 2007 року № 950.

Проєкт Постанови вже надсилався на погодження до Міністерства фінансів України, Міністерства економічного розвитку і торгівлі України, Служби безпеки України, Міністерства внутрішніх справ України, Міністерства енергетики та вугільної промисловості України, Міністерства інфраструктури України, Міністерства оборони України, Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України, Міністерства екології та природних ресурсів України, Державної служби України з надзвичайних ситуацій, Національної поліції України, Державного агентства водних ресурсів України, Адміністрації Державної прикордонної служби України.

Міністерство фінансів України, Міністерство економічного розвитку і торгівлі України, Міністерство внутрішніх справ України, Міністерство інфраструктури України, Міністерство оборони України, Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України, Адміністрація Державної прикордонної служби України, Державна регуляторна служба України погодили без зауважень.

Міністерство енергетики та вугільної промисловості України погоджено із зауваженнями, які враховано частково.

Служба безпеки України, Міністерство екології та природних ресурсів України – погоджено із зауваженнями, які не враховано.

Міністерством юстиції України проведено правову експертизу та погоджено проєкт Постанови із зауваженнями, які було враховано. Проєкт Постанови потребує повторного проведення правової експертизи Міністерством юстиції України.

8. Підстава розроблення проєкту акта

Правовими підставами розроблення проєкту Постанови є вимоги частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» та завдання, передбачене Планом організації підготовки проєктів актів, необхідних для забезпечення реалізації Закону України від 05 жовтня 2017 р. № 2163–VIII «Про основні засади забезпечення кібербезпеки України».

Основними нормативно-правовими актами у сфері регулювання проєкту 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», 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».

Голова Державної служби спеціального зв'язку та захисту інформації України Валентин ПЕТРОВ

«27» 11 2019 року

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проєкту 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

Проєкт 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 – проєкт 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 їм 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.

Так, протягом останніх трьох років на інформаційно-телекомунікаційні системи деяких об'єктів, які за своїм значенням і роллю для життєдіяльності суспільства є об'єктами критичної інфраструктури, здійснено низку масштабних кібератаки, зокрема:

1) 21 - 25 травня 2014 року відбулися DDoS-атаки і злом сайта ЦВК під час президентських виборів, внаслідок чого на сайті з'явилися хибні результати. Незважаючи на повідомлення про злом сайта ЦВК, саме ці дані були озвучені в новинах на російському Першому каналі як реальні результати виборів в Україні;

2) у червні 2014 року на серверах приватних компаній України і країн НАТО були виявлені шкідливі програми, які займалися кібершпіонажем. Серед них такі як Turla/Uroburos/Snake, RedOctober, MiniDuke і NetTraveler;

3) 23 грудня 2015 року за допомогою троянської програми BlackEnergy3, у використанні якої були раніше помічені російські хакери, було відключено близько 30 підстанцій Прикарпаттяобленерго, через що більш ніж 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго;

4) 6 грудня 2016 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, яка

вивела з ладу низку комп'ютерів, а також знищила критично важливі бази даних, що призвело до затримки бюджетних виплат та завдало шкоди на сотні мільйонів гривень;

5) 15 грудня 2016 року українські хакери на замовлення невстановленої особи із Санкт-Петербурга здійснили DDOS-атаку на сайт Укрзалізниці, внаслідок чого протягом дня була повністю заблокована його робота. Атака була націлена на крадіжку даних про пассажироперевезення;

6) 17 грудня 2016 року кібератака на підстанцію Північної компанії Укренерго призвела до збою в автоматиці управління, через що більше години знеструмленими залишалися райони у північній частині правобережного Києва і прилеглі райони області.

7) у першій половині дня 27 червня 2017 року розпочалася масова кібератака на український державний та комерційний сектор із застосування шкідливого програмного забезпечення – віруса-шифрувальника файлів Petya Ransomware. Її жертвами стали інформаційно-телекомунікаційні системи "Укрпошти", аеропорту "Бориспіль", "Укренерго", ДТЕК, багатьох банків, ЗМІ, телеканалів, АЗС і інших компаній.

Загалом кібератаки на комунікаційні системи та системи управління технологічними процесами об'єктів критичної інфраструктури держави можуть призвести та призводять до виникнення надзвичайних ситуацій техногенного характеру, можуть мати негативний вплив на стан енергетичної, екологічної, економічної, національної безпеки держави. Тому забезпечення кібербезпеки комунікаційних та технологічних систем, що забезпечують функціонування об'єктів критичної інфраструктури, сьогодні виходить на перший план діяльності у сфері національної безпеки і вимагає розбудови в Україні цілісної системи кібербезпеки.

Як один з перших кроків – чітке окреслення об'єктів кібербезпеки, передусім шляхом визначення переліку тих об'єктів критичної інформаційної інфраструктури, щодо яких пріоритетно мають проводитися 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 від 23.08.2016 № 563 «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 внесення 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 підтримання 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 немає механізму 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 чинних регуляторних актів, оскільки на сьогодні таких нормативно-правових актів немає.

II. Цілі державного регулювання

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

Одним зі 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 через те, що норми, викладені 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 у повному обсязі відповідають нормам Закону України «Про основні засади забезпечення кібербезпеки України» та не дозволяють повною мірою охопити всі об'єкти критичної інформаційної інфраструктури
Альтернатива 2	Прийняття проєкту 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	Немає, 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	Додаткових витрат 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	Додаткових витрат не потребує
Альтернатива 3	Немає, 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	Додаткових витрат не потребує

	від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки	

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	Відповідно до Зеленої книги з питань захисту критичної інфраструктури в Україні, підготовленої Національним інститутом стратегічних досліджень із залученням українських та іноземних експертів і за підтримки Офісу зв'язку НАТО, в Україні на сьогодні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних. Понад чверть з них ідентифіковані як об'єкти підвищеної небезпеки. З прийняттям проєкту Постанови буде задіяний галузевий (секторальний) підхід віднесення об'єктів до об'єктів критичної інформаційної інфраструктури, що дозволить чітко визначити всі об'єкти критичної інформаційної інфраструктури.		Дія регуляторного акта не буде розповсюджуватися на малі та мікро суб'єктіви господарювання		–
Питома вага групи у загальній	Питома вага великих та середніх суб'єктів		0		100 %

кількості, відсотків	господарювання у загальній кількості може бути визначена тільки після віднесення об'єктів до об'єктів критичної інформаційної інфраструктури, 100 %		

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає, 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 проєкту 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	Немає, 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

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	Немає	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	Немає	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.

Проєкт Постанови визначає механізм формування переліку об'єктів критичної інформаційної інфраструктури, основні засади організації діяльності суб'єктів забезпечення кібербезпеки під час його формування, а також механізм внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

Проєкт Постанови розроблено з урахуванням вимог та Директиви Ради 2008/114/ЄС від 8.12.2008 «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту» та Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 06.07.2019 «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» (далі – Директива ЄС 2016/1148). Треба також зазначити, що термінологія, яка використовується в проєкті Постанови, максимально наближена до термінології зазначених документів ЄС.

Проєкт Постанови надає можливість операторам основних послуг провести ідентифікацію об'єктів критичної інформаційної інфраструктури, що забезпечують функціонування об'єкта критичної інфраструктури та надання ним основних послуг, та їх категоризацію. Для оцінки критичності об'єкта інформаційної інфраструктури оператором основних послуг використовуються три критерії.

Об'єкти інформаційної інфраструктури, що відповідають всім трьом критеріям, визначаються оператором основних послуг як об'єкти критичної інформаційної інфраструктури. При цьому категорія критичності об'єкта критичної інформаційної інфраструктури встановлюється за категорією критичності об'єкта критичної інфраструктури.

Визначений проєктом Постанови механізм формування Переліку об'єктів критичної інформаційної інфраструктури та механізм формування та забезпечення функціонування Реєстру цих об'єктів дасть змогу запровадити єдину систему обліку відомостей про об'єкти критичної інформаційної інфраструктури держави.

Одним зі шляхів удосконалення існуючого порядку формування Переліку є залучення до його формування не тільки власників та/або керівників критичної інформаційної інфраструктури, але й уповноважених органів, які через ведення секторальних переліків отримують можливість координувати та контролювати заходи з кіберзахисту на об'єктах критичної інфраструктури, які знаходяться в сфері їх управління.

Для досягнення цієї цілі проєктом 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 проєкт Постанови з Міністерством цифрової трансформації України, Міністерством фінансів України, Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством внутрішніх справ України, Міністерством оборони України, Міністерством енергетики та захисту довкілля України, Міністерством інфраструктури України, Міністерством розвитку громад та території України, Службою безпеки України, Державною службою України з надзвичайних ситуацій, Національною поліцією та Адміністрацією Державної прикордонної служби України;

надіслати проєкт Постанови на правову експертизу до Міністерства юстиції України;

забезпечити інформування громадськості про вимоги регуляторного акта шляхом його оприлюднення на офіційному вебсайті Держспецзв'язку;

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

Реалізація положень проєкту 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.

Державний реєстр об'єктів критичної інформаційної інфраструктури також може стати системою раннього попередження про кіберзагрози шляхом надання методичної допомоги та попереджень щодо виявлених вразливостей (загроз) у програмному забезпеченні, операційних системах тощо, 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 об'єктів критичної інфраструктури.

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

Упровадження положень проєкту 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 регуляторним актом настає з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності проєкту Постанови як регуляторного акта є:

розмір надходжень до державного та місцевого бюджетів і державних цільових фондів, пов'язаних з дією акта, – надходжень не передбачається;

кількість суб'єктів господарювання та/або фізичних осіб, на яких поширюватиметься дія акта, – відповідно до Зеленої книги з питань захисту критичної інфраструктури в Україні, підготовленої Національним інститутом стратегічних досліджень із залученням українських та зарубіжних експертів і за підтримки Офісу зв'язку НАТО в Україні, в Україні на сьогодні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних. Понад чверть з них ідентифіковані як об'єкти підвищеної небезпеки. З прийняттям проєкту Постанови буде задіяний галузевий (секторальний) підхід до віднесення об'єктів до об'єктів критичної інформаційної інфраструктури, що дозволить чітко визначити всі об'єкти критичної інформаційної інфраструктури. Дія проєкту Постанови буде стосуватися тільки великих та середніх суб'єктів господарювання та не стосуватиметься фізичних осіб;

розмір коштів і час, що витрачатимуться суб'єктами господарювання та/або фізичними особами, пов'язаними з виконанням вимог акта – додаткових витрат та часу від суб'єктів господарювання, пов'язаними з виконанням вимог акта, не передбачається;

рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта – проєкт акта розміщено на вебсайті Держспецзв'язку (електронна адреса: www.dsszzi.gov.ua) у підрозділі «Повідомлення про оприлюднення та проєкти» розділу «Регуляторна діяльність»;

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

кількість об'єктів критичної інформаційної інфраструктури, внесених до Реєстру;

кількість сформованих галузевих переліків об'єктів критичної інформаційної інфраструктури;

кількість вжитих 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 акта з метою внесення до нього змін.

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

Повторне відстеження результативності регуляторного акта буде здійснюватися не пізніше двох років з дня набрання чинності цього документу шляхом аналізу статистичних даних.

Періодичні відстеження результативності регуляторного акта будуть здійснюватися 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 Валентин ПЕТРОВ

«22» 11 2019 року

Повідомлення про оприлюднення проєкту постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури»

1. Стислий виклад змісту проєкту акта

Проєкт постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури» 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».

Проєкт Постанови визначає механізм і критерії віднесення об'єктів до об'єктів критичної інфраструктури, перелік секторів (підсекторів), основних послуг критичної інфраструктури держави та механізм віднесення об'єкта критичної інфраструктури до однієї з категорій критичності.

2. Адреси для зауважень та пропозицій до проєкту акта

Пропозиції та зауваження до проєкту 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) 281-87-54;

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 проєкту акта

Проєкт акта та аналіз його регуляторного впливу розміщено на веб-сайті Держспецзв'язку (електронна адреса: www.dsszzi.gov.ua) у підрозділі «Оприлюднення проєктів регуляторних актів» розділу «Регуляторна діяльність».

4. Строк, протягом якого приймаються зауваження та пропозиції

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

Голова Державної служби спеціального зв'язку та захисту інформації України Валентин ПЕТРОВ

«12» 11 2019 р.

Повідомлення про оприлюднення
проєкту 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 проєкту акта

Проєкт 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» 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».

Проєкт Постанови визначає механізм формування переліку об'єктів критичної інформаційної інфраструктури, основні засади організації діяльності суб'єктів забезпечення кібербезпеки під час його формування, а також механізм 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 проєкту акта

Пропозиції та зауваження до проєкту 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) 281-87-54;
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 проєкту акта

Проєкт акта та аналіз його регуляторного впливу розміщено на веб-сайті Держспецзв'язку (електронна адреса: www.dsszzi.gov.ua) у підрозділі «Оприлюднення проєктів регуляторних актів» розділу «Регуляторна діяльність».

4. Строк, протягом якого приймаються зауваження та пропозиції

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

Голова Державної служби спеціального
зв'язку та захисту інформації України Валентин ПЕТРОВ

«22» 11 2019 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту постанови Кабінету Міністрів України
«Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури»

1. Резюме

Проєкт постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури» (далі – проєкт Постанови) створить правові засади для визначення порядку віднесення підприємств, установ та організацій до об'єктів критичної інфраструктури.

Прийняття проєкту Постанови дозволить створити правові засади для формування критеріїв та визначення порядку віднесення до критичної інфраструктури тих об'єктів, які є важливими для економіки і національної безпеки та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

2. Проблема, яка потребує розв'язання

Законом України «Про основні засади забезпечення кібербезпеки України» визначено, що до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; 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.

Віднесення об'єктів до об'єктів критичної інфраструктури є обов'язковою умовою для формування цілісної системи захисту критичної інфраструктури, зокрема й у контексті захисту її від загроз у кіберпросторі, зважаючи на роль інформаційно-комунікаційних технологій у процесах забезпечення функціонування сучасних інфраструктурних об'єктів.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до вирішення завдань із захисту інфраструктурних об'єктів від сучасних загроз на загальнодержавному рівні, вироблення критеріїв та визначення порядку віднесення об'єктів до об'єктів критичної інфраструктури є першим кроком на шляху створення цілісної системи захисту критичної інфраструктури.

Головним критерієм віднесення об'єктів до об'єктів критичної інфраструктури є визнання того, що наслідки порушення сталого функціонування одного або низки об'єктів критичної інфраструктури можуть спричинити надзвичайні ситуації та/або мати негативний вплив на стан екологічної, енергетичної, економічної фінансової безпеки, на стан обороноздатності держави, порушити систему управління нею. Тому передусім необхідно визначити важливість інфраструктурних об'єктів для надання основних послуг у всіх

секторах економіки та сферах діяльності задля впровадження низки заходів щодо захисту таких об'єктів від реалізації можливості виникнення кризових ситуацій.

3. Суть проєкту акта

Проєкт Постанови визначає механізм і критерії віднесення об'єктів до об'єктів критичної інфраструктури, перелік секторів (підсекторів), основних послуг критичної інфраструктури держави та механізм віднесення об'єкта критичної інфраструктури до однієї з категорій критичності.

Проєкт Постанови розроблено з урахуванням вимог законодавства ЄС, зокрема Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 06.07.2019 «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» та Директиви Ради 2008/114/ЄС від 08.12.2008 «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту», та узгоджені з текстом проєкту Закону України «Про критичну інфраструктуру та її захист». Треба також зазначити, що термінологія, яка використовується в проєкті Постанови, максимально наближена до термінології зазначених документів ЄС.

Порядок віднесення об'єктів до об'єктів критичної інфраструктури, який входить до складу проєкту Постанови, встановлює категорії критичності об'єктів критичної інфраструктури, механізм ідентифікації таких об'єктів уповноваженими органами державної влади, відповідальними за сектор (підсектор) критичної інфраструктури та їх категоризацію уповноваженими органами спільно з операторами основних послуг, а також визначає необхідність формування Національного переліку об'єктів критичної інфраструктури та секторальних переліків об'єктів критичної інфраструктури та відповідальних за їх формування.

Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави, який входить до складу проєкту Постанови, визначає перелік основних послуг, які надаються об'єктами критичної інфраструктури і є послугами та функціями, які надаються органами державної влади, державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України.

Перелік визначає також сектори та підсектори, об'єкти інфраструктури яких належиться до критичної інфраструктури, за умови, що такі об'єкти надають основні послуги, визначені для такого сектору або підсектору. Треба зазначити, що перелік секторів (підсекторів), основних послуг гармонізовано з відповідним переліком, який наведено в Директиві ЄС 2016/1148.

Також у Переліку секторів (підсекторів), основних послуг критичної інфраструктури держави наведено уповноважені органи державної влади, відповідальні за кожний сектор або підсектор критичної інфраструктури держави.

Методика категоризації об'єктів критичної інфраструктури, яка входить до складу проєкту Постанови, визначає процедуру віднесення об'єктів критичної інфраструктури до певної категорії критичності.

Для визначення категорії об'єкта критичної інфраструктури уповноважені органи в своїх секторах разом з операторами критичної інфраструктури проводять бальну оцінку критичності кожного об'єкта критичної інфраструктури за допомогою форм із секторальними та міжсекторальними критеріями визначення рівня негативного впливу, які наведені у додатках до Методики.

Зазначені критерії враховують важливість об'єкта критичної інфраструктури на основі аналізу потенційної шкоди, яку суспільство, навколишнє середовище, економіка та національна безпека держави можуть зазнати внаслідок порушення або припинення функціонування об'єкта інфраструктури. Важливість об'єктів інфраструктури оцінюється за допомогою низки секторальних та міжсекторальних критеріїв.

Сума всіх балів, що отримується під час оцінки об'єкта критичної інфраструктури згідно із секторальними та міжсекторальними критеріями визначення рівня негативного впливу, використовується для розрахунку узагальненої нормованої оцінки рівня критичності об'єкта за формулою та правилом, які наведені у документі.

Також в додатку до Методики категоризації об'єктів критичної інфраструктури наведено приклад категоризацію об'єкта критичної інфраструктури на прикладі підприємства, яке надає послуги кваліфікованого надавача електронних довірчих послуг.

У проєкті Постанови враховані результати наукових досліджень з питань кіберзахисту критичної інфраструктури, які проводилися на замовлення Адміністрації Держспецзв'язку у 2019 році.

4. Вплив на бюджет

Реалізація проєкту Постанови не потребує додаткового фінансування з Державного бюджету України.

5. Позиція заінтересованих сторін

Проєкт Постанови не матиме впливу на ключові інтереси заінтересованих сторін та не потребує проведення консультацій із заінтересованими сторонами.

Проєкт Постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку.

Проєкт Постанови не стосується питань соціально-трудової сфери та сфери наукової та науково-технічної діяльності.

6. Прогноз впливу

Проєкт Постанови є регуляторним актом. Державна регуляторна служба України за результатами проведення аналізу регуляторного впливу проєкту Постанови 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 зазначеного Закону прийняла рішення погодити проєкт Постанови. У зв'язку зі значними змінами в тексті проєкт Постанови потребує повторного аналізу Державною регуляторною службою України.

Проєкт Постанови не стосується питання розвитку адміністративно-територіальних одиниць.

Проєкт Постанови не спрямований безпосередньо на регулювання трудових відносин, а тому реалізація його положень не вплине на ринок праці.

Проєкт Постанови не стосується питань громадського здоров'я, екології та навколишнього середовища, інших сфер суспільних відносин.

7. Позиція заінтересованих органів

Проєкт Постанови потребує повторного погодження з Міністерством цифрової трансформації України, Міністерством фінансів України, Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством внутрішніх справ України, Міністерством оборони України, Міністерством енергетики та захисту довкілля України, Міністерством інфраструктури України, Міністерством розвитку громад та території України, Службою безпеки України, Державною службою України з надзвичайних ситуацій, Національною поліцією, та Адміністрацією Державної прикордонної служби України з урахуванням абзацу третього пункту 2 § 40 Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 18 серпня 2007 року № 950.

Проєкт Постанови вже надсилався на погодження до Міністерства фінансів України, Міністерства економічного розвитку і торгівлі України, Служби безпеки України, Міністерства внутрішніх справ України, Міністерства енергетики та вугільної промисловості України, Міністерства інфраструктури України, Міністерства оборони України, Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України, Міністерства екології та природних ресурсів України, Державної служби України з надзвичайних ситуацій, Національної поліції України, Державного агентства водних ресурсів України, Адміністрації Державної прикордонної служби України.

Міністерство фінансів України, Служба безпеки України, Міністерство інфраструктури України, Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України, Національна поліція України, Державне агентство водних ресурсів України, Адміністрація Державної прикордонної служби України, Державна регуляторна служба України, Міністерство екології та природних ресурсів України погодили без зауважень.

Міністерство економічного розвитку і торгівлі України погодило без зауважень, але з пропозиціями, які враховано.

Міністерство внутрішніх справ України, Міністерство енергетики та вугільної промисловості України, Міністерство оборони України, Державна служба України з надзвичайних ситуацій погодили із зауваженнями, які враховано частково.

Міністерством юстиції України проведено правову експертизу та погоджено проєкт Постанови із зауваженнями, які було враховано. Проєкт Постанови потребує повторного проведення правової експертизи Міністерством юстиції України.

8. Підстава розроблення проєкту акта

Правовими підставами розроблення проєкту Постанови є вимоги частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» та завдання, передбачене Планом організації підготовки проєктів актів, необхідних для забезпечення реалізації Закону України від 05 жовтня 2017 р. № 2163–VIII «Про основні засади забезпечення кібербезпеки України».

Правову основу забезпечення кібербезпеки України становлять Конституція України, Закон України «Про основи національної безпеки України», інші закони України, Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти.

Голова Державної служби спеціального зв'язку та захисту інформації України Валентин ПЕТРОВ

«22» 11 2019 року

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проєкту постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури»

I. Визначення проблеми

Проєкт постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури» (далі – проєкт Постанови) підготовлено Адміністрацією Державної служби спеціальної зв'язку та захисту інформації України на виконання вимог частини другої статті 6 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 їм та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів.

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 можуть призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави.

Так, протягом останніх трьох років на інформаційно-телекомунікаційні системи деяких об'єктів, які за своїм значенням і роллю для життєдіяльності суспільства є об'єктами критичної інфраструктури, здійснено низку масштабних кібератаки, зокрема:

1) 21-25 травня 2014 року відбулися DDoS-атаки і злом сайта ЦВК під час президентських виборів, внаслідок яких на сайті з'явилися помилкові результати. Незважаючи на повідомлення про злом, саме ці дані були озвучені в новинах на російському Першому каналі як реальні результати виборів в Україні;

2) у червні 2014 року на серверах приватних компаній України і країн НАТО були виявлені шкідливі програми, які займалися кібершпіонажем. Серед них такі як Turla/Uroburos/Snake, RedOctober, MiniDuke і NetTraveler;

3) 23 грудня 2015 року за допомогою троянської програми BlackEnergy3, у використанні якої були раніше помічені російські хакери, було відключено близько 30 підстанцій Прикарпаттяобленерго, в зв'язку з чим більш 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго;

4) 6 грудня 2016 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, яка вивела з ладу низку комп'ютерів, а також знищила критично важливі бази даних, що призвело до затримки бюджетних виплат на сотні мільйонів гривень;

5) 15 грудня 2016 року українські хакери на замовлення невстановленої особи з Санкт-Петербурга здійснили DDOS-атаку на сайт Укрзалізниці, внаслідок чого протягом дня була повністю заблокована його робота. Атака була націлена на крадіжку даних про пассажироперевезення;

6) 17 грудня 2016 року кібератака на підстанцію Північна компанії Укренерго призвела до збою в автоматиці управління, через що більше години знеструмленими залишалися райони у північній частині правобережного Києва і прилеглі райони області;

7) у першій половині дня 27 червня 2017 року розпочалася масова кібератака на український державний та комерційний сектор із застосування шкідливого програмного забезпечення – віруса-шифрувальника файлів Petya Ransomware. Її жертвами стали інформаційно-телекомунікаційні системи "Укрпошти", аеропорту "Бориспіль", "Укренерго", ДТЕК, багатьох банків, ЗМІ, телеканалів, АЗС і багатьох інших компаній.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Водночас набуття чинності Законом України «Про основні засади забезпечення кібербезпеки України» визначає, що до Переліку об'єктів критичної інфраструктури (далі – Перелік) можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; 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.

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. Важливим кроком при формуванні Переліку є визначення критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури.

На сьогодні результатом кібератак є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування об'єктів критичної інфраструктури, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку з цим існуючі кіберзагрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки. Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» визначено базовий перелік вимог з кіберзахисту, які повинні

бути впроваджені на об'єкті критичної інфраструктури. Однак без визначення порядку віднесення об'єктів до об'єктів критичної інфраструктури ця постанова не може бути застосована суб'єктами кіберзахисту.

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 на сьогодні немає критеріїв та поряду віднесення об'єктів до об'єктів критичної інфраструктури.

Проблема не може бути розв'язана за допомогою чинних регуляторних актів, оскільки на сьогодні таких нормативно-правових актів немає.

II. Цілі державного регулювання

Проєкт Постанови створить правові засади для визначення порядку віднесення підприємств, установ та організацій до об'єктів критичної інфраструктури.

Прийняття проєкту Постанови дозволить створити правові засади для формування критеріїв та визначення порядку віднесення до критичної інфраструктури тих об'єктів, які є важливими для економіки і національної безпеки та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Збереження чинного стану законодавства, що призведе до неможливості визначення об'єктів критичної інфраструктури та, як наслідок, завадить запровадженню системного підходу до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури
Альтернатива 2	Прийняття проєкту Постанови
Альтернатива 3	Внесення змін до чинного законодавства, які передбачать введення норм щодо віднесення до об'єктів критичної інфраструктури всіх суб'єктів господарювання, в тому числі суб'єктів малого

	підприємництва, які безпосередньо не впливають на стан національної безпеки і оборони, а також висування до них вимог із кіберзахисту

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає, оскільки такий підхід призведе до неможливості визначення об'єктів критичної інфраструктури та, як наслідок, завадить запровадженню системного підходу до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури	Додаткових витрат не потребує
Альтернатива 2	Високі, оскільки прийняття Постанови дозволить визначити об'єкти критичної інфраструктури та, як наслідок, запровадити системний підхід до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури, зокрема шляхом висування до таких об'єктів вимог із кіберзахисту	Додаткових витрат не потребує
Альтернатива 3	Немає, оскільки такий підхід призведе до надмірної кількості об'єктів критичної інфраструктури, в тому числі суб'єктів малого підприємництва, які безпосередньо не впливають на стан національної безпеки і оборони	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	Відповідно до Зеленої книги з питань захисту критичної інфраструктури в Україні, підготовленої Національним інститутом стратегічних досліджень із залученням українських та зарубіжних експертів і за підтримки Офісу зв'язку НАТО, в Україні, в Україні на сьогодні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних. Понад чверть з них ідентифіковані як об'єкти підвищеної небезпеки. З прийняттям проєкту Постанови буде задіяний галузевий (секторальний) підхід до віднесення об'єктів до об'єктів критичної інфраструктури, що дозволить чітко визначити всі об'єкти критичної інфраструктури.		Дія регуляторного акта не буде розповсюджуватися на малі та мікро суб'єкти господарювання		–

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 інфраструктури, - %.	0	100 %

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає, оскільки такий підхід призведе до неможливості визначення об'єктів критичної інфраструктури, та висування до них вимог із кіберзахисту, що може призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави у випадку здійснення терористичних актів по відношенню до таких об'єктів	Додаткових витрат не потребує
Альтернатива 2	Високі, оскільки прийняття проєкту Постанови дозволить визначити об'єкти критичної інфраструктури, що дозволить власникам та/або керівникам підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури впровадити на цих об'єктах заходи із захисту, зокрема із кіберзахисту, що може завадити виникненню надзвичайних ситуацій	Додаткових витрат не потребує

	техногенного характеру та/або негативного впливу на стан екологічної безпеки держави у випадку здійснення терористичних актів по відношенню до таких об'єктів.	
Альтернатива 3	Немає, оскільки такий підхід призведе до надмірної кількості об'єктів критичної інфраструктури, в тому числі суб'єктів малого підприємництва, які безпосередньо не впливають на стан національної безпеки і оборони	Додаткових витрат не потребує

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	Немає	Додаткових витрат не потребує	Проблема продовжує існувати
Альтернатива 2	Визначення об'єктів критичної інфраструктури, та висунення до них вимог із кіберзахисту, що може завадити виникненню надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави у	Додаткових витрат не потребує	Проблема більше існувати не буде

	випадку здійснення терористичних актів по відношенню до таких об'єктів		
Альтернатива 3	Немає	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.

Законом України «Про основні засади забезпечення кібербезпеки України» визначено, що до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; 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.

Віднесення об'єктів до об'єктів критичної інфраструктури є обов'язковою умовою для формування цілісної системи захисту критичної інфраструктури, зокрема й у контексті захисту її від загроз у кіберпросторі, зважаючи на роль інформаційно-комунікаційних технологій у процесах забезпечення функціонування сучасних інфраструктурних об'єктів.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до вирішення завдань із захисту інфраструктурних об'єктів від сучасних загроз на загальнодержавному рівні, вироблення критеріїв та визначення порядку віднесення об'єктів до об'єктів критичної інфраструктури є першим кроком на шляху створення цілісної системи захисту критичної інфраструктури.

Головним критерієм віднесення об'єктів до об'єктів критичної інфраструктури є визнання того, що наслідки порушення сталого функціонування одного або низки об'єктів критичної інфраструктури можуть спричинити надзвичайні ситуації та/або мати негативний вплив на стан екологічної, енергетичної, економічної фінансової безпеки, на стан

обороноздатності держави, порушити систему управління нею. Тому передусім необхідно визначити важливість інфраструктурних об'єктів для надання основних послуг у всіх секторах економіки та сферах діяльності задля впровадження низки заходів щодо захисту таких об'єктів від реалізації можливості виникнення кризових ситуацій.

Для досягнення цієї цілі проєктом Постанови передбачається:

затвердити Порядок віднесення об'єктів до об'єктів критичної інфраструктури.

Заходи, що пропонуються для розв'язання проблеми:

погодити проєкт Постанови з Міністерством цифрової трансформації України, Міністерством фінансів України, Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством внутрішніх справ України, Міністерством оборони України, Міністерством енергетики та захисту довкілля України, Міністерством інфраструктури України, Міністерством розвитку громад та території України, Службою безпеки України, Державною службою України з надзвичайних ситуацій, Національною поліцією, та Адміністрацією Державної прикордонної служби України;

надіслати проєкт Постанови на правову експертизу до Міністерства юстиції України;

забезпечити інформування громадськості про вимоги регуляторного акта шляхом його оприлюднення на офіційному вебсайті Держспецзв'язку;

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

Реалізація положень проєкту Постанови:

Дозволить створити правові засади для формування критеріїв та визначення порядку віднесення до критичної інфраструктури тих об'єктів, які є важливими для економіки і національної безпеки та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

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

Упровадження положень проєкту Постанови дозволить створити дієвий механізм визначення об'єктів критичної інфраструктури та, як наслідок, запровадити системний підхід до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури, зокрема шляхом висування до таких об'єктів вимог із кіберзахисту.

Такі вимоги з кіберзахисту стануть обов'язковими до виконання підприємствами, установами та організаціями, які згідно із законодавством віднесені до об'єктів критичної інфраструктури.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується.

Строк набрання чинності регуляторним актом настає з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності проєкту Постанови як регуляторного акта є:

розмір надходжень до державного та місцевого бюджетів і державних цільових фондів, пов'язаних з дією акта, – надходжень не передбачається;

кількість суб'єктів господарювання та/або фізичних осіб, на яких поширюватиметься дія акта, – відповідно до Зеленої книги з питань захисту критичної інфраструктури в Україні, підготовленої Національним інститутом стратегічних досліджень із залученням українських та зарубіжних експертів і за підтримки Офісу зв'язку НАТО в Україні, в Україні на сьогодні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних. Понад чверть з них ідентифіковані як об'єкти підвищеної небезпеки. З прийняттям проєкту Постанови буде задіяний галузевий (секторальний) підхід до віднесення об'єктів до об'єктів критичної інфраструктури, що дозволить чітко визначити всі об'єкти критичної інфраструктури. Дія проєкту Постанови буде стосуватися тільки великих та середніх суб'єктів господарювання та не стосуватиметься фізичних осіб;

розмір коштів і час, що витрачатимуться суб'єктами господарювання та/або фізичними особами, пов'язаними з виконанням вимог акта, – додаткових витрат та часу від суб'єктів господарювання, пов'язаними з виконанням вимог акта, не передбачається;

рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта – проєкт акта розміщено на вебсайті Держспецзв'язку (електронна адреса: www.dsszzi.gov.ua) у підрозділі «Повідомлення про оприлюднення та проєкти» розділу «Регуляторна діяльність»;

кількість об'єктів критичної інфраструктури;

кількість сформованих галузевих переліків об'єктів критичної інфраструктури;

кількість вжитих 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 акта з метою внесення до нього змін.

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

Повторне відстеження результативності регуляторного акта буде здійснюватися не пізніше двох років з дня набрання ним чинності шляхом аналізу статистичних даних.

Періодичні відстеження результативності регуляторного акта будуть здійснюватися 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 Валентин ПЕТРОВ

«22» 11 2019 року

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2019 р. №

Київ

Про затвердження 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**:

Затвердити такі, що додаються:

Порядок віднесення об'єктів до об'єктів критичної інфраструктури;

Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави;

Методику категоризації об'єктів критичної інфраструктури.

Прем'єр-міністр України **О. ГОНЧАРУК**

Валентин ПЕТРОВ

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 201_ р. № _____

ПОРЯДОК
віднесення об'єктів до об'єктів критичної інфраструктури

1. Цей Порядок визначає критерії і механізм віднесення об'єктів до об'єктів критичної інфраструктури та їх категоризації.

2. У цьому документі терміни вживаються у такому значенні:

безпека об'єкта критичної інфраструктури – стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи, а також можливість надання ним основних послуг;

власник та/або керівник об'єкта критичної інфраструктури (далі – оператор основних послуг) – державний орган, підприємство, установа, організація, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належать об'єкти критичної інфраструктури та який/яка відповідає за їх поточне функціонування;

життєво важливі послуги та функції (далі – основні послуги) – послуги та функції, які надаються органами державної влади, установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України;

захист об'єктів критичної інфраструктури – організаційні, нормативно-правові, інженерно-технічні та інші заходи, спрямовані на забезпечення безпеки об'єктів критичної інфраструктури;

ідентифікація об'єкта критичної інфраструктури – процедура віднесення об'єкта інфраструктури до об'єктів критичної інфраструктури;

категоризація об'єктів критичної інфраструктури – процедура віднесення об'єктів критичної інфраструктури до певної категорії критичності;

категорія критичності об'єкта критичної інфраструктури – відносна міра важливості об'єкта критичної інфраструктури, класифікована залежно від ступеня його впливу на надання основних послуг;

кризова ситуація – порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів;

критична інфраструктура – сукупність об'єктів критичної інфраструктури;

сектор (підсектор) критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до одного сектору (підсектору) економіки та/або мають спільну функціональну спрямованість;

уповноважений орган державної влади відповідальний за сектор (підсектор) критичної інфраструктури (далі – уповноважений орган) – центральний орган виконавчої влади, інший державний орган, який забезпечує формування та/або реалізацію державної політики в одній чи декількох сферах;

час відновлення – час, що необхідний для відновлення функціонування об'єкта критичної інфраструктури у штатному режимі після усунення загрози.

Інші терміни вживаються у значенні, наведеному в Законі України «Про основні засади забезпечення кібербезпеки України».

3. Встановлюються такі категорії критичності об'єктів критичної інфраструктури:

I категорія критичності – критично важливі об'єкти, які мають загальнодержавне значення, значний вплив на інші об'єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації національного значення;

II категорія критичності – життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

III категорія критичності – важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

IV категорія критичності – необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

4. Відповідальність за безпеку об'єкта критичної інфраструктури несуть оператори основних послуг.

5. Уповноважені органи, використовуючи Перелік секторів (підсекторів), основних послуг критичної інфраструктури, ідентифікують об'єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури.

6. Уповноважені органи спільно з операторами основних послуг здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до Методики категоризації об'єктів критичної інфраструктури.

7. Об'єкти критичної інфраструктури, що віднесені до I, II III та IV категорій критичності, вносяться уповноваженими органами до секторальних переліків об'єктів критичної інфраструктури, які ними формуються та ведуться.

8. Уповноважені органи складають зведені переліки всіх об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури, що віднесені до I та II категорій критичності, та надають їх до уповноваженого органу з питань захисту критичної інфраструктури для формування Національного переліку об'єктів критичної інфраструктури.

Уповноважені органи подають оновлені відомості щодо об'єктів критичної інфраструктури свого сектору (підсектору) критичної інфраструктури до Національного переліку об'єктів критичної інфраструктури кожні два роки та невідкладно у разі:

зміни власника або назви об'єкта критичної інфраструктури;

зміни категорії об'єкта критичної інфраструктури;

ліквідації об'єкта критичної інфраструктури.

9. Відомості щодо об'єктів критичної інфраструктури, що містяться у Національному переліку об'єктів критичної інфраструктури та секторальних переліках об'єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства у сфері захисту інформації та охорони державної таємниці.

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 201_ р. № _____

ік секторів (підсекторів), основних послуг критичної інфраструктури

Сектор	Підсектор	Тип основної послуги
Паливно-енергетичний сектор	Електроенергетика	Виробництво електроенергії
		Забезпечення функціонування ринку електроенергії, організація купівлі-продажу електроенергії на ринку
		Управління системами передачі та енергопостачання
		Розподіл електроенергії
	Нафта та нафтопродукти	Видобуток нафти
		Передача (транзит) нафти та нафтопродуктів
		Очищення, переробка та обробка нафти
		Експлуатація нафтопроводів
		Зберігання та постачання нафти та нафтопродуктів
	Газ	Видобуток газу

				Переробка та очищення газу
				Передача (транзит) газу
				Розподіл газу
				Експлуатація газотранспортної системи
				Зберігання природного газу
				Забезпечення роботи систем зрідження природного газу
			Ядерна енергетика	Виробництво електроенергії на атомних стаціях
				Експлуатація атомних станцій
				Переробка та зберігання ядерного палива
2	Міністерство цифрової трансформації України	Інформаційний сектор	Інформаційні технології	Зберігання та обробка даних у центрах обробки даних та/або хмарних сховищах
				Забезпечення функціонування систем електронного урядування
				Хмарні обчислення
				Електронні довірчі послуги
				Забезпечення функціонування схем електронної ідентифікації
			Телекомунікації	Поширення телевізійного (у тому числі цифрового) та радіосигналів
				Забезпечення функціонування точок обміну трафіком (IXP)

				Підтримка системи доменних імен (DNS) в Інтернеті
3	Міністерство розвитку громад та територій України	Мережі життєзабезпечення	Питна вода	Виробництво, транспортування, та/або постачання питної води
				Експлуатація систем централізованого водопостачання
			Стічні води	Збір та очищення стічних вод
				Експлуатація систем централізованого водовідведення
			Теплопостачання	Виробництво теплової енергії
				Експлуатація систем централізованого теплопостачання
4	Міністерство розвитку економіки, торгівлі та сільського господарства України	Харчова промисловість та агропромисловий комплекс		Виробництво та переробка сільськогосподарської та/або харчової продукції
				Експлуатація великих зрошувальних систем, каналів
				Забезпечення зберігання стратегічних державних запасів та резервів
5	Міністерство охорони здоров'я України	Охорона здоров'я		Надання екстреної медичної допомоги
				Надання послуг стаціонарного та амбулаторного лікування та інших медичних послуг
				Виробництво, закупівля та постачання, фармацевтичних препаратів, ліків, вакцин, крові та інших медикаментів і медичного обладнання

				Надання послуг eHealth
				Контроль за інфекційними захворюваннями та/або епідеміями
6	Національна комісія з цінних паперів та фондового ринку	Фінансовий сектор		Забезпечення функціонування фондових бірж та фондового ринку
7	Міністерство інфраструктури України	Транспорт і пошта	Повітряний транспорт	Управління повітряним рухом
				Авіаперевезення (робота повітряного транспорту)
				Забезпечення роботи аеропортів та допоміжного обладнання, що знаходиться в аеропортах
			Автомобільний транспорт	Автобусні перевезення (міжміські, міжнародні)
				Міські перевезення (автобуси, трамваї, тролейбуси, метро)
				Технічне обслуговування транспортної інфраструктури (доріг, мостів, тунелів, шляхопроводів)
				Служби контролю трафіку
				Функціонування інтелектуальних транспортних систем (управління рухом, мобільністю, взаємодія з іншими видами транспорту)
			Залізничний транспорт	Пасажирські залізничні перевезення
				Вантажні залізничні перевезення

				Експлуатація та технічне обслуговування залізниці
				Забезпечення роботи вокзалів та вузлових станцій
			Морський та річний транспорт	Контроль і управління судноплавством
				Операції на внутрішньому, морському або прибережному пасажирському та вантажному транспорті
				Функціонування керуючих органів портів або суб'єктів експлуатації портового обладнання
				Експлуатація та обслуговування інфраструктури (каналів, дамб, фарватерів тощо)
			Пошта	Поштовий зв'язок
8	Міністерство розвитку економіки, торгівлі та сільського господарства України	Промисловість	Хімічна та атомна промисловість	Виробництво промислового газу
				Виробництво добрив або азотистих сполук
				Виробництво пестицидів або інших агрохімічних продуктів
				Виробництво вибухових речовин
				Виробництво основних органічних хімічних речовин
				Виробництво основних неорганічних речовин

			Оборонна промисловість	Виробництво та постачання озброєнь та військової техніки (військово-промисловий комплекс)
				Постачання (продаж) та закупівля озброєнь та військової техніки за міжнародними контрактами
			Ракетно-космічна та авіаційна промисловість	Виробництво та постачання продукції ракетно-космічної та авіаційної промисловості
9	Міністерство внутрішніх справ України	Цивільний захист населення та територій		Служба телефону екстреної допомоги
				Аварійне і екстрене оповіщення населення, ліквідація і аварійне відновлення, організація і координація порятунку жителів і майна
10	Міністерство енергетики та захисту довкілля України	Екологічна безпека		Моніторинг забруднення повітря та раннє попередження
				Метеорологічне спостереження та раннє попередження
				Моніторинг поверхневих вод (річок, озер) та раннє попередження
				Моніторинг та контроль забруднення морського середовища

Валентин ПЕТРОВ

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 201_ р. № _____

МЕТОДИКА

категоризації об'єктів критичної інфраструктури

1. Ця Методика визначає механізм віднесення об'єкта критичної інфраструктури до однієї з категорій критичності.

2. У цьому документі терміни вживаються у такому значенні:

безпека об'єкта критичної інфраструктури – стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи, а також можливість надання ним основних послуг;

власник та/або керівник об'єкта критичної інфраструктури (далі – оператор основних послуг) – державний орган, підприємство, установа, організація, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належать об'єкти критичної інфраструктури та який/яка відповідає за їх поточне функціонування;

життєво важливі послуги та функції (далі – основні послуги) – послуги та функції, які надаються органами державної влади, установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України;

захист об'єктів критичної інфраструктури – організаційні, нормативно-правові, інженерно-технічні та інші заходи, спрямовані на забезпечення безпеки об'єктів критичної інфраструктури;

ідентифікація об'єкта критичної інфраструктури – процедура віднесення об'єкта інфраструктури до об'єктів критичної інфраструктури;

категоризація об'єктів критичної інфраструктури – процедура віднесення об'єктів критичної інфраструктури до певної категорії критичності;

категорія критичності об'єкта критичної інфраструктури – відносна міра важливості об'єкта критичної інфраструктури, класифікована в залежності від ступеня його впливу на надання основних послуг;

кризова ситуація – порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів;

критична інфраструктура – сукупність об'єктів критичної інфраструктури;

сектор (підсектор) критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до одного сектору (підсектору) економіки та/або мають спільну функціональну спрямованість;

уповноважений орган державної влади, відповідальний за сектор (підсектор) критичної інфраструктури (далі – уповноважений орган), – центральний орган виконавчої влади, інший державний орган, який забезпечує формування та/або реалізацію державної політики в одній чи декількох сферах;

час відновлення – час, необхідний для відновлення функціонування об'єкта критичної інфраструктури у штатному режимі після усунення загрози.

Інші терміни вживаються у значенні, наведеному в Законі України «Про основні засади забезпечення кібербезпеки України».

3. Категорія критичності об'єкта критичної інфраструктури визначається на основі аналізу рівня негативного впливу, яку особа, суспільство, навколишнє середовище, економіка, національна безпека та обороноздатність країни можуть зазнати внаслідок порушення або припинення функціонування об'єкта інфраструктури відповідно до критеріїв, зазначених у додатках 1 та 2 до цієї Методики.

4. Категорія об'єкта критичної інфраструктури визначається за такою процедурою.

4.1. Уповноважений орган ідентифікує всі об'єкти критичної інфраструктури свого сектору (підсектору) критичної інфраструктури згідно з Порядком віднесення об'єктів до об'єктів критичної інфраструктури.

4.2. Уповноважений орган відповідно до Порядку віднесення об'єктів до об'єктів критичної інфраструктури для кожного об'єкта свого сектору (підсектору) критичної інфраструктури визначає, які основні послуги надає цей об'єкт.

4.3. Уповноважений орган разом з оператором критичної інфраструктури проводить оцінку критичності об'єкта критичної інфраструктури з використанням секторальних та міжсекторальних критеріїв визначення рівня негативного впливу, наведених у додатках 1 та 2 до цієї Методики, та з урахуванням:

рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури;

соціальної значущості об'єкта критичної інфраструктури;

політичної значущості об'єкта інфраструктури;

економічної значущості об'єкта;

наявності взаємозв'язків між об'єктам критичної інфраструктури;

значущості для забезпечення національної безпеки та обороноздатності країни.

4.3.1. Під час заповнення форми додатка 1 до цієї методики обирається рівень негативного впливу в рамках сектору або підсектору об'єкта критичної інфраструктури та у графі «Оцінка $РК_i$» виставляється бал, який відповідає

рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об'єкта критичної інфраструктури.

4.3.2. Під час заповнення форми додатка 2 до цієї методики обирається рівень негативного впливу за кожним критерієм, наведеним у формі, та у графі «Оцінка $РК_і$» виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об'єкта критичної інфраструктури.

4.3.3. Підсумовуються всі бали, що були отримані під час оцінки об'єкта критичної інфраструктури згідно з формами, наведеними в додатках 1 та 2 до цієї Методики.

4.3.4. Розраховується узагальнена нормована оцінка рівня критичності за формулою:

$$РК_{ОКІ} = \frac{\Sigma РК_і}{\Sigma РК_{max}},$$

де:

$РК_{ОКІ}$ – узагальнена нормована оцінка рівня критичності об'єкта критичної інфраструктури;

$\Sigma РК_і$– сума балів, які отримав об'єкт критичної інфраструктури за всіма критеріями критичності (додатки 1 та 2 до цієї методики);

$\Sigma РК_{max}$ – максимальна можлива сума балів (розраховується виходячи з того, що об'єкт отримує максимальні бали за всіма критеріями оцінки рівня негативного впливу).

Примітка: у цьому документі залежно від сектору використовується 19 або 20 критеріїв. Тому для ОКІ, що належать до секторів критичної інфраструктури за пунктами 1, 3 - 7 додатка 1, максимальна можлива сума балів буде дорівнювати $\Sigma РК_{max}$ *= 20*4=80 балів, для ОКІ, що належать до секторів за пунктами 2, 8 - 14 додатка 1, максимальна можлива сума балів буде дорівнювати* $\Sigma РК_{max}$ *= 19*4=76 балів.*

4.3.5. Рішення щодо категорії критичності об'єкта критичної інфраструктури приймається на основі узагальненої нормованої оцінки рівня критичності об'єкта критичної інфраструктури відповідно до такого правила:

I категорія критичності, якщо $0{,}8 < РК_{ОКІ} \leq 1$;
II категорія критичності, якщо $0{,}63 < РК_{ОКІ} \leq 0{,}8$;
III категорія критичності, якщо $0{,}37 < РК_{ОКІ} \leq 0{,}63$;
IV категорія критичності, якщо $0{,}2 < РК_{ОКІ} \leq 0{,}37$;
об'єкт не є критичним, якщо $РК_{ОКІ} \leq 0{,}2$.

4.4. Відомості про об'єкти критичної інфраструктури, що віднесені до об'єктів I та II категорій критичності, уповноважений орган надає до уповноваженого органу у сфері захисту критичної інфраструктури для формування Національного переліку об'єктів критичної інфраструктури.

4.5. Відомості про об'єкти критичної інфраструктури, що віднесені до об'єктів III та IV категорій критичності вносяться до секторального переліку об'єктів критичної інфраструктури, який веде уповноважений орган у відповідному секторі (підсекторі).

4.6. Приклад категоризації об’єкта критичної інфраструктури наведено у додатку 3 до цієї Методики.

Валентин ПЕТРОВ

Додаток 1
до Методики категоризації
об'єктів критичної інфраструктури

Форма визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (секторальні критерії)

№ З/п	Сектор/підсектор	Фактор негативного впливу в секторі/підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бал)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка PK_i
1.	Послуги, що надаються підсектором електроенергетики та підсектором ядерної енергетики	у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури припиниться електропостачання	для більш ніж 145 000 жителів АБО для споживачів першої категорії на території більш ніж однієї області АБО на території не менш ніж 3 міст обласного значення	для більш ніж 30 000 жителів АБО для споживачів другої категорії на території однієї області АБО на території більш одного району міста обласного центру АБО вся територія одного міста обласного значення	для більш ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може складати від 6 до 24 годин	час відновлення функціонування у штатному режимі може складати від однієї до 3 діб	час відновлення функціонування у штатному режимі може бути більше трьох діб	

2.	Послуги, що надаються підсектором нафти та нафтопродуктів	у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури зменшиться постачання нафти та нафтопродуктів для споживання на внутрішньому ринку України	більш ніж на 25% відносно аналогічного періоду календарного року чи попереднього календарного місяця у межах граничного обсягу визначеного центральним органом виконавчої влади, що реалізує політику у сфері державного матеріального резерву (ЦОМР)	від 12 до 25% відносно аналогічного періоду календарного року чи попереднього календарного місяця у межах граничного обсягу визначеного ЦОМР	від 7 до 12% відносно аналогічного періоду календарного року чи попереднього календарного місяця у межах граничного обсягу визначеного ЦОМР	менш ніж на 7% відносно аналогічного періоду календарного року чи попереднього календарного місяця у межах граничного обсягу визначеного ЦОМР	
3.	Послуги, що надаються підсектором постачання газу	у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури припиниться постачання газу	для більш ніж 145 000 жителів АБО для споживачів з безперервною подачею газу на території більш ніж однієї області АБО на території не менш ніж 3 міст обласного значення	для більш ніж 20 000 жителів на території однієї області АБО на території більш одного району міста-обласного центру АБО на всій території одного міста обласного значення	для більш ніж 5000 жителів	для менше ніж 5000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може складати від 6 до 24 годин	час відновлення функціонування у штатному режимі від однієї до 3 діб.	час відновлення функціонування у штатному режимі може бути більше трьох діб	

4.	Послуги, що надаються інформаційним сектором	у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури припиниться або порушиться надання основних послуг об'єктом	для більш ніж 145 000 жителів на території більш ніж однієї області АБО на території не менш ніж 3 міст обласного значення	для більш ніж 20 000 жителів на території однієї області АБО на території більш одного району міста-обласного центру АБО на всій території одного міста обласного значення	для більш ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може складати від 6 до 24 годин	час відновлення функціонування у штатному режимі від однієї до 3 діб.	час відновлення функціонування у штатному режимі може бути більше трьох діб	
5.	Послуги, що надаються підсектором центрального опалення (теплопостачання)	у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури теплопостачання буде перервано (під час опалювального сезону)	для більш ніж 145 000 жителів АБО споживачів безперервного теплопостачання на території більш ніж однієї області АБО не менш ніж 3 міст обласного значення	для більш ніж 30000 жителів АБО на території більш одного району міста-обласного центру АБО на всій території одного міста обласного значення	для більш ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 24 годин	час відновлення функціонування у штатному режимі може складати від доби до трьох діб	час відновлення функціонування у штатному режимі від трьох діб.	не застосовується	

6.	Послуги, що надаються підсектором питної води	у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури буде припинено постачання питної води	для більш ніж 145 000 жителів на території більш ніж однієї області АБО не менш ніж 3 міст обласного значення	для більш ніж 30000 жителів АБО стаціонарним лікувальним закладам, домам соціальної допомоги, установам, що надають послуги освіти на території області АБО більш одного району міста-обласного центру АБО вся територія одного міста обласного значення	для більш ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 24 годин (час кризової ситуації не може перевищувати 24 годин)	час відновлення функціонування у штатному режимі може складати від доби до трьох діб (час кризової ситуації може складати від доби до трьох діб)	час відновлення функціонування у штатному режимі від трьох діб (час кризової ситуації може складати більше трьох діб).	не застосовується	

7.	Послуги, що надаються підсектором стічних вод	у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури буде припинено централізоване водовідведення та очищення стічних вод	для більш ніж 145 000 жителів на території обласного центру АБО не менш ніж 3 міст обласного значення	для більш ніж 30 000 жителів на території одного міського району обласного центру АБО всій території одного міста обласного значення	для більш ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 24 годин (час кризової ситуації не може перевищувати 24 годин)	час відновлення функціонування у штатному режимі може складати від доби до трьох діб (час кризової ситуації може складати від доби до трьох діб)	час відновлення функціонування у штатному режимі від трьох діб. (час кризової ситуації може складати від доби до трьох діб)	не застосовується	
8.	Послуги, що надаються підсектором повітряного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до	неможливості надання послуг по перевезенню пасажирів та вантажів по повітрю хоча б одним зі стратегічно важливих аеропортів* України на протязі більш ніж 24 годин без можливості організації альтернативного способу надання послуг. ** до стратегічних аеропортів належать аеропорти "Бориспіль",*	неможливості надання послуг по перевезенню пасажирів та вантажів по повітрю хоча б одним зі стратегічно важливих аеропортів* України на протязі більш ніж 24 годин при цьому зберігається можливість організації	припинення повітряного руху на час відновлення штатного режиму функціонування.	не застосовується	

			"Жуляни", "Одеса", "Львів", "Дніпропетровськ", "Харків", "Запоріжжя"	альтернативного способу надання послуги			
9.	Послуги, що надаються підсектором автомобільного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до	блокування (припинення) дорожнього руху на міжнародних ТА національних дорогах на протязі більше ніж на 24 годин ТА якщо немає обхідного шляху АБО немає можливості його відновлення на протязі не більше ніж 24 години	блокування (припинення) дорожнього руху на міжнародних ТА національних дорогах на протязі не більше ніж на 24 годин ТА якщо немає обхідного шляху	блокування (припинення) дорожнього руху на регіональних дорогах на протязі не більше ніж на 48 годин ТА якщо немає обхідного шляху АБО немає можливості його відновлення на протязі не більше ніж 48 години	блокування (припинення) дорожнього руху на регіональних дорогах на протязі не більше ніж на 48 годин ТА якщо немає обхідного шляху	
10.	Послуги, що надаються підсектором залізничного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до	припинення залізничного руху більш ніж на 24 години на залізничних магістральних лініях I (I-П, I-ПС) та II категорий* *(Категорію залізничної лінії визначено відповідно до ДБН В.2.3-19-2018)*	припинення залізничного руху більш ніж на 24 години на залізничних магістральних лініях III категорії	припинення залізничного руху більш ніж на 24 години на залізничних магістральних лініях IV категорії	припинення залізничного руху більш ніж на 24 години на залізничних магістральних лініях V категорії	

11.	Послуги, що надаються підсектором морського та річного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до	припинення надання морських послуг у морських портах більше ніж на 72 години *(Правила надання послуг у морських портах України. Наказ Міністерства інфраструктури України від 05.06.2013 № 348)*	припинення надання морських послуг у морських портах від 24 до 72 годин	припинення надання морських послуг у морських портах буде перервано до 24 годин	не застосовується	
12.	Послуги, що надаються поштовим підсектором	у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури буде припинено надання послуг поштового зв'язку	для більш ніж 145 000 жителів на території більш ніж однієї області АБО більше ніж 3 міст обласного значення	для більш ніж 20 000 жителів на території області АБО більш одного району міста-обласного центру АБО на всій території одного міста обласного значення	для більш ніж 6000 жителів	для менше ніж 6000 жителів	
13.	Послуги, що надаються сектором харчової промисловості та агропромислового комплексу, сектором охорони здоров'я, фінансовим сектором, сектором промисловості,	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до не надання об'єктом основних послуг	для більш ніж 145 000 жителів на території більш ніж однієї області АБО не менш ніж 3 міст обласного значення	для більш ніж 30 000 жителів на території області АБО більш одного району міста-обласного центру АБО на всій території одного міста обласного значення	для більш ніж 6000 жителів	для менше ніж 6000 жителів	

	сектором цивільного захисту населення та територій, сектором екологічної безпеки						
Сумарна оцінка ΣPK_i							

Валентин ПЕТРОВ

Додаток 2
до Методики категоризації
об'єктів критичної інфраструктури

Форма визначення рівня негативного впливу у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (міжсекторальні критерії)

№ з/п	Негативний вплив	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бал)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу пренебрежимо малий (0 балів)	Оцінка PK_i
I. Соціальна значущість об'єкта інфраструктури							
1.	Заподіяння шкоди життю та здоров'ю людей	Кількість населення, що може постраждати					
		Небезпека для життя або здоров'я 75 000 людей	Небезпека для життя та здоров'я більш ніж 5000 людей	Небезпека для життя або здоров'я більш ніж 50 людей	Небезпека для життя або здоров'я менше ніж 50 людей	Не критично	PK_1=
		Географічний масштаб					

		Небезпека для життя та здоров'я мешканців на території однієї або більш ніж однієї області АБО на території 3 та більше міст обласного значення	Небезпека для життя та здоров'я мешканців на території однієї області АБО міського району міста обласного центру АБО на всій території одного міста обласного значення	Небезпека для життя та здоров'я для людей на території об'єкта та для мешканців, що проживають у безпосередній близькості до розміщення об'єкта	Небезпека для життя та здоров'я людей на території об'єкта	Не критично	PK_2=
2.	Рівень панічних настроїв населення	Дуже великий рівень панічних настроїв: панічні настрої розповсюджуються на території більш ніж одна область АБО не менш ніж 3 міст обласного значення	Великий рівень панічних настроїв: панічні настрої розповсюджуються на території однієї області АБО одного міста обласного значення	Панічні настрої розповсюджуються на частині території міста обласного значення	Панічні настрої роз-повсюджуються на території об'єкта	Не критично	PK_3=
3.	Заподіяння шкоди навколишньому середовищу	Економічні втрати					
		Нанесені збитки більш ніж 30 млн грн	Нанесені збитки більш ніж 18 млн грн	Нанесені збитки більш ніж 2 млн грн	Нанесені збитки менше ніж на 2 млн грн	Не критично	PK_4=
		Географічний масштаб					

		Шкідливий вплив розповсюджується на територію більш ніж одна область АБО на території не менш ніж 3 міст обласного значення	Шкідливий вплив розповсюджується на територію однієї області АБО на територію більш ніж одного міста обласного значення	Шкідливий вплив розповсюджується на територію одного міста обласного значення	Шкідливий вплив роз-повсюджується на територію об'єкта інфраструктури	Не критично	$PK_5=$
		Час					
		Шкідливий вплив на навколишнє середовище та безпечні умови життя зберігається протягом більш ніж один рік	Шкідливий вплив на навколишнє середовище та безпечні умови життя зберігається протягом від півроку до одного року	Шкідливий вплив на навколишнє середовище та безпечні умови життя зберігається протягом від одного місяця до півроку	Шкідливий вплив на навколишнє середовище та безпечні умови життя зберігається протягом до одного місяця	Не критично	$PK_6=$
II. Політична значущість об'єкта інфраструктури							

4.	Припинення або порушення функціонування державних органів влади	Припинення або порушення функціонування Адміністрації Президента України, Верховної Ради України, Кабінету Міністрів України, Ради безпеки та оборони України, Конституційного Суду України, Верховного Суду України	Припинення або порушення функціонування центральних органів виконавчої влади та обласних державних адміністрацій	Припинення або порушення роботи місцевих державних адміністрацій, органів державного управління в адміністративно-територіальних одиницях України	Припинення або порушення роботи місцевих органів влади.	Не критично	$РК_7=$
5.	Негативний вплив на довіру людей до державних інституцій	Матиме значний вплив	Матиме великий вплив	Матиме середній вплив	Матиме незначний вплив	Не критично	$РК_8=$
6.	Шкода інтересам іншим державам-партнерам України	Так, принаймні двом країнам або порушення умов міждержавного договору	Так, принаймні однієї країні або порушення умов міжурядового договору	Можливі негативні наслідки для інших держав, але їх вплив навряд чи буде значним	Держави не постраждають або не має місце порушенню умов міжвідомчого договору	Не критично	$РК_9=$

7.	Рівень протестних настроїв	Дуже високий рівень протестних настроїв: ризик протестів з блокуванням роботи Адміністрації Президента України, Верховної Ради України, Кабінету Міністрів України, Ради безпеки та оборони України, Конституційного Суду України, Верховного Суду України.	Високий рівень протестних настроїв: ризик протестів з блокуванням центральних органів виконавчої влади та обласних державних адміністрацій	Середній рівень протестних настроїв ризик блокування роботи місцевих органів влади, об'єктів критичної інфраструктури	Незначний рівень протестних настроїв: блокування роботи об'єкта критичної інфраструктури	Не критично	PK_{10}=
III. Економічна значущість об'єкта інфраструктури							
8.	Заподіяння збитків об'єкту інфраструктури (у відсотках прогнозованого обсягу річного доходу за всіма видами діяльності)	Більш ніж 15%	Від 10 до 15%	Від 5 до 10%	Менш ніж 5%	Не критично	PK_{11}=
9.	Заподіяння збитків державному бюджету України (зниження прибутків бюджету у відсотках прогнозованого річного прибутку	Більш ніж 0,1%	Від 0,1% до 0,05%	Від 0,05% до 0,01%	Менш ніж 0,01%	Не критично	PK_{12}=

	бюджету)						
10.	Заподіяння збитків місцевим бюджетам (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	Більш ніж 0,1%	Від 0,1% до 0,05%	Від 0,05% до 0,01%	Менш ніж 0,01%	Не критично	$PK_{13}=$
IV. Взаємозв'язок між об'єктами критичної інфраструктури							
11.	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує такі ж основні послуги	Матиме негативний вплив (якщо так, вкажіть який)			Не матиме впливу	Не критично	$PK_{14}=$
12.	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що надає інші основні послуги	Матиме негативний вплив (якщо так, вкажіть який)			Не матиме впливу	Не критично	$PK_{15}=$
V. Значущість для забезпечення національної безпеки та обороноздатності країни							

13.	Припинення або порушення (невиконання встановлених показників) функціонування пунктів управління (ситуаційного центру), що оцінюється в рівні (значущості) пункту управління або ситуаційного центру	Припинення або порушення функціонування пунктів управління Верховного головнокомандувача ЗСУ, Головнокомандувача ЗСУ- начальника Генерального штабу або ситуаційного центру Адміністрації Президента України, Кабінету Міністрів України, Ради безпеки та оборони України	Припинення або порушення функціонування пунктів управління або ситуаційного центру органів центральної виконавчої влади, пунктів управління Сухопутних військ, Повітряних Сил, військово-морських Сил, десантно-штурмових військ, сил спеціальних операцій, Національної гвардії України, Державної прикордонної служби	Припинення або порушення функціонування обласної державної адміністрації, ситуаційних центрів органів державної влади на місцях		Не критично	$РК_{16}$=
14.	Зниження показників державного оборонного замовлення	Зниження обсягів продукції (робіт, послуг) в заданий період часу (у відсотках)					
		Більше ніж 15%	Від 10 до 15%	Від 5 до 10%	Менше ніж 5%.	Не критично	$РК_{17}$=
		Збільшення часу виготовлення продукції (робіт, послуг) із заданим обсягом (відсотків встановленого часу на виготовлення продукції)					
		Більше ніж 40%	Від 10% до 40%	Від 5% до 10%	Менше ніж 5%	Не критично	$РК_{18}$=
Сумарна оцінка $\Sigma РК_i$							

Валентин ПЕТРОВ

Додаток 3
до Методики категоризації
об'єктів критичної інфраструктури

Приклад категоризації об'єкта критичної інфраструктури

1. Розглянемо порядок категоризації об'єкта критичної інфраструктури на прикладі кваліфікованого надавача електронних довірчих послуг (далі – КНЕДП). Власник (оператор) – державне підприємство «ЗЕТ».

2. КНЕДП належить до об'єкта, який надає послуги з надання кваліфікованих електронних довірчих послуг формування, перевірки та підтвердження чинності:

кваліфікованого сертифіката електронного підпису чи печатки;

кваліфікованої електронної позначки часу.

3. Далі в таблиці 1 знаходимо основну послугу «Електронні довірчі послуги», яка відповідає підсектору інформаційні технології інформаційного сектору. Уповноважений орган – Міністерство цифрової трансформації України.

4. Далі здійснюється визначення рівня негативного впливу об'єкта критичної інфраструктури за секторальним критерієм (додаток 1 до Методики віднесення об'єкта критичної інфраструктури до однієї з категорій критичності). Згідно з додатком 1 КНЕДП буде оцінюватися за критерієм п. 4 цього додатка. У разі інциденту в КНЕДП надання електронних довірчих послуг буде припинено для всіх клієнтів центру (більше ніж 900 000). Тому за секторальним критерієм КНЕДП отримує 4 бали.

Далі наведено приклад заповнення додатка 1 до Методики віднесення об'єкта критичної інфраструктури до однієї з категорій критичності.

Приклад заповнення додатка 1 до Методики віднесення об'єкта критичної інфраструктури до однієї з категорій критичності

№	Сектор/підсектор	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бал)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка PK_i
4.	Послуги, що надаються інформаційним сектором: у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури припиниться або порушиться надання основних послуг об'єктом	**для більш ніж 145 000 жителів на території більш ніж однієї області АБО на території не менш ніж 3 міст обласного значення**	для більш ніж 20 000 жителів на території однієї області АБО на території більш одного району міста-обласного центру АБО на всій території одного міста обласного значення	для більш ніж 2000 жителів	для менше ніж 2000 жителів	**4**
		час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може складати від 6 до 24 годин	час відновлення функціонування у штатному режимі від однієї до 3 діб.	час відновлення функціонування у штатному режимі може бути більше трьох діб	**4**
				Сумарна оцінка ΣPK_i		**8**

5. Далі проводиться оцінка за міжсекторальними критеріями (додаток 2 Методики). Приклад оцінки наведено у таблиці додатка 2. Оцінка проводиться шляхом вибору варіанта негативного впливу за кожним критерієм та обґрунтування вибору.

5.1. Соціальна значущість об'єкта інфраструктури

У разі припинення надання послуг КНЕДП прямої небезпеки для життя та здоров'я людей не існує, тому PK_1=0. Також за географічним критерієм небезпеки для життя та здоров'я людей не існує PK_2=0. У разі припинення надання послуги КНЕДП буде припинено надання послуг його клієнтам. Припинення надання таких послуг у фінансовому секторі, секторах обробки податкових декларацій, здійснення електронної ідентифікації громадян за електронними паспортами, технологіями MobileID тощо може призвести до розповсюдження панічних настроїв на великі території. Тому PK_3=4. Заподіяння шкоди навколишньому середовищу не має місця. Тому PK_4=0, PK_5=0 та PK_6=0.

5.2. Політична значущість об'єкта інфраструктури

КНЕДП є великим надавачем в інфраструктурі надання електронних довірчих послуг. У разі припинення його функціонування може бути припинено виконання основних послуг та порушено роботу центральних органів влади (у разі реалізації у повному обсязі електронного документообігу, електронного судочинства тощо). Тому PK_7=4. Також здійснюється значний вплив на довіру населення до державних інституцій, як наслідок - невиконання ними відповідних функцій. Тому PK_8=4. На цей час шкода іншим країнам не може бути нанесена, але можуть бути порушення міжурядових угод - PK_9=3. Рівень протестних настроїв буде незначний, PK_{10}=1.

5.3. Економічна значущість об'єкта інфраструктури

Припинення надання послуг КНЕДП призведе до заподіяння збитків об'єкта критичної інфраструктури (тобто державного підприємства) на 23% (згідно зі звітністю за останні роки). Збитки бюджету країни на цей час незначні (поширення довірчих послуг недостатнє). Збитки місцевим бюджетам також незначні (також через недостатню поширеність послуг). Тому PK_{11}=4, PK_{12}=1, PK_{13}=1.

5.4. Взаємозв'язок між об'єктами критичної інфраструктури

Переривання надання послуг КНЕДП не вплине на роботу інших надавачів електронних довірчих послуг. Водночас переривання надання послуг КНЕДП призведе до порушень надання послуг в інших секторах, де діяльність пов'язана з використанням електронного підпису та довірчих послуг (наприклад, фінансовий сектор). Тому PK_{14}=0, PK_{15}=4.

5.5 Значущість для забезпечення обороноздатності країни та безпеки держави

Припинення роботи КНЕДП не вплине на функціонування пунктів управління (ситуаційних центрів). Тому PK_{16}=0. Зниження показників державного оборонного замовлення не очікується. Тому PK_{17}=0, PK_{18}=0.

Далі наведено приклад заповнення додатка 2 до Методики віднесення об'єкта критичної інфраструктури до однієї з категорій критичності.

Приклад заповнення додатка 2 до Методики віднесення об'єкта критичної інфраструктури до однієї з категорій критичності

№ З/п	Негативний вплив	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бал)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу пренебрежимо малий (0 балів)	Оцінка PK_i
I. Соціальна значущість об'єкта інфраструктури							
1.	Заподіяння шкоди життю та здоров'ю людей	Кількість населення, що може постраждати					
		Небезпека для життя або здоров'я 75 000 людей	Небезпека для життя та здоров'я більш ніж 5000 людей	Небезпека для життя або здоров'я більш ніж 50 людей	Небезпека для життя або здоров'я менше ніж 50 людей	**Не критично**	PK_1=0
		Географічний масштаб					
		Небезпека для життя та здоров'я мешканців на території однієї або більш ніж однієї області АБО на території 3 та більше міст обласного значення	Небезпека для життя та здоров'я мешканців на території однієї області АБО міського району міста обласного центру АБО на всій території одного міста обласного значення	Небезпека для життя та здоров'я для людей на території об'єкта та для мешканців, що проживають у безпосередній близькості до розміщення об'єкта	Небезпека для життя та здоров'я людей на території об'єкта	**Не критично**	PK_2=0

2.	Рівень панічних настроїв населення	**Дуже великий рівень панічних настроїв: панічні настрої розповсюджуються на території більш ніж одна область АБО не менш ніж 3 міст обласного значення**	Великий рівень панічних настроїв: панічні настрої розповсюджуються на території однієї області АБО одного міста обласного значення	Панічні настрої розповсюджуються на частині території міста обласного значення	Панічні настрої роз-повсюджуються на території об'єкта	Не критично	PK_3=4
3.	Заподіяння шкоди навколишньому середовищу	Економічні втрати					
		Нанесені збитки більш ніж 30 млн грн	Нанесені збитки більш ніж на 18 млн грн	Нанесені збитки більш ніж на 2 млн грн	Нанесені збитки менше ніж на 2 млн грн	**Не критично**	PK_4=0
		Географічний масштаб					
		Шкідливий вплив розповсюджується на територію більш ніж одна область АБО на території не менш ніж 3 міст обласного значення	Шкідливий вплив розповсюджується на територію однієї області АБО на територію більш ніж одного міста обласного значення	Шкідливий вплив розповсюджується на територію одного міста обласного значення	Шкідливий вплив роз-повсюджується на територію об'єкта інфраструктури	**Не критично**	PK_5=0
		Час					

Продовження додатка 3

		Шкідливий вплив на навколишнє середовище та безпечні умови життя зберігається протягом більш ніж один рік	Шкідливий вплив на навколишнє середовище та безпечні умови життя зберігається протягом від півроку до одного року	Шкідливий вплив на навколишнє середовище та безпечні умови життя зберігається протягом від одного місяця до півроку	Шкідливий вплив на навколишнє середовище та безпечні умови життя зберігається протягом до одного місяця	Не критично	PK_6=0
II. Політична значущість об'єкта інфраструктури							
4	Припинення або порушення функціонування державних органів влади	**Припинення або порушення функціонування Адміністрації Президента України, Верховної Ради України, Кабінету Міністрів України, Ради безпеки та оборони України, Конституційного Суду України, Верховного Суду України.**	Припинення або порушення функціонування центральних органів виконавчої влади та обласних державних адміністрацій	Припинення або порушення роботи місцевих державних адміністрацій, органів державного управління в адміністративно-територіальних одиницях України	Припинення або порушення роботи місцевих органів влади	Не критично	PK_7=4
5.	Негативний вплив на довіру людей до державних інституцій	**Матиме значний вплив**	Матиме великий вплив	Матиме середній вплив	Матиме незначний вплив	Не критично	PK_8=4

6.	Шкода інтересам іншим державам-партнерам України	Так, принаймні двом країнам або порушення умов міждержавного договору	Так, принаймні однієї країні або порушення умов міжурядового договору	Можливі негативні наслідки для інших держав, але їх вплив навряд чи буде значним	Держави не постраждають або не має місце порушення умов міжвідомчого договору	Не критично	PK_9=3
7.	Рівень протестних настроїв	Дуже високий рівень протестних настроїв: ризик протестів з блокуванням роботи Адміністрації Президента України, Верховної Ради України, Кабінету Міністрів України, Ради безпеки та оборони України, Конституційного Суду України, Верховного Суду України.	Високий рівень протестних настроїв: ризик протестів з блокуванням центральних органів виконавчої влади та обласних державних адміністрацій	Середній рівень протестних настроїв ризик блокування роботи місцевих органів влади, об'єктів критичної інфраструктури	Незначний рівень протестних настроїв: блокування роботи об'єкта критичної інфраструктури	Не критично	PK_{10}=0
III. Економічна значущість об'єкта інфраструктури							
8.	Заподіяння збитків об'єкта інфраструктури (у відсотках прогнозованого обсягу річного доходу за всіма	Більш ніж 15%	Від 10 до 15%	Від 5 до 10%	Менш ніж 5%	Не критично	PK_{11}=4

	видами діяльності)						
9.	Заподіяння збитків державному бюджету України (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	Більш ніж 0,1%	Від 0,1% до 0,05%	Від 0,05% до 0,01%	Менш ніж 0,01%	Не критично	PK_{12}=1
10.	Заподіяння збитків місцевим бюджетам (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	Більш ніж 0,1%	Від 0,1% до 0,05%	Від 0,05% до 0,01%	Менш ніж 0,01%	Не критично	PK_{13}=1
IV. Взаємозв'язок між об'єктами критичної інфраструктури							
11.	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує такі ж основні послуги	Матиме негативний вплив (якщо так, вкажіть який)			Не матиме впливу	Не критично	PK_{14}=0

12.	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що надає інші основні послуги	Матиме негативний вплив (якщо так, вкажіть який)			Не матиме впливу	Не критично	PK_{15}=4
V. Значущість для забезпечення оборони країни та безпеки держави							
13.	Припинення або порушення (невиконання встановлених показників) функціонування пунктів управління (ситуаційного центру), що оцінюється в рівні (значущості) пункту управління або ситуаційного центру	Припинення або порушення функціонування пунктів управління Верховного головнокомандувача ЗСУ, Головнокомандувача ЗСУ- начальника Генерального штабу або ситуаційного центру Адміністрації Президента України, Кабінету Міністрів України, Ради безпеки та оборони України.	Припинення або порушення функціонування пунктів управління або ситуаційного центру органів центральної виконавчої влади, пунктів управління Сухопутних військ, Повітряних Сил, військово-морських Сил, десантно-штурмових військ, сил спеціальних операцій, Національної гвардії України, Державної прикордонної служби.	Припинення або порушення функціонування обласної державної адміністрації, ситуаційних центрів органів державної влади на місцях		Не критично	PK_{16}=0

14.	Зниження показників державного оборонного замовлення	Зниження обсягів продукції (робіт, послуг) у заданий період часу (у відсотках)					
		Більше ніж 15%	Від 10 до 15%	Від 5 до 10%	Менше ніж 5%.	Не критично	PK_{17}=0
		Збільшення часу виготовлення продукції (робіт, послуг) із заданим обсягом (відсотків встановленого часу на виготовлення продукції)					
		Більше ніж 40%	Від 10% до 40%	Від 5% до 10%	Менше ніж 5%	Не критично	PK_{18}=0
Сумарна оцінка ΣPK_i							

6. Визначення категорії критичності.

$$PK_{\text{ОКІ}} = \frac{\Sigma PK_i}{\Sigma PK_{max}} = \frac{8+25}{20*4} = \frac{32}{80} = 0{,}4.$$

Відповідно до правила:

I категорія критичності, якщо $0{,}8 < PK_{OKI} \leq 1$;
II категорія критичності, якщо $0{,}63 < PK_{OKI} \leq 0{,}8$;
III категорія критичності, якщо $0{,}37 < PK_{OKI} \leq 0{,}63$;
IV категорія критичності, якщо $0{,}2 < PK_{OKI} \leq 0{,}37$;
об'єкт не є критичним, якщо $PK_{OKI} \leq 0{,}2$.

КНЕДП може бути віднесено до III категорії критичності.

Валентин ПЕТРОВ