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

16.07.18 № 05/01-2200

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

Щодо погодження проектів
постанов КМУ

Направляємо на погодження проекти постанов Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування» та «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури», розроблені Адміністрацією Державної служби спеціального зв'язку та захисту інформації України на виконання вимог частини третьої статті 4 та частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» та завдань, передбачених абзацами 1 та 3 пункту 1 Плану організації підготовки проектів актів, необхідних для забезпечення реалізації зазначеного Закону України, схваленого на засіданні Кабінету Міністрів України 22.11.2017.

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

Зазначені проекти постанов доопрацьовано з урахуванням зауважень Інтернет Асоціації України, надісланих листами № 81 від 06.06.2018 та № 87 від 14.06.2018. Інформація щодо врахування наданих зауважень наведена у додатку.

Додатки: 1. Проект постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування», прим. № 1, на 10 арк.;
2. Пояснювальна записка до проекту постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів

0.31

критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування», прим. № 1, на 5 арк.;

3. Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування», прим. № 1, на 12 арк.;

4. Повідомлення про оприлюднення проекту нормативно-правового акта на 1 арк., тільки на адресу;

5. Інформація щодо врахування зауважень Інтернет Асоціації України на 6 арк., тільки на адресу;

6. Проект постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури», прим. № 1, на 22 арк.;

7. Пояснювальна записка до проекту постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури», прим. № 1, на 7 арк.;

8. Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури», прим. № 1, на 15 арк.;

9. Повідомлення про оприлюднення проекту нормативно-правового акта на 1 арк., тільки на адресу;

10. Інформація щодо врахування зауважень Інтернет Асоціації України на 5 арк., тільки на адресу.

Голова Служби Л.О. Євдоченко

Проект

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2018 р. №

Київ

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

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

1. Затвердити такі, що додаються:

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

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

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

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

Л.О. Євдоченко

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 2018 р. № _____

ЗАГАЛЬНІ ВИМОГИ
з кіберзахисту об'єктів критичної інфраструктури

1. Цей документ визначає загальні вимоги з кіберзахисту об'єктів критичної інфраструктури (далі – Загальні вимоги). Ці Загальні вимоги є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури (далі – ОКІ).

2. У цих Загальних вимогах терміни вживаються у такому значенні:

критичні бізнес/операційні процеси ОКІ – це процеси організації функціонування об'єктів критичної інфраструктури, реалізація загроз на які призводить до найбільших втрат самого об'єкта критичної інфраструктури, навколишнього середовища, суспільства, держави; для організації функціонування цього процесу можуть використовуватися декілька інформаційно-телекомунікаційних систем;

система інформаційної безпеки – сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об'єкті критичної інформаційної інфраструктури ОКІ з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об'єкті критичної інформаційної інфраструктури ОКІ (далі – ОКІІ або Система), порушенню режиму функціонування та/або недоступності служб (функцій) ОКІІ, порушення функціонування компонентів ОКІІ, забезпечення спостережності за діями користувачів ОКІІ та функціонуванням засобів захисту ОКІІ;

політика інформаційної безпеки – політика, яка визначає підхід організації до інформаційної безпеки, набір вимог, правил, обмежень, рекомендацій, які регламентують порядок дотримання та забезпечення інформаційної безпеки.

Інші терміни вживаються у значеннях, наведених у Законах України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373.

3. Метою забезпечення кіберзахисту ОКІ є запобігання кіберінцидентам, виявлення та захист від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) в ОКІІ, порушення режиму функціонування та/або недоступності служб (функцій) ОКІІ, порушення функціонування компонентів ОКІІ тощо.

4. Кіберзахист ОКІ забезпечується впровадженням на ОКІІ комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю.

5. Кіберзахист ОКІ є складовою частиною робіт зі створення (модернізації) та експлуатації ОКІІ. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу ОКІІ.

6. Кіберзахист об'єкта критичної інфраструктури забезпечується власником та/або керівником ОКІ відповідно до цієї постанови та законодавства в сфері захисту інформації та кібербезпеки.

7. У випадку, якщо в ОКІІ обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вимоги цих Загальних вимог повинні бути враховані під час створення (модернізації) в такій Системі комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи в сфері технічного захисту інформації.

Створення комплексної системи захисту інформації ОКІІ та її державна експертиза здійснюється відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

Під час створення комплексної системи захисту інформації ОКІІ повинна надаватися перевага засобам захисту інформації українського виробництва за умови, що такі засоби не порушують стале функціонування ОКІІ та можуть бути впроваджені в цій Системі.

8. У випадку, якщо в ОКІІ не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вимоги цих Загальних вимог повинні бути враховані під час створення (модернізації) системи інформаційної безпеки об'єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки цього об'єкта.

Створення системи інформаційної безпеки ОКІІ здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки.

Технічне завдання формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків в Системі. Методичною основою для оцінки ризиків в ОКІІ є стандарт ДСТУ ISO/IEC 27005.

Власник та/або керівник ОКІ організовує проведення незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури згідно з вимогами законодавства.

9. Власник та/або керівник ОКІ організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузевий CERT) про кіберінциденти та кібератаки, які стосуються його ОКІІ.

10. Органи державної влади отримують доступ до мережі Інтернет через Систему захищеного доступу державних органів до мережі Інтернет Держспецзв'язку (далі – СЗДІ) або через тих операторів, провайдерів телекомунікацій, які мають захищені вузли доступу до глобальних мереж передачі даних зі створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не розповсюджуються на Системи закордонних дипломатичних установ України.

11. Власник та/або керівник ОКІ з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує створення резервних копій інформаційних ресурсів ОКІІ та критичних бізнес/операційних процесів ОКІ для оперативного їх відновлення у разі пошкодження або знищення.

Органи державної влади для збереження резервних копій своїх інформаційних ресурсів та їх оперативного відновлення використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Держспецзв'язку.

12. Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій інформаційних ресурсів, підключення до СЗДІ використовують ресурси Національної телекомунікаційної мережі.

13. Організаційні та технічні заходи з кіберзахисту, які впроваджуються в ОКІІ, повинні забезпечувати:

визначення в ОКІ загальної політики інформаційної безпеки;

управління доступом суб'єктів доступу до об'єктів захисту ОКІІ;

ідентифікацію та автентифікацію суб'єктів доступу та об'єктів захисту ОКІІ;

реєстрацію подій компонентами ОКІІ та їх періодичний аудит;

мережевий захист компонентів та інформаційних ресурсів ОКІІ;

забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів ОКІІ;

визначення умов використання змінних носіїв інформації в ОКІІ;

визначення умов використання програмного та апаратного забезпечення ОКІІ;

визначення умов розміщення компонентів ОКІІ.

Мінімальний склад заходів із забезпечення кіберзахисту ОКІ, які повинні бути впроваджені при створенні комплексної системи захисту інформації (системи інформаційної безпеки) ОКІІ, наведено у додатку до цих Загальних вимог.

Мінімальний склад заходів із забезпечення кіберзахисту ОКІ підлягає доповненню відповідно до технології обробки інформації в ОКІІ, особливостей функціонування та програмно-апаратного складу Системи, складу інформаційних ресурсів та компонентів ОКІІ, які підлягають захисту, тощо.

При доповненні мінімального складу заходів із забезпечення кіберзахисту ОКІ для кожної загрози ОКІІ зіставляється захід або група заходів, що забезпечують блокування однієї або декількох загроз, або знижують ризик її реалізації виходячи з умов функціонування ОКІІ. У разі, якщо базовий набір заходів не дозволяє забезпечити блокування (нейтралізацію) усіх загроз ОКІІ, мають бути визначені додаткові заходи, які ці загрози блокують.

При формуванні додаткових заходів із забезпечення кіберзахисту ОКІ розробник комплексної системи захисту інформації (системи інформаційної безпеки) ОКІІ може керуватися нормативними документами сфери технічного захисту інформації, міжнародними та/або галузевими стандартами з питань інформаційної безпеки.

14. При відсутності можливості реалізації окремих заходів з кіберзахисту, наведених в додатку до цих Загальних вимог, і/або неможливості їх застосування до окремих об'єктів захисту чи суб'єктів доступу, у тому числі внаслідок їх можливого негативного впливу на функціонування ОКІІ, або неможливості їх реалізації в ОКІІ через особливості функціонування або складу компонентів ОКІІ, повинні бути розроблені і впроваджені компенсуючі заходи, що забезпечують блокування (нейтралізацію) загроз ОКІІ, або обґрунтовано виключені окремі заходи з мінімального складу заходів із забезпечення кіберзахисту ОКІ.

Власник та/або керівник ОКІ у ході розробки організаційних і технічних заходів щодо забезпечення кіберзахисту ОКІ обґрунтовує застосування компенсуючих заходів або виключення окремих заходів з мінімального складу заходів із забезпечення кіберзахисту ОКІ. При цьому у ході проведення незалежного аудиту інформаційної безпеки ОКІ або державної експертизи комплексної системи захисту інформації ОКІІ має бути оцінена достатність і адекватність компенсуючих заходів, які застосовані для блокування (нейтралізації) загроз ОКІІ та зменшення ризиків ОКІ, або обґрунтованість виключення окремих заходів з мінімального складу заходів із забезпечення кіберзахисту ОКІ.

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

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

Л.О. Євдоченко

Додаток
до Загальних вимог з
кіберзахисту об'єктів
критичної інфраструктури

Мінімальний склад заходів із забезпечення кіберзахисту ОКІ

Загальна політика інформаційної безпеки

1. Об'єкт критичної інфраструктури повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки. Повинні бути визначені відповідальні за забезпечення політики інформаційної безпеки, яка прийнята в ОКІ, та контроль за її дотриманням. При визначенні відповідальних за забезпечення політики інформаційної безпеки повинна надаватися перевага особам, які мають освіту або досвід роботи у сфері технічного захисту інформації або інформаційної безпеки.

Підрозділ або посадова особа з інформаційної безпеки повинні бути підпорядковані безпосередньо керівнику ОКІ.

Функції підрозділу або посадової особи з інформаційної безпеки можуть бути покладені на службу захисту інформації підприємства, установи, організації.

2. В ОКІ повинні бути визначені права та обов'язки всіх категорій користувачів та адміністраторів ОКІІ. Повинні бути задокументовані обов'язки адміністраторів з обслуговування компонентів Системи та забезпечення її інформаційної безпеки.

В ОКІ повинні бути призначені відповідальні за функціонування та інформаційну безпеку критичних бізнес/операційних процесів з числа керівного складу підрозділів ОКІ, працівники яких забезпечують функціонування цих критичних процесів.

3. В ОКІ повинен бути визначений перелік інформаційних, програмних та апаратних ресурсів ОКІІ, рівень їх критичності для ОКІ та/або функціонування Системи та можливий рівень наслідків у випадку порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) Системи, порушення функціонування компонентів Системи.

4. В ОКІ повинно бути розроблено та затверджено політику управління ризиками інформаційної безпеки, з визначенням методики їх оцінювання та оброблення. Методичною основою для вибору методики є стандарт ДСТУ ISO/IEC 27005.

5. Власник/керівник ОКІ зобов'язаний не рідше одного разу на рік організовувати та проводити обстеження своїх ОКІІ з метою оновлення даних щодо програмно-апаратного складу ОКІІ, технології обробки

інформації в ОКІІ, переліку критичних інформаційних ресурсів та компонентів ОКІІ, які підлягають захисту, тощо. Методичною основою для проведення обстеження ОКІІ є вимоги НД ТЗІ 3.7-003-05.

Якщо за результатами обстеження ОКІІ виявлено, що в Системі змінилася технологія обробки інформації, впроваджені нові програмні або апаратні компоненти, змінився перелік критичних інформаційних ресурсів та компонентів ОКІІ, які підлягають захисту, тощо здійснюється перегляд загроз ОКІІ, ризиків інформаційній безпеці та рівня прийнятного ризику.

У випадку виявлення нових загроз та/або ризиків, здійснюється оновлення технічного завдання на створення комплексної системи захисту інформації (системи інформаційної безпеки) ОКІІ, іншої документації Системи та впровадження оновлених вимог в Системі.

6. Власник/керівник ОКІ зобов'язаний забезпечити розробку та підтримання в актуальному стані технічної, проектної тощо документації на комплексну систему захисту інформації (систему інформаційної безпеки) ОКІІ (в захищеному від модифікації електронному та/або паперовому вигляді) з обов'язковим описом реалізованих в Системі організаційних та технічних заходів безпеки інформації.

Мінімальний перелік документації ОКІІ визначається в технічному завданні на створення комплексної системи захисту інформації (системи інформаційної безпеки) ОКІІ.

Програмні та апаратні компоненти ОКІІ повинні бути налаштовані відповідно до встановленої в організації політики інформаційної безпеки та технічної, проектної тощо документації на комплексну систему захисту інформації (систему інформаційної безпеки) ОКІІ.

Інформація щодо програмно-апаратного складу ОКІІ, налаштування та конфігураційна інформація програмних та апаратних компонентів ОКІІ, інформація про параметри та режими їх функціонування, журнали реєстрації подій (логи) та дані аудиту компонентів Системи, інформація про облікові записи користувачів, їх атрибути та права доступу, об'єкти захисту та їх атрибути доступу, інша інформація, яка розкриває параметри та особливості функціонування компонентів ОКІІ є інформацією з обмеженим доступом. Ступінь обмеження доступу до цієї інформації визначається власником та/або керівником ОКІ відповідно до вимог законодавства.

7. В ОКІ необхідно розробити та затвердити політику інформаційної безпеки в організації, яка:

визначає мету та основні принципи забезпечення захисту інформаційних ресурсів, критичних бізнес/операційних процесів тощо в ОКІ;

визначає опис критичних бізнес/операційних процесів. Опис повинен включати схему кожного критичного бізнес процесу з описом компонентів та користувачів ОКІІ, які задіяні в цьому процесі;

встановлює вимоги щодо порядку визначення, надання, зміни та скасування прав доступу користувачів та адміністраторів до служб (функцій), інформації та компонентів ОКІІ та порядок контролю (аудиту) використання прав доступу користувачами та адміністраторами. При цьому необхідно дотримуватися принципу надання мінімального рівня повноважень користувачам та адміністраторам відповідно до їх службових обов'язків;

визначає політику фізичної безпеки та захисту ОКІІ від навколишнього середовища;

встановлює вимоги щодо забезпечення інформаційної безпеки при взаємовідносинах з постачальниками;

визначає політику управління обліковими записами в програмному та апаратному забезпеченні ОКІІ. Політика повинна визначати порядок створення, блокування та призупинення облікових записів користувачів та адміністраторів в компонентах Системи;

встановлює вимоги щодо порядку формування, надання, скасування та контролю (аудиту) за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних, для доступу до служб (функцій), інформації та компонентів ОКІІ. Повинні бути визначені також вимоги до складності паролів, періодичності їх зміни, блокування роботи користувача при певній кількості спроб підбору паролю, порядок поводження із зовнішніми носіями автентифікаційних даних тощо;

визначає політику забезпечення безперебійної роботи ОКІІ, зокрема порядок резервування даних та компонентів ОКІІ, зберігання резервних копій даних, відновлення даних з резервних копій та заміни компонентів Системи у випадку виходу їх з ладу, тощо;

визначає політику дій персоналу ОКІІ у випадку відмов або збоїв Системи в цілому або окремих її компонентів;

визначає порядок використання змінних (зовнішніх) носіїв інформації в ОКІІ;

визначає політику мережевого захисту, зокрема, щодо сегментації мережі ОКІІ, захисту від вірусів, зловмисного коду, шкідливого програмного забезпечення, встановлення та налаштування засобів мережевого захисту тощо;

визначає політику проведення модернізації (оновлення) компонентів ОКІІ, внесення змін до складу Системи та в налаштування компонентів Системи. Повинні бути визначені відповідальні особи, які мають право проводити ці робити, а також порядок дотримання політики безпеки, яка прийнята в ОКІ, при їх проведенні;

визначає опис критичних бізнес/операційних процесів. Опис повинен включати схему кожного критичного бізнес процесу з описом компонентів та користувачів ОКІІ, які задіяні в цьому процесі;

визначає політику управління оновленнями (порядок отримання, перевірки, розповсюдження та застосування оновлень програмного забезпечення компонентів ОКІІ);

визначає політику реєстрації та аудиту подій, що реєструються компонентами ОКІІ. Політика повинна містити перелік подій, які повинні реєструватися кожним компонентом Системи, параметри ведення журналів (логів) реєстрації подій та їх архівування, порядок та періодичність аудиту журналів (логів) реєстрації подій адміністраторами ОКІІ на предмет виявлення ознак кібератак або кіберінцидентів;

визначає політику управління інцидентами кібербезпеки. Політика повинна містити перелік подій, які кваліфікуються як кіберінциденти, описи дій користувачів та адміністраторів при їх виникненні, порядок інформування посадових осіб ОКІ, CERT-UA (у разі наявності – галузевий CERT);

визначає політику використання електронної пошти користувачами ОКІІ.

Політика інформаційної безпеки може розроблятися у вигляді одного або групи окремих документів. Повинні бути встановлені правила та порядок внесення змін до таких документів.

8. Вимоги прийнятої в ОКІ політики інформаційної безпеки повинні бути доведені під підпис або в інший юридично значимий спосіб до всіх його співробітників. В ОКІ повинна бути визначена відповідальність його співробітників за порушення встановленої політики інформаційної безпеки.

9. Власник/керівник ОКІ повинен впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль обізнаності.

10. В підрозділі, або у посадової особи з інформаційної безпеки ОКІ повинен бути створений та підтримуватись в актуальному стані перелік програмного та апаратного забезпечення, що використовується в ОКІІ (в захищеному від модифікації електронному та/або паперовому вигляді).

Управління доступом суб'єктів доступу до об'єктів захисту ОКІІ

11. Механізми розподілу прав доступу ОКІІ повинні:

охоплювати всі інформаційні ресурси Системи (інформацію, яка зберігається та обробляється в Системі, технологічну інформацію програмного та апаратного забезпечення Системи, журнали реєстрації подій тощо);

визначати права на виконання операцій для всіх користувачів та адміністраторів (за необхідності, також активних процесів) над інформаційними ресурсами Системи (читання, модифікація, створення, видалення, тощо);

за необхідності, також визначати права доступу користувачів та адміністраторів до служб (функцій) Системи.

12. За можливості реалізації, в ОКІІ повинна надаватися перевага централізованому розповсюдженню налаштувань прав та атрибутів доступу, параметрів реєстрації подій, інших параметрів безпеки та системних налаштувань компонентів Системи.

Ідентифікація та автентифікація суб'єктів доступу та об'єктів захисту ОКІІ

13. Користувачі та адміністратори ОКІІ повинні отримувати доступ до служб (функцій), інформації та компонентів Системи в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) користувача і деякої інформації, що вводиться користувачем (пароль), та/або фізичного ідентифікатора, що надається користувачем (ключ, сертифікат, токен тощо).

14. Засоби ОКІІ повинні надавати можливість ідентифікації кожної операції користувача в Системі та їх протоколювання в журналах реєстрації подій.

15. Для надання доступу до служб (функцій) та інформації ОКІІ повинна використовуватись багатофакторна автентифікація користувачів та адміністраторів. Допускається використання двофакторної автентифікації тільки в тому програмному забезпеченні компонентів ОКІІ, яке не підтримує багатофакторну автентифікацію.

16. В ОКІІ повинні бути заблоковані або змінені облікові записи адміністраторів та їх паролів встановлені за замовчуванням в усіх компонентах Системи. Забороняється використовувати облікові записи та паролі за замовчуванням в програмному та апаратному забезпеченні Системи.

17. В ОКІІ повинні бути видалені або заблоковані неперсоналізовані і гостьові облікові записи користувачів і адміністраторів та використовуватись виключно персоналізовані облікові записи користувачів і адміністраторів в усіх компонентах Системи. При звільненні співробітника його обліковий запис повинен бути негайно заблокований або видалений в усіх компонентах Системи.

18. Обладнання, яке підключається до системи управління технологічними процесами ОКІ повинно бути ідентифіковане (наприклад, за IP-адресою, MAC-адресою тощо), та повинні бути вжиті заходи, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.

Реєстрація подій компонентами ОКІІ та їх періодичний аудит

19. Компоненти ОКІІ повинні забезпечити реєстрацію, збереження у електронних журналах та захист від модифікації інформації щонайменше про такі події:

доступ та дії з інформацією, яка зберігається та обробляється в Системі, а також з налаштуваннями програмного та апаратного забезпечення Системи, журналами реєстрації подій тощо (читання, модифікація, створення, видалення тощо);

реєстрація подій, пов'язаних із встановленням та зміною прав доступу до служб (функцій), інформації та компонентів Системи;

вхід/вихід користувачів та адміністраторів в/із компонентів Системи;

невдалі спроби входу користувачів та адміністраторів в Систему та перевищення граничної кількості спроб введення пароля;

реєстрація, видалення (блокування) облікових записів користувачів та адміністраторів в компонентах Системи;

зміна паролю користувача в компонентах Системи;

реєстрація подій, пов'язаних зі зміною конфігураційних настроювань компонентів Системи;

спроби здійснення несанкціонованого доступу до ресурсів Системи;

негативні результати перевірок цілісності даних та програмного і апаратного забезпечення Системи;

всі дії адміністратора з журналами реєстрації подій компонентів Системи та налаштування ним параметрів реєстрації.

Повний перелік подій, які реєструються компонентами ОКІІ, визначається виходячи із встановленої в ОКІ політики інформаційної безпеки.

20. Журнали реєстрації подій компонентів ОКІІ повинні містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнали реєстрації повинні містити інформацію, достатню для встановлення користувача, процесу і мережного об'єкта, що мали відношення до кожної зареєстрованої події.

21. Має бути забезпечений захист журналів реєстрації подій компонентів ОКІІ від несанкціонованого доступу, модифікації або руйнування. Електронні журнали реєстрації подій повинні зберігатися не менше ніж рік з дати їх утворення.

22. В ОКІ повинно бути впроваджено систему збору та аналізу журналів реєстрації подій програмного та апаратного забезпечення ОКІІ. Така система повинна мати можливість встановлення фільтрів, які

дозволяють робити вибірку та аналіз журналів та подій за різними критеріями та, за потреби, мати інтерфейси обміну з іншими системами.

Оброблення журналів реєстрації подій не повинно впливати на функціонування критичних бізнес/операційних процесів ОКІ.

23. В ОКІІ повинна бути забезпечена можливість роботи з архівними журналами реєстрації подій за попередні періоди шляхом завантаження журналів в ОКІІ із зовнішнього джерела. При цьому, дані, що завантажуються, повинні тільки доповнювати існуючі журнали, але не затирати і не змінювати інформацію, що вже зберігається в них.

Архівні журнали реєстрації подій зберігаються на фізично відокремленому компоненті ОКІІ або окремому носії даних не менше року з дати їх утворення.

Мережевий захист компонентів та інформаційних ресурсів ОКІІ

24. В ОКІІ повинні використовуватись засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів. Повинно бути забезпечене централізоване управління засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

25. Доступ адміністраторам до компонентів ОКІІ повинен надаватися виключно з IP-адрес (робочих станцій), які визначені для адміністрування Системи.

26. У разі неможливості фізичного розділення зовнішньої мережі та ОКІІ на межі (периметрі) між зовнішніми мережами, іншими інформаційно-телекомунікаційними системами, що обслуговують ОКІ, та Системою повинні бути встановлені засоби мережевого захисту, що реалізують щонайменше такі функції захисту:

захист від атак «нульового дня», виявлення зловмисного коду та шкідливого програмного забезпечення;

фільтрація трафіку та розмежування доступу між мережею ОКІ та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з'єднань, небажаних сайтів тощо. Блокування трафіку та з'єднань які не відповідають визначеним критеріям;

фільтрація та аналіз трафіку за визначеними відповідно до політики безпеки критеріями;

моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики безпеки критеріями;

виявлення та запобігання атакам та вторгненням направленим на програмні та апаратні компоненти та інформацію ОКІІ;

захист від атак типу «відмова в обслуговуванні»;

захист від несанкціонованого доступу з боку мережі Інтернет;

балансування навантаження;

маскування топології і мережевих адрес мережі;

завершення з'єднання з вузлом, у разі атаки;

здійснення реєстрації подій, що мають відношення до безпеки.

Для захисту повинні використовуватись програмно-апаратні засоби, потужність яких визначається виходячи із потужності трафіку, який передбачається в мережі, з урахуванням потенціального його збільшення.

27. В ОКІ необхідно здійснити розподіл ОКІІ на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту.

28. Реалізована архітектура ОКІІ повинна надавати можливість розподілу мережі щонайменше на такі частини (сегменти):

зовнішня (DMZ): демілітаризована зона із зовнішніми діапазонами адресації мережі для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів Системи;

зона прикладних застосувань Системи (APP-зона): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення серверів застосувань, доступна для виконання функціональних запитів користувачів інформаційних сервісів;

зона сховищ даних Системи (DB-зона): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення баз даних, доступна для доступу за запитами прикладних застосувань APP-зони;

зона прикладних застосувань Системи безпеки (Security-зона): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення сервісів та служб захисту інформації;

тестова зона (Test-зона): захищена внутрішня зона із внутрішньою адресацією, призначена для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення ОКІІ перед тим як впровадити їх в промислову експлуатацію в Системі.

29. Сервери та обладнання, що забезпечують функціонування сервісів та віддалений доступ клієнтів/користувачів ОКІІ із зовнішніх мереж, повинні бути розміщені в демілітаризованій зоні системи. З'єднання серверів та обладнання, що розміщено в демілітаризованій зоні, з серверами та обладнанням внутрішньої мережі ОКІІ повинні захищатися міжмережевим екраном.

30. Робочі станції, з яких виконуються дії щодо адміністрування програмного та апаратного забезпечення ОКІІ, а також серверні частини

засобів захисту інформації, повинні бути розміщені в Security-зоні мережі, захищеної за допомогою міжмережевого екрана.

31. Сегмент інформаційної інфраструктури ОКІ в якому знаходиться система керування технологічними процесами повинен бути відокремленим від інших Систем ОКІ. У випадку логічного відокремлення, на межі сегменту повинен бути встановлений міжмережевий екран.

32. Повинні бути визначені та відключені (заблоковані) програмні порти компонентів ОКІІ, які є небезпечними для використання з точки зору кібербезпеки.

33. Власник/керівник ОКІ зобов'язаний виконувати перевірку ефективності заходів щодо захисту ОКІІ від зовнішнього проникнення шляхом виконання періодичних (не рідше одного разу на рік) тестів на проникнення (Penetration test). У разі отримання негативних результатів після проведення тестів, необхідно вжити заходів щодо усунення їх причин.

34. В ОКІІ передача даних бездротовими мережами передачі даних повинна здійснюватися виключно захищеними з'єднаннями із забезпеченням її конфіденційності та цілісності. Забороняється використання в ОКІІ технологій Wi-Fi та Bluetooth.

35. Для захисту даних, які передаються через незахищене середовище між віддаленими користувачами, адміністраторами та системою, між компонентами ОКІІ (поза контрольованою територією ОКІ), між ОКІІ та іншими (зовнішніми) інформаційно-телекомунікаційними системами, необхідно використовувати захищені з'єднання із забезпеченням конфіденційності та цілісності цих даних.

36. Систему управління технологічними процесами ОКІ дозволяється підключати до глобальних мереж передачі даних, зокрема до мережі Інтернет, тільки у випадку неможливості функціонування технологічного процесу без підключення до мережі Інтернет та за умови впровадження усіх заходів захисту відповідно до вимог цих Загальних вимог або конкретизованих вимог з кіберзахисту відповідної сфери регулювання, до якої відноситься ОКІ.

37. Доступ до глобальних мереж передачі даних, зокрема до мережі Інтернет, ОКІІ повинні отримувати через тих операторів, провайдерів телекомунікацій, які мають захищені вузли доступу до глобальних мереж передачі даних зі створеними комплексними системами захисту інформації з підтвердженою відповідністю. У договорі з надавачем цих послуг вказуються зобов'язання щодо виконання тієї частини цих Загальних вимог, які він надає ОКІ та наявність КСЗІ з підтвердженою відповідністю.

Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів ОКІІ

38. Інформаційна інфраструктура ОКІ повинна будуватися на базі відмовостійкого підходу. Для забезпечення відмовостійкості ОКІІ повинно здійснюватися, як мінімум, таке:

періодичне створення резервних копій інформаційних ресурсів ОКІІ та критичних бізнес/операційних процесів ОКІ, включаючи інформацію, яка зберігається в системі, технологічну інформацію компонентів системи та образів серверів системи, та їх відновлення у випадку втрати або пошкодження;

резервування критичних для функціонування ОКІІ та бізнес/операційних процесів ОКІ програмних та апаратних компонентів з метою їх гарячої заміни у випадку виходу з ладу компонента. У разі використання в системі віртуальних серверів, використання резервних віртуальних машин у випадку виходу з ладу серверу або при збільшенні навантаження на нього;

дублювання (кластеризація) критичних для функціонування ОКІІ та бізнес/операційних процесів ОКІ програмних та апаратних компонентів системи з метою гарячої заміни, зниження навантаження та збільшення продуктивності;

використання засобів балансування навантаження;

використання джерел безперебійного живлення для критичних компонентів системи;

зв'язок з мережею Інтернет з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами) – для ОКІ, які надають свої послуги через мережу Інтернет.

39. Під час розроблення, модернізації або оновлення компонентів системи управління технологічними процесами ОКІ зобов'язаний використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента його мережі для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення перед тим як впровадити їх в промислову експлуатацію.

Умови використання змінних носіїв інформації в ОКІІ

40. В ОКІІ повинна здійснюватися перевірка всіх змінних (зовнішніх) носіїв інформації перед кожним їх використанням в системі засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

41. В ОКІІ повинна здійснюватися ідентифікація всіх змінних (зовнішніх) носіїв інформації за допомогою унікального ідентифікатора.

Повинно бути унеможливлено використання змінних (зовнішніх) носіїв інформації, які не зареєстровані в Системі.

42. В ОКІІ повинний бути відключений автоматичний запуск програм із змінних (зовнішніх) пристроїв та носіїв інформації.

43. Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, мають бути заблоковані адміністраторами ОКІІ.

Умови використання програмного та апаратного забезпечення

44. В ОКІІ повинна здійснюватися перевірка на цілісність та авторство оновлень компонентів системи. У разі порушення цілісності або не підтвердження авторства оновлення, воно повинно бути відхилене і не застосовуватись, а ця подія запротокольована в журналі подій.

45. У складі ОКІІ повинно використовуватись програмне та апаратне забезпечення, для якого не припинено підтримку виробника. Повинні використовуватись офіційні стабільні версії прикладного програмного забезпечення та драйверів.

В ОКІІ повинна надаватися перевага програмному забезпеченню, яке має більш вищий рівень гарантій, відповідно до НД ТЗІ 2.5-004-99, за результатами державної експертизи у сфері технічного захисту інформації.

46. В ОКІІ повинно блокуватися самостійне встановлення або видалення користувачами програмного забезпечення в системі. Право на встановлення або видалення програмного забезпечення повинен мати тільки уповноважений адміністратор.

47. Засоби ОКІІ повинні забезпечувати неприйняття файлу/повідомлення в обробку при отриманні негативного результату перевірки електронного цифрового підпису файлу/повідомлення, що надійшло. Ця подія повинна відображатися в журналі реєстрації подій.

48. Програмні та апаратні засоби, які використовуються у складі ОКІІ, не повинні мати походження з іноземної держави, до якої застосовано санкції згідно з Законом України «Про санкції» (далі у цьому пункті – іноземна держава) або розроблених/виготовлених юридичною особою-резидентом іноземної держави, або юридичною особою, частка статутного капіталу якої знаходиться у власності іноземної держави, або юридичною особою, яка знаходиться під контролем юридичної особи іноземної держави.

Умови розміщення компонентів ОКІІ

49. Компоненти та/або інформація ОКІІ, крім систем управління технологічними процесами, можуть знаходитись в сторонньому (не власному) центрі обробки даних тільки за умови, що центр обробки даних знаходиться на території, підконтрольній України, а власником центру обробки даних є резидент України. При цьому у договорі з цим центром

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

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

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

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

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

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

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

Л.О. Євдоченко

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 2018 р. № _____

Критерії та порядок
віднесення об'єктів до об'єктів критичної інфраструктури

1. Цей документ визначає критерії та порядок віднесення інфраструктурних об'єктів до об'єктів критичної інфраструктури (далі – ОКІ).

2. У цьому документі терміни вживаються у такому значенні:

життєво-важливі послуги – послуги, які забезпечуються державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні яких призводять до швидких негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

життєво-важливі функції – функції, які виконують державні органи, державні установи, підприємства та організації будь-якої форми власності, порушення яких призводить до швидких негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

категорія критичності об'єкту критичної інфраструктури – відносна міра важливості об'єкта критичної інфраструктури, класифікована в залежності від ступеня його впливу на реалізацію життєво-важливих функцій та надання життєво-важливих послуг;

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

суб'єкт (оператор) критичної інфраструктури - державний орган, підприємство, установа або організація, юридична та/або фізична особа, який (яка) на правах власності, оренди або на інших законних підставах має право розпоряджатися об'єктом критичної інфраструктури, що виконує життєво-важливі функції або надає життєво-важливі послуги за призначенням у відповідних секторах (галузях) економіки або сферах діяльності;

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

уповноважений орган – державний орган, орган місцевого самоврядування, орган управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронний орган, який забезпечує формування і реалізацію державної політики у відповідному секторі (галузі) економіки або сфері діяльності та у власності чи розпорядженні якого (яких) є об'єкт критичної інфраструктури, та/або до сфери управління якого (яких) належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта.

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

3. Віднесення об'єкта до об'єктів критичної інфраструктури здійснюється на підставі аналізу ймовірних ризиків для його діяльності, який передбачає оцінку рівня захисту об'єкта критичної інфраструктури від загроз усіх видів, уразливості об'єкта до цих загроз та можливих наслідків від їх реалізації.

4. Оцінка ступеня ризиків щодо діяльності об'єкта критичної інфраструктури визначається Методикою оцінки ризиків на об'єктах критичної інфраструктури, яка затверджується уповноваженим органом.

5. Критерієм віднесення об'єкта до об'єктів критичної інфраструктури є настання негативних наслідків для функціонування суспільства та безпеки населення, забезпечення національної безпеки і оборони України через порушення його сталого функціонування.

До негативних наслідків, до яких може призвести порушення сталого функціонування об'єкта критичної інфраструктури, відносяться:

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

негативний вплив на стан енергетичної безпеки держави (регіону);

негативний вплив на стан економічної безпеки держави;

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

негативний вплив на систему управління державою;

негативний вплив на суспільно-політичну ситуацію в державі;

негативний вплив на імідж держави;

порушення сталого функціонування фінансової системи держави;

порушення сталого функціонування транспортної інфраструктури держави (регіону);

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

негативний вплив на критичну інфраструктуру ЄС.

6. Об'єкти критичної інфраструктури включаються до загальнодержавного переліку об'єктів критичної інфраструктури, який формується на базі секторальних (галузевих) переліків об'єктів критичної інфраструктури.

7. Секторальні (галузеві) переліки об'єктів критичної інфраструктури формуються та ведуться уповноваженими органами на підставі відомостей про об'єкти критичної інфраструктури, що знаходяться у їх власності чи розпорядженні, та відомостей, отриманих від суб'єктів (операторів) критичної інфраструктури відповідних секторів (галузей) економіки або сфер діяльності.

8. Пропозиції щодо внесення об'єкта критичної інфраструктури до секторального (галузевого) переліку об'єктів критичної інфраструктури подаються суб'єктом (оператором) критичної інформаційної інфраструктури до уповноваженого органу.

9. Відомості про об'єкт критичної інфраструктури для внесення до секторального (галузевого) переліку об'єктів критичної інфраструктури подаються суб'єктом (оператором) критичної інфраструктури уповноваженому органу у паперовій та електронній формі.

10. Уповноважений орган, який забезпечує формування і реалізацію державної політики у відповідному секторі (галузі) економіки або сфері діяльності, погоджує секторальний (галузевий) перелік об'єктів критичної інфраструктури з СБУ та розглядає її обґрунтовані пропозиції щодо включення до секторального (галузевого) переліку об'єктів критичної інфраструктури тих об'єктів критичної інфраструктури, які за її оцінками є значущими для національної безпеки України.

11. Секторальні (галузеві) критерії віднесення об'єкта критичної інфраструктури до галузевого переліку об'єктів критичної інфраструктури затверджуються уповноваженим органом.

12. Для формування секторального (галузевого) переліку об'єктів критичної інфраструктури суб'єкти (оператори) критичної інфраструктури збирають та подають до уповноваженого органу відомості щодо:

призначення і складу об'єкта критичної інфраструктури;

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

можливих загроз для об'єкта критичної інфраструктури, у т.ч. відомостей щодо інцидентів, які раніше виникали на об'єкті критичної інфраструктури та мали негативний вплив на стабільне його функціонування;

осіб, відповідальних за своєчасне подання зазначених вище відомостей.

13. Суб'єкти (оператори) критичної інфраструктури здійснюють заходи щодо актуалізації відомостей, що містяться у секторальних (галузевих) переліках об'єктів критичної інфраструктури, у разі:

зміни відомостей, визначених у пункті 12 цього документу;

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

зміни категорії об'єкта критичної інфраструктури.

14. Уповноважені органи подають відомості про об'єкти критичної інфраструктури до уповноваженого органу, який забезпечує формування і реалізацію державної політики в сфері захисту критичної інфраструктури, та здійснюють заходи щодо актуалізації відомостей, що містяться у загальнодержавному переліку об'єктів критичної інфраструктури, у разі:

зміни призначення об'єкта критичної інфраструктури, відомостей про відповідальних осіб;

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

зміни категорії об'єкта критичної інфраструктури.

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

I категорія критичності – критично-важливі об'єкти;

II категорія критичності – життєво-важливі об'єкти;

III категорія критичності – важливі об'єкти;

IV категорія критичності – необхідні об'єкти.

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

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

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

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

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

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

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

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

Л.О. Євдоченко

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту постанови Кабінету Міністрів України

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

Мета: проект постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури» врегулює питання забезпечення кіберзахисту об'єктів критичної інфраструктури держави шляхом визначення загальних вимог з кіберзахисту об'єктів критичної інфраструктури та створить правові засади віднесення підприємств, установ та організацій до об'єктів критичної інфраструктури.

1. Підстава розроблення проекту акта

Проект постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури» (далі – проект 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».

2. Обґрунтування необхідності прийняття акта

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії ним та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів та кібератак. Аналіз кіберзагроз свідчить, що кібератаки на комунікаційні системи та системи управління технологічними процесами об'єктів критичної інфраструктури держави таких галузей, як енергетика, хімічна промисловість та інші може призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави. 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. Таким чином, існуючі кіберзагрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки. Тому, важливим є розроблення загальних вимог з кіберзахисту об'єктів критичної інфраструктури. Запропоновані вимоги з кіберзахисту розроблені на базі сучасного досвіду провідних країн світу і є усталеною практикою як в ЄС так і в США та гармонізовані з вимогами міжнародних стандартів ЄС, НАТО та NIST з питань забезпечення кіберзахисту.

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 реалізації життєво-важливих функцій та надання життєво-важливих послуг у всіх секторах економіки та сферах діяльності задля впровадження низки заходів щодо захисту таких об'єктів від реалізації можливості виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму.

Впровадження заходів з кіберзахисту, що передбачені проектом Постанови, дозволить підприємствам, установам та організаціям, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, забезпечити захист від кібератак, запобігти порушенню конфіденційності, цілісності та доступності своїх інформаційних ресурсів, порушенню режиму сталого функціонування об'єкта критичної інфраструктури.

3. Суть проекту акта

Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури встановлюють низку обов'язкових заходів, які мають бути виконані на об'єктах критичної інфраструктури задля забезпечення їх захисту від кібератак, запобігання порушенню конфіденційності, цілісності та доступності їх інформаційних ресурсів, порушенню режиму сталого функціонування об'єкта критичної інфраструктури.

Серед основних вимог – невідкладне інформування про кіберінциденти та кібератаки, які стосуються його об'єкту критичної інформаційної інфраструктури, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, обов'язковість створення резервних копій інформаційних ресурсів, необхідність виконання організаційних та технічних заходів з кіберзахисту на об'єкті критичної інформаційної інфраструктури. Крім того, проектом Постанови визначається можливість розробки центральними органами виконавчої влади конкретизованих вимог з кіберзахисту з урахуванням галузевої специфіки функціонування об'єктів критичної інфраструктури, які відносяться до сфери їх управління, а також встановлюється мінімальний склад заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури, який включає:

загальну політику інформаційної безпеки;

заходи із забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єктів критичної інформаційної інфраструктури;

умови використання змінних носіїв інформації в об'єктів критичної інформаційної інфраструктури;

умови використання програмного та апаратного забезпечення;

умови розміщення компонентів об'єктів критичної інформаційної інфраструктури.

Одночасно проектом Постанови встановлюються підходи до визначення критеріїв віднесення об'єктів до об'єктів критичної інфраструктури за секторами (галузями) критичної інфраструктури або сферами діяльності, а також порядок їх віднесення. Критерієм віднесення об'єкта до об'єктів критичної інфраструктури є настання негативних наслідків для функціонування суспільства та безпеки населення, забезпечення національної безпеки і оборони України через порушення його сталого функціонування. Проектом Постанови наводиться перелік негативних наслідків, до яких може призвести порушення сталого функціонування об'єкта критичної інфраструктури, а також встановлюється, що віднесення об'єкта до об'єктів критичної інфраструктури здійснюється на підставі аналізу ймовірних ризиків для його діяльності, який передбачає оцінку рівня захисту об'єкта критичної інфраструктури від загроз усіх видів, уразливості об'єкта до цих загроз та можливих наслідків від їх реалізації.

Встановленим проектом Постанови порядком віднесення об'єктів до об'єктів критичної інфраструктури визначається необхідність залучення до цієї діяльності суб'єктів (операторів) критичної інфраструктури будь-якої форми власності та уповноважених органів, які через ведення галузевих (секторальних) переліків отримують можливість координувати та контролювати заходи з захисту

на об'єктах критичної інфраструктури, щодо яких вони здійснюють владні повноваження.

Розробка галузевих (секторальних) критеріїв віднесення об'єкта критичної інфраструктури до галузевого переліку об'єктів критичної інфраструктури дозволить чітко окреслити секторальні об'єкти критичної інфраструктури та забезпечити належний їх захист, у тому числі й від кіберзагроз, з урахуванням галузевих особливостей.

4. Правові аспекти

Правовими підставами розроблення проекту Постанови є вимоги частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» та завдання, передбачене Планом організації підготовки проектів 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.

5. Фінансово-економічне обґрунтування

Реалізація проекту Постанови потребує від підприємств, установ та організацій, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, додаткового фінансування заходів з кіберзахисту таких об'єктів для забезпечення виконання визначеного проектом Постанови мінімального складу заходів щодо кіберзахисту.

Мінімальний склад заходів із забезпечення кіберзахисту впроваджується під час створення на об'єкті критичної інформаційної інфраструктури об'єктів критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки.

Мінімальний склад заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури може бути доповнений відповідно до специфіки функціонування конкретного об'єкта критичної інфраструктури.

При цьому, з метою скорочення витрат, проектом постанови передбачена розробка на об'єкті критичної інфраструктури політики управління ризиками інформаційної безпеки, виходячи з якої власник та/або керівник об'єктів критичної інфраструктури може оцінити рівні ризиків та визначити, які заходи додатково йому потрібно вжити.

При відсутності можливості реалізації окремих заходів з кіберзахисту і/або неможливості їх застосування до окремих об'єктів захисту чи суб'єктів доступу, в тому числі внаслідок їх можливого негативного впливу на функціонування об'єкта критичної інформаційної інфраструктури, або неможливості їх реалізації на об'єкті критичної інформаційної інфраструктури через особливості

функціонування або складу компонентів об'єкта критичної інформаційної інфраструктури, власниками та/або керівниками об'єктів критичної інфраструктури розробляються і впроваджуються компенсуючі заходи, що забезпечують блокування (нейтралізацію) загроз об'єкта критичної інформаційної інфраструктури або обґрунтовано виключаються окремі заходи з мінімального складу заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури.

Проектом постанови також передбачено, що центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури, які відносяться до сфери їх управління, за погодженням з Адміністрацією Держспецзв'язку. Підприємства, установи та організації, які відносяться до сфери управління такого центрального органу виконавчої влади, можуть при створенні комплексної системи захисту інформації (системи інформаційної безпеки) своїх об'єктів критичної інформаційної інфраструктури використовувати такі конкретизовані вимоги з кіберзахисту.

Таким чином власникам та/або керівникам об'єктів критичної інфраструктури надані всі можливості для мінімізації витрат на заходи кіберзахисту виходячи з ризикоорієнтованого підходу. Одночасно, враховуючи специфіку функціонування багатьох підприємств, установ та організацій, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, їх власникам та/або керівникам надана можливість впровадження додаткових заходів з кіберзахисту, впровадження альтернативних або виключення деяких заходів з мінімального переліку виходячи із специфіки функціонування об'єктів критичної інфраструктури з одночасним обґрунтуванням цих дій під час створення комплексної системи захисту інформації або системи інформаційної безпеки.

Слід зазначити, що системи захисту, які впроваджуються на кожному з підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури, різні за своєю складністю і, відповідно, складність заходів і засобів захисту, які впроваджуються на кожному об'єкті, різні і залежать від специфіки функціонування та складності об'єкта критичної інфраструктури. Тому не можливо розрахувати витрати на впровадження заходів з кіберзахисту та проведення їх незалежного аудиту для усіх підприємств, установ та організацій.

Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення комплексної системи захисту (системи інформаційної безпеки) в інформаційно-телекомунікаційній системі з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи.

Водночас, якщо в інформаційно-телекомунікаційній системі об'єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, в таких інформаційно-телекомунікаційних системах, відповідно до вимог статті 8 Закону України «Про захист інформації в інформаційно-

телекомунікаційних системах» повинна бути створена комплексна система захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється шляхом проведення державної експертизи в сфері технічного захисту інформації. Відповідно до проекту Постанови у випадку створення комплексної системи захисту інформації заходи з кіберзахисту повинні бути враховані при створенні комплексної системи захисту інформації, а їх відповідність підтверджена під час державної експертизи комплексної системи захисту інформації, тобто в рамках коштів, які виділяються на створення комплексної системи захисту інформації, які власник повинен був передбачити все рівно відповідно до вимог вищенаведеного Закону України.

Розпорядженням Кабінету Міністрів України від 13.12.2001 № 572-р «Про фінансування заходів щодо криптографічного та технічного захисту інформації, охорона якої забезпечується державою відповідно до законодавства» передбачається, зокрема, що міністерства, інші центральні органи виконавчої влади, Рада міністрів Автономної Республіки Крим, обласні, Київська та Севастопольська міські держадміністрації щороку під час підготовки бюджетних запитів повинні передбачати кошти на фінансування заходів щодо криптографічного та технічного захисту інформації, охорона якої забезпечується державою відповідно до законодавства, в тому числі для розпорядників бюджетних коштів нижчого рівня. Мінфін щороку під час розроблення проекту Державного бюджету України повинен передбачати кошти для фінансування зазначених заходів.

6. Прогноз впливу

Проект Постанови є регуляторним актом.

Проект Постанови не стосується питання розвитку адміністративно-територіальних одиниць.

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

Проект Постанови не стосується питань громадського здоров'я, екології та навколишнього середовища.

7. Позиція заінтересованих сторін

Проект Постанови не матиме впливу на ключові інтереси заінтересованих сторін.

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

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

8. Громадське обговорення

Проект Постанови розміщено на офіційному веб-сайті Держспецзв'язку за адресою: www.dsszzi.gov.ua. Зауваження і пропозиції, отримані від громадських

організацій, обговорені у ході зустрічі з їх представниками та частково враховані при доопрацюванні проекту Постанови.

9. Позиція заінтересованих органів

Проект Постанови було надіслано на погодження до Державної регуляторної служби України, 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 гвардії України, Національної поліції України, Адміністрації Державної прикордонної служби України. Зауваження та пропозиції заінтересованих органів у цілому враховані при доопрацюванні проекту постанови. Ті зауваження і пропозиції, які були відхилені або враховані частково, обговорені на міжвідомчій узгоджувальній нараді, за результатами якої підготовлено нову редакцію проекту Постанови, яка надсилається на повторне погодження до заінтересованих органів.

10. Правова експертиза

Проект Постанови потребує правової експертизи Мін'юсту.

11. Запобігання дискримінації

Проект Постанови не містить положень, які мають ознаки дискримінації.

12. Запобігання корупції

У проекті Постанови відсутні норми, які можуть містити ризики вчинення корупційних правопорушень.

13. Прогноз результатів

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

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

«___» _____ 2018 року

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту Постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури»

І. Визначення проблеми

Проект постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури» (далі – проект 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 ним та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів.

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

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 відбулися DDoS-атаки і злом сайту 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 вивела з ладу ряд 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 привела 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 визначити критерії 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. Тому, важливим також є розроблення загальних вимог з кіберзахисту об'єктів критичної інфраструктури.

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 відсутні критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, а також відсутні загальні вимоги з кіберзахисту таких об'єктів.

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

II. Цілі державного регулювання

Основною ціллю проекту Постанови є створення правових засад для забезпечення кіберзахисту об'єктів критичної інфраструктури держави, шляхом визначення загальних вимог з кіберзахисту об'єктів критичної інфраструктури, а також визначення критеріїв та порядку віднесення підприємств, установ та організацій до об'єктів критичної інфраструктури.

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

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 проекту 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	Відсутні, оскільки такий підхід	Додаткових витрат не потребує

	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	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	Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи
Альтернатива 3	Відсутні 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	Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи

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		Дія регуляторного акта не буде розповсюджуватися на малі та мікро суб'єктів господарювання		–

	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 проекту Постанови буде задіяний галузевий (секторальний) підхід до віднесення об'єктів до об'єктів критичної інфраструктури, що дозволить чітко визначити всі об'єкти критичної інфраструктури.		
Питома вага групи у загальній кількості, відсотків	Питома вага великих та середніх суб'єктів господарювання у загальній кількості може бути визначена тільки після віднесення об'єктів до об'єктів критичної інфраструктури, 100	0	100 %

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні, оскільки такий підхід призведе до неможливості визначення об'єктів критичної інфраструктури, та висування до них вимог із кіберзахисту, що може	Додаткових витрат не потребує

	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	
Альтернатива 2	Високі, оскільки прийняття проекту Постанови дозволить визначити об'єкти критичної інфраструктури, та висунути до них вимоги із кіберзахисту, що може завадити виникненню надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави у випадку здійснення терористичних актів по відношенню до таких об'єктів. Прийняття проекту Постанови дозволить забезпечити власникам та/або керівникам підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури, запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються в об'єкті критичної інфраструктури, порушенню режиму функціонування та/або недоступності служб (функцій) об'єкту критичної інфраструктури, порушення функціонування його	Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи

	компонентів тощо. Таким чином прийняття на об'єкті критичної інфраструктури заходів з кіберзахисту дозволить забезпечити підприємствам, установам та організаціям, що віднесені до об'єктів критичної інфраструктури, їх стале функціонування.	
Альтернатива 3	Відсутні, 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	Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	Додаткових витрат не потребує
Альтернатива 2	Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи
Альтернатива 3	Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

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

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

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

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

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

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

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

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1	Відсутні	Додаткових витрат не потребує	Проблема продовжує існувати
Альтернатива 2	Визначення об'єктів критичної інфраструктури, та висунення до них	Виходячи зі сталої практики створення систем захисту в інформаційно-	Проблема більше існувати не буде

	вимог із кіберзахисту, що може завадити виникненню надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави у випадку здійснення терористичних актів по відношенню до таких об'єктів	телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи	
Альтернатива 3	Відсутні	Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи	Проблема значно зменшиться, деякі важливі та критичні аспекти проблеми залишаться невирішеними

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

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

Адміністрацією Держспецзв'язку підготовлено проект Постанови, яким пропонується затвердити Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури, а також Критерії та порядоквіднесення об'єктів до об'єктів критичної інфраструктури.

Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури визначають:

– вимоги, які згідно із законодавством віднесені до об'єктів критичної інфраструктури;

– норму щодо невідкладного інформування власником та/або керівником об'єкту критичної інфраструктури урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузевий CERT) про кіберінциденти та кібератаки, які стосуються його об'єкту критичної інформаційної інфраструктури;

– обов'язковість забезпечення створення власником та/або керівником об'єкту критичної інфраструктури резервних копій своїх інформаційних ресурсів;

– вимоги до організаційних та технічних заходів з кіберзахисту, які впроваджуються на об'єкті критичної інформаційної інфраструктури;

– можливість розробки центральними органами виконавчої влади конкретизованих вимог з кіберзахисту з урахуванням галузевої специфіки функціонування об'єктів критичної інфраструктури, які відносяться до сфери їх управління;

– мінімальний склад заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури, який включає:

1) загальну політику інформаційної безпеки;

2) заходи із забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єктів критичної інформаційної інфраструктури;

3) умови використання змінних носіїв інформації в об'єктів критичної інформаційної інфраструктури;

4) умови використання програмного та апаратного забезпечення;

5) умови розміщення компонентів об'єктів критичної інформаційної інфраструктури.

Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури визначають:

– типи підприємств, установ, організацій незалежно від форми власності, які можуть бути віднесені до об'єктів критичної інфраструктури;

– критерії віднесення об'єктів до об'єктів критичної інфраструктури;

– категоризацію об'єктів критичної інфраструктури;

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

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

В додатку до Загальних вимог з кіберзахисту об'єктів критичної інфраструктури визначений мінімальний склад заходів із забезпечення кіберзахисту, які повинні бути впроваджені власниками та/або керівниками підприємств, установ та організацій, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури.

Мінімальний склад заходів із забезпечення кіберзахисту впроваджується під час створення на об'єкті критичної інформаційної інфраструктури об'єктів критичної інфраструктури комплексної системи захисту інформації або системи

інформаційної безпеки. Випадки, коли на об'єкті критичної інформаційної інфраструктури впроваджується комплексна система захисту інформації, а коли системи інформаційної безпеки визначені в п.7 та п. 8 Загальних вимог.

Мінімальний склад заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури може бути доповнений під час створення в об'єкті критичної інформаційної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки відповідно до специфіки функціонування об'єктів критичної інфраструктури.

При доповненні мінімального складу заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури для кожної загрози об'єкту критичної інформаційної інфраструктури зіставляється захід або група заходів, що забезпечують блокування однієї або декількох загроз або знижують ризик її реалізації виходячи з умов функціонування об'єкта критичної інформаційної інфраструктури. У разі якщо мінімальний набір заходів не дозволяє забезпечити блокування (нейтралізацію) усіх загроз об'єкта критичної інформаційної інфраструктури, повинні бути визначені додаткові заходи, які ці загрози блокують.

При цьому з метою скорочення витрат, в об'єктів критичної інфраструктури розробляється політика управління ризиками інформаційної безпеки виходячи з якої власник та/або керівник об'єктів критичної інфраструктури може оцінити рівні ризиків та визначити які заходи додатково йому потрібно вжити. Методичною основою для оцінки ризиків може слугувати стандарт з інформаційної безпеки ДСТУ ISO/IEC 27005.

При відсутності можливості реалізації окремих заходів з кіберзахисту, і/або неможливості їх застосування до окремих об'єктів захисту чи суб'єктів доступу, в тому числі внаслідок їх можливого негативного впливу на функціонування об'єкта критичної інформаційної інфраструктури або неможливості їх реалізації в об'єкт критичної інформаційної інфраструктури через особливості функціонування або складу компонентів об'єкта критичної інформаційної інфраструктури, власниками та/або керівниками об'єктів критичної інфраструктури розробляються і впроваджуються компенсуючі заходи, що забезпечують блокування (нейтралізацію) загроз об'єкта критичної інформаційної інфраструктури або обґрунтовано виключаються окремі заходи з мінімального складу заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури.

Центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури, які відносяться до сфери їх управління, за погодженням з Адміністрацією Держспецзв'язку. Підприємства, установи та організації, які відносяться до сфери управління такого центрального органу виконавчої влади, можуть при створенні комплексної системи захисту інформації (системи інформаційної безпеки) своїх об'єктів критичної інформаційної інфраструктури використовувати такі конкретизовані вимоги з кіберзахисту.

Таким чином власникам та/або керівникам об'єктів критичної інфраструктури надані всі можливості мінімізації витрат на заходи кіберзахисту виходячи з ризикоорієнтованого підходу. Одночасно, враховуючи специфіку функціонування багатьох підприємств, установ та організацій, які відповідно до

законодавства віднесені до об'єктів критичної інфраструктури, їх власникам та/або керівникам надана можливість впровадження додаткових заходів з кіберзахисту, впровадження альтернативних або виключення деяких заходів з мінімального переліку виходячи із специфіки функціонування об'єктів критичної інфраструктури з одночасним обґрунтуванням цих дій під час створення комплексної системи захисту інформації або системи інформаційної безпеки.

Системи захисту, які впроваджуються на кожному з підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури, різні за своєю складністю і, відповідно, складність заходів і засобів захисту, які впроваджуються на кожному об'єкті різні і залежать від специфіки функціонування та складності об'єкту критичної інфраструктури. Тому не можливо розрахувати витрати на впровадження заходів з кіберзахисту та проведення їх незалежного аудиту для усіх підприємств, установ та організацій.

Для досягнення цієї цілі проектом постанови передбачається:

– затвердити Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури;

– затвердити Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури.

Заходи, що пропонуються для розв'язання проблеми:

– погодити проект Постанови з Державною регуляторною службою України, Міністерством фінансів України, Міністерством економічного розвитку і торгівлі України, Службою безпеки України, Міністерством внутрішніх справ України, Міністерством енергетики та вугільної промисловості України, Міністерством інфраструктури України, Міністерством оборони України, Міністерством регіонального розвитку, будівництва та житлово-комунального господарства України, Державною службою України з надзвичайних ситуацій, Національною гвардією України, Національною поліцією України, Адміністрацією Державної прикордонної служби України;

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

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

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

Реалізація положень проекту Постанови:

Дозволить створити правові засади для забезпечення кіберзахисту об'єктів критичної інфраструктури держави, шляхом визначення загальних вимог з кіберзахисту об'єктів критичної інфраструктури, а також визначення критеріїв та порядку віднесення підприємств, установ та організацій до 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

Впровадження положень проекту 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 до законодавства віднесені до об'єктів критичної інфраструктури.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується.

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

VIII. Визначення показників результативності дії регуляторного акта

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

– 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 проекту 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 проекту 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 – якщо в інформаційно-телекомунікаційній системі обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, в таких інформаційно-телекомунікаційних системах, відповідно до вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» повинна бути створена комплексна система захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється шляхом проведення державної експертизи в сфері технічного захисту інформації. Відповідно до Проекту постанови у випадку створення комплексної системи захисту інформації заходи з кіберзахисту повинні бути враховані при створенні комплексної системи захисту інформації, а їх відповідність підтверджена під час державної експертизи комплексної системи захисту інформації, тобто в рамках коштів які виділяються на створення

комплексної системи захисту інформації, які власник повинен був передбачити все рівно відповідно вимог вищенаведеного закону.

Розпорядженням Кабінету Міністрів України від 13.12.2001 № 572-р «Про фінансування заходів щодо криптографічного та технічного захисту інформації, охорона якої забезпечується державою відповідно до законодавства» передбачається, зокрема, що органи державної влади під час складання бюджетних запитів на наступні бюджетні періоди зобов'язані передбачати виділення коштів на реалізацію заходів із технічного та криптографічного захисту інформації в інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності.

Виходячи зі сталої практики створення систем захисту в інформаційно-телекомунікаційних системах різного ступеня складності, можна визначити орієнтовну вартість створення системи захисту в інформаційно-телекомунікаційних системах з підтвердженням її відповідності на рівні 10-15% вартості самої інформаційно-телекомунікаційної системи;

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

– кількість об'єктів критичної інфраструктури;

– кількість сформованих галузевих переліків об'єктів критичної інфраструктури;

– кількість здійсненихзаходів щодо актуалізації відомостей, що містяться у Переліку;

– кількість створених комплексних систем захисту інформації об'єктів критичної інформаційної інфраструктури;

– кількість створених систем інформаційної безпеки об'єктів критичної інфраструктури.

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

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

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

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

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

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

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

Повідомлення про оприлюднення проекту постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури»

1. Стислий виклад змісту проекту акта

Проект постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури» 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».

Документ визначає загальні вимоги з кіберзахисту об'єктів критичної інфраструктури, критерії та порядок віднесення підприємств, установ та організацій до об'єктів критичної інфраструктури.

2. Адреси для зауважень та пропозицій до проекту акта

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

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

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

електронна: cyber@dsszzi.gov.ua;

- Державної регуляторної служби України:

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

факс (044) 254-43-93;

електронна: inform@dkrp.gov.ua

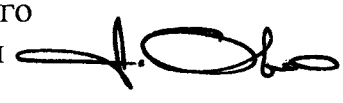
3. Обраний спосіб оприлюднення проекту акта

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

4. Строк, протягом якого приймаються зауваження та пропозиції

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

Доопрацьований проект акта та аналіз його регуляторного впливу.

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

___.___ 2018 р.

Інформація щодо врахування зауважень Інтернет Асоціації України

Проект ПОСТАНОВИ КМУ **Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури**			
Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури			
життєво-важливі послуги – послуги, які забезпечуються державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні яких призводять до настання негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки; життєво-важливі функції – функції, які виконують державні органи, державні установи, підприємства та організації будь-якої форми власності, порушення яких призводить до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;	Визначення окремих термінів, наведених у пункті 2 проекту Критеріїв, потрібно доопрацювати. У проекті Критеріїв пропонується надати визначення термінів, окремі з яких, не у повній мірі відповідають визначенню термінів у сфері законодавства з кібербезпеки. наприклад, у Законі. Зазначене, на нашу думку, одразу ж призведе до різного застосування Закону та нормативно-правового акту. До прикладу, у проекті Критеріїв пропонуються визначення та застосовуються терміни «життєво-важливі послуги» та «життєво-важливі функції», проте, у Законі, застосовується, схожий за змістом, термін «критично важливі об'єкти інфраструктури». Крім цього, зі змісту не зрозуміло, які саме «негативні наслідки для населення, суспільства, соціально-економічного стану та національної безпеки» слід розуміти у визначенні термінів «життєво-важливі послуги» та «життєво-важливі функції».	Відхилено Терміни узгоджуються з термінами, які використовуються у проекті закону «Про критичну інфраструктуру та її захист» (пройшов процедуру зовнішнього погодження)	життєво-важливі послуги – послуги, які забезпечуються державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні яких призводять до настання негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки; життєво-важливі функції – функції, які виконують державні органи, державні установи, підприємства та організації будь-якої форми власності, порушення яких призводить до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;
кризова ситуація – ситуація, що склалася на елементі об'єкта критичної інфраструктури або у взаємопов'язаних сферах внаслідок настання надзвичайної	потребує доопрацювання визначення терміну «кризова ситуація», оскільки, запропонована редакція є нечіткою, а, відтак, незрозумілою та	Враховано Термін виключено	

ситуації або небезпечної події, яка призвела до порушення функціонування об'єкта критичної інфраструктури, для реагування на яку та/або відновлення до штатного режиму необхідне залучення зовнішніх сил і ресурсів;	неоднозначною для застосування у сфері законодавства про кібербезпеку. Зокрема, що таке «елемент об'єкта критичної інфраструктури», «взаємопов'язані сфери» з елементом об'єкта критичної інфраструктури, «небезпечна подія», «штатний режим», «залучення зовнішніх сил і ресурсів»		
суб'єкт критичної інфраструктури - державний орган, підприємство, установа, організація, юридична та (або) фізична особа, якому (якій) на правах власності, оренди або на інших законних підставах належить об'єкт критичної інфраструктури та який (яка) відповідає за його поточне функціонування; уповноважений орган – державний орган, орган місцевого самоврядування, орган управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронні органи, у власності чи розпорядженні якого (яких) є об'єкт критичної інфраструктури, та/або до сфери управління яких належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта;	Наслідком нечіткого формулювання визначення термінів є й те, що фактично однаковими за своїм змістом є терміни «суб'єкт критичної інфраструктури» та «уповноважений орган».	враховано	суб'єкт (оператор) критичної інформаційної інфраструктури - державний орган, підприємство, установа або організація, юридична та/або фізична особа, який (яка) на правах власності, оренди або на інших законних підставах має право розпоряджатися об'єктом критичної інформаційної інфраструктури, що використовується для виконання життєво-важливих функцій або надання життєво-важливих послуг за призначенням у відповідних секторах (галузях) економіки або сферах діяльності; уповноважений орган – державний орган, орган місцевого самоврядування, орган управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронний орган, який забезпечує формування і реалізацію державної політики у відповідному секторі (галузі) економіки або сфері діяльності, у власності чи розпорядженні якого є об'єкт критичної інформаційної

			інфраструктури та/або до сфери управління якого належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта.
3. До Переліку включаються об'єкти критичної інфраструктури об'єктів критичної інфраструктури, які: провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами потенційно небезпечних технологій і виробництв.	2. У пункті 3 проекту Критеріїв, в основному, повторюється інформація, яка зазначена у частині першій статті 6 Закону, хоча, з переліку виключено сфери сільського господарства, комунальні підприємства, натомість, хоч Законом і не встановлено, у проекті Критеріїв до об'єктів критичної інфраструктури запропоновано включити «об'єкти, що підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду». Тому, вважаємо за доцільне, пункт 3 проекту Критеріїв привести у відповідність до Закону та зазначити, що перелік видів та сфер діяльності, у яких підприємства, установи, організації незалежно від форми власності можуть бути віднесені до об'єктів критичної інфраструктури, визначено частиною першою статті 6 Закону України «Про основні засади забезпечення кібербезпеки України».	Враховано	виключено
4. Ступінь ризиків щодо діяльності об'єкта критичної інфраструктури, визначається Методикою оцінки ризиків на об'єктах критичної інфраструктури, яка затверджується Кабінетом Міністрів України. 7. Порядок віднесення до категорій	3. Пунктом 4 проекту Критеріїв пропонується визначити, що ступінь ризиків щодо діяльності об'єкта критичної інфраструктури, визначається Методикою оцінки ризиків на об'єктах критичної інфраструктури, яка затверджується	враховано	4. Оцінка ступеня ризиків щодо діяльності об'єкта критичної інфраструктури визначається Методикою оцінки ризиків на об'єктах критичної інфраструктури, яка затверджується уповноваженим

критичності об'єктів критичної інфраструктури визначається Кабінетом Міністрів України.	Кабінетом Міністрів України. А, положеннями пункту 7 проекту Критеріїв пропонується встановити, що порядок віднесення до категорій критичності об'єктів критичної інфраструктури визначається Кабінетом Міністрів України. Проте, Законом не встановлено повноважень Кабінету Міністрів України щодо розроблення таких нормативно-правових актів та, взагалі, не зазначено на необхідність розроблення ані Методики оцінки ризиків на об'єктах критичної інфраструктури, ані Порядку віднесення до категорій критичності об'єктів критичної інфраструктури. Тому, за необхідності та доцільності прийняття окремими документами, механізми оцінки ризиків на об'єктах критичної інфраструктури та порядок віднесення до категорій критичності об'єктів критичної інфраструктури, вважаємо, що ці документи повинні бути розроблені та включені, як додатки, до даної постанови.		органом.
12. Галузеві критерії віднесення об'єкта критичної інфраструктури до галузевого переліку об'єктів критичної інфраструктури розробляються та затверджуються уповноваженим органом з урахуванням критеріїв, викладених у пункті 6 цього документу.	4. Є підстави вважати, що у проекті Критеріїв розробником не враховано вимоги Директиви Ради 2008/114/ЄС від 08.12.2008 про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту, зокрема, при визначенні критеріїв у пунктах 5, 6 та 12 проекту Критеріїв.	враховано	9. Секторальні (галузеві) критерії віднесення об'єкта критичної інфраструктури до галузевого переліку об'єктів критичної інфраструктури затверджуються уповноваженим органом.

	Зокрема, у статті 3 вказаної Директиви ЄС рекомендовано ідентифікувати потенційні ЄКІ, що відповідають як наскрізним, так і секторальним критеріям та означенням, наданим в статті 2(a) і (b). При цьому, секторальні критерії повинні враховувати особливості окремих секторів ЄКТ. Разом з цим. у пункті 12 проекту Критеріїв не передбачено можливості врахування особливості окремих секторів та галузей економіки при розробленні галузевих критеріїв віднесення об'єкта критичної інфраструктури до галузевого переліку об'єктів критичної інфраструктури.		

Проект

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2018 р. №

Київ

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

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

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

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

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

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

3. Міністерствам та іншим центральним органам виконавчої влади:

розробити протягом трьох місяців з дня набрання чинності цієї постанови секторальні (галузеві) критерії віднесення об'єктів до секторального (галузевого) переліку об'єктів критичної інформаційної інфраструктури;

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

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

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

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

Л.О. Євдоченко

Затверджено
постановою Кабінету Міністрів України
від 2018 р. №

Порядок
формування переліку об'єктів критичної інформаційної інфраструктури

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

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

життєво-важливі послуги – послуги, які забезпечуються державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні яких призводять до настання негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

життєво-важливі функції – функції, які виконують державні органи, державні установи, підприємства та організації будь-якої форми власності, порушення яких призводить до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

секторальний (галузевий) перелік об'єктів критичної інформаційної інфраструктури – перелік об'єктів критичної інформаційної інфраструктури, які у певному секторі (галузі) економіки або сфері діяльності використовуються для виконання життєво-важливих функцій або надання життєво-важливих послуг за призначенням;

суб'єкт (оператор) критичної інформаційної інфраструктури - державний орган, підприємство, установа або організація, юридична та/або фізична особа, який (яка) на правах власності, оренди або на інших законних підставах має право розпоряджатися об'єктом критичної інформаційної інфраструктури, що використовується для виконання життєво-важливих функцій або надання життєво-важливих послуг за призначенням у відповідних секторах (галузях) економіки або сферах діяльності;

уповноважений орган – державний орган, орган місцевого самоврядування, орган управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронний орган, який забезпечує формування і реалізацію державної політики у відповідному секторі (галузі) економіки або сфері діяльності, у власності чи розпорядженні якого є об'єкт критичної інформаційної інфраструктури та/або до сфери управління якого належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта.

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

3. До Переліку включаються об'єкти критичної інформаційної інфраструктури тих інфраструктурних об'єктів, що включені до переліку об'єктів критичної інфраструктури.

4. Критерієм віднесення об'єкта до об'єктів критичної інфраструктури є настання негативних наслідків для функціонування суспільства та безпеки населення, забезпечення національної безпеки і оборони України через порушення його сталого функціонування.

До негативних наслідків, до яких може призвести порушення сталого функціонування об'єкта критичної інформаційної інфраструктури, відносяться:

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

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

негативний вплив на стан економічної безпеки держави (Н3);

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

негативний вплив на систему управління державою (Н5);

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

негативний вплив на імідж держави (Н7);

порушення сталого функціонування фінансової системи держави (Н8);

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

порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури, у тому числі її взаємодії з відповідними інфраструктурами інших держав (Н10);

негативний вплив на критичну інформаційну інфраструктуру ЄС (Н11).

5. Включений до Переліку об'єкт критичної інформаційної інфраструктури захищається від кібератак у першу чергу (пріоритетно).

6. Відомості про об'єкти критичної інформаційної інфраструктури, що включені до Переліку, вносяться до державного реєстру об'єктів критичної інформаційної інфраструктури.

7. Перелік об'єктів критичної інформаційної інфраструктури формується на базі секторальних (галузевих) переліків об'єктів критичної інформаційної інфраструктури.

8. Секторальні (галузеві) переліки об'єктів критичної інформаційної інфраструктури формуються та ведуться уповноваженими органами на підставі відомостей про об'єкти критичної інформаційної інфраструктури, що знаходяться у їх власності чи розпорядженні, та відомостей, отриманих від суб'єктів (операторів) критичної інформаційної інфраструктури.

9. Пропозиції щодо внесення об'єкта критичної інформаційної інфраструктури до секторального (галузевого) переліку об'єктів критичної інформаційної інфраструктури подаються суб'єктом (оператором) критичної інформаційної інфраструктури до уповноваженого органу.

10. Відомості про об'єкт критичної інформаційної інфраструктури для внесення до секторального (галузевого) переліку об'єктів критичної інформаційної інфраструктури подаються суб'єктом (оператором) критичної інформаційної інфраструктури уповноваженому органу у паперовій та електронній формі.

11. Уповноважений орган, який забезпечує формування і реалізацію державної політики у відповідному секторі (галузі) економіки або сфері діяльності, погоджує секторальний (галузевий) перелік об'єктів критичної інформаційної інфраструктури з СБУ та розглядає її обґрунтовані пропозиції щодо включення до Переліку тих об'єктів критичної інформаційної інфраструктури, які за її оцінками є значущими для національної безпеки України.

12. Для формування секторального (галузевого) переліку об'єктів критичної інформаційної інфраструктури суб'єкти (оператори) критичної інформаційної інфраструктури збирають та подають до уповноваженого органу відомості:

щодо назви (призначення) об'єкта критичної інформаційної інфраструктури, форми власності, наявність доступу до телекомунікаційних мереж;

виду інформації (інформаційні ресурси, технологічна інформація), виду інформації за порядком доступу (відкрита, інформація з обмеженим доступом (конфіденційна, службова)), яка обробляється об'єктом критичної інформаційної інфраструктури, сервіси з управління, контролю або моніторингу, які здійснюються об'єктом критичної інформаційної інфраструктури;

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

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

про осіб (адміністраторів безпеки), відповідальних за забезпечення кібербезпеки об'єкта критичної інформаційної інфраструктури.

13. Суб'єкти (оператори) критичної інформаційної інфраструктури здійснюють заходи щодо актуалізації відомостей, що містяться у секторальних (галузевих) переліках об'єктів критичної інформаційної інфраструктури, у разі:

суттєвої зміни відомостей, визначених у пункті 12 цього Порядку;

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

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

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

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

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

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

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

Л.О. Євдоченко

Додаток
до Порядку формування переліку
об'єктів критичної інформаційної
інфраструктури

Відомості про об'єкт критичної інформаційної інфраструктури

_____
(найменування заінтересованого органу)

для внесення до переліку об'єктів критичної інформаційної інфраструктури

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

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

___ _____ 20__ р.

*Зазначаються умовні позначення негативних наслідків згідно з пунктом 4 Порядку формування переліку об'єктів критичної інфраструктури інфраструктур.

Затверджено
постановою Кабінету Міністрів України
від 2018 р. № _____

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

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

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

Реєстр – автоматизована система накопичення, обліку, обробки і зберігання відомостей про об'єкти критичної інформаційної інфраструктури (далі – Системи) об'єктів критичної інфраструктури, які внесені до Переліку об'єктів критичної інформаційної інфраструктури.

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

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

здійснює заходи з адміністрування Реєстру;

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

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

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

вживає необхідних заходів для захисту відомостей інформаційного фонду Реєстру;

виконує інші заходи щодо забезпечення функціонування Реєстру.

4. Реєстр формується з метою:

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

надання методичної допомоги суб'єктам, які безпосередньо здійснюють у межах своєї компетенції заходи з кіберзахисту Систем, забезпечення захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

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

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

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

повну та скорочену назву Системи або її призначення;

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

технічне завдання на створення Системи;

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

місце розташування Системи та/або її елементів (підсистем);

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

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

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

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

сервери, які входять до складу Системи, у разі, коли вона підключена до мережі Інтернет, інших глобальних мереж передачі даних;

відповідальну особу та/або підрозділ, відповідальні за стан захисту інформації або за забезпечення інформаційної безпеки у Системі, у тому числі про ті, на які покладено функції служби захисту інформації;

проведення та результати державної експертизи комплексної системи захисту інформації системи та (або) результати незалежного аудиту інформаційної безпеки;

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

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

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

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

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

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

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

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

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

Л.О. Євдоченко

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

Мета: проект постанови Кабінету Міністрів України «Про затвердження Порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури» удосконалить порядок формування переліку об'єктів критичної інформаційної інфраструктури та визначить механізм формування та функціонування реєстру об'єктів критичної інформаційної інфраструктури.

1. Підстава розроблення проекту постанови

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

2. Обґрунтування необхідності прийняття акта

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

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

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

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

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

Крім того, забезпечення кіберзахисту об'єктів критичної інфраструктури в сучасних умовах 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 проекту постанови

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

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

Зважаючи на важливість створення виваженого механізму формування Переліку для подальшого впровадження відповідних загрозам заходів з

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

Визначення 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 надавати методичну допомогу щодо виявлених вразливостей (загроз) на об'єктах критичної інформаційної інфраструктури.

4. Правові аспекти

Правовими підставами розроблення проекту постанови є вимоги частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» та завдання, передбачене Планом організації підготовки проектів 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 проекту Постанови є: Конституція України, Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про телекомунікації», 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».

5. Фінансово-економічне обґрунтування

Реалізація проекту Постанови потребує витрат з державного бюджету у частині створення державного реєстру об'єктів критичної інформаційної інфраструктури. Адміністрація Держспецзв'язку включила до бюджетних пропозицій на 2019 рік кошти в в обсязі 500 тис. грн. на ці цілі.

6. Прогноз впливу

Проект постанови є регуляторним актом.

Проект постанови не стосується питання розвитку адміністративно-територіальних одиниць.

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

Проект постанови не стосується питань громадського здоров'я, екології та навколишнього середовища.

7. Позиція заінтересованих сторін

Проект постанови не матиме впливу на ключові інтереси заінтересованих сторін.

Проект постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку.

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

8. Громадське обговорення

Проект постанови розміщено на офіційному веб-сайті Держспецзв'язку за адресою: www.dsszzi.gov.ua. В рамках громадського обговорення були проведені робочі зустрічі з представниками громадських організацій для обговорення їх пропозицій та зауважень до проекту постанови.

9. Позиція заінтересованих органів

Проект Постанови було надіслано на погодження до Міністерства фінансів України, Міністерства економічного розвитку і торгівлі України, Міністерства внутрішніх справ України, Міністерства оборони України, Служби безпеки України, Державного агентства з питань електронного урядування України, Міністерства екології та природних ресурсів України, Міністерства енергетики та вугільної промисловості України, Міністерства закордонних справ України, Міністерства інфраструктури України, Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України, Міністерства соціальної політики України, Міністерства юстиції України, Державної казначейської служби України, Державної міграційної служби України, Державної служби України з надзвичайних ситуацій, Державної служби фінансового моніторингу України, Державної фіскальної служби України, Адміністрації Державної прикордонної служби України, Пенсійного фонду України та Служби зовнішньої розвідки України.

Зауваження та пропозиції заінтересованих органів в цілому враховані при доопрацюванні проекту постанови. Ті зауваження і пропозиції, що були відхилені або враховані частково, обговорені на міжвідомчій узгоджувальній нараді, за результатами якої підготовлено нову редакцію проекту постанови, яка надсилається на повторне погодження до заінтересованих органів.

10. Правова експертиза

Проект постанови потребує правової експертизи Мін'юсту.

11. Запобігання дискримінації

Проект постанови не містить положень, які мають ознаки дискримінації.

12. Запобігання корупції

У проекті постанови відсутні норми, які можуть містити ризики вчинення корупційних правопорушень.

13. Прогноз результатів

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

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

«___» _____ 2018 року

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

І. Визначення проблеми

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

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

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:

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

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.

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.

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

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.

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

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 національно 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 здійснюватись заходи з кіберзахисту, а також заходи з аудиту інформаційної безпеки.

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

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

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

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

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

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

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

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

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

II. Цілі державного регулювання

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

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

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

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні, 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	Витрати державного

	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	бюджету України на створення Реєстру становитимуть 500 тис. грн. Зазначена сума бюджетних коштів закладена у бюджетному запиті Держспецзв'язку на 2019 рік.
Альтернатива 3	Відсутні оскільки такий підхід призведе до надмірної кількості об'єктів критичної інформаційної інфраструктури та не дозволить коректно визначити першочерговість (пріоритетність) об'єктів критичної інформаційної інфраструктури, які мають захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки	Додаткових витрат не потребує

Оцінка впливу на сферу інтересів 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		Дія регуляторного акта не буде розповсюджуватися на малі та мікро суб'єктів господарювання		–

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

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

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

			критичні аспекти проблеми залишаться невирішеними

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

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

Адміністрацією Держспецзв'язку підготовлено проект Постанови, яким пропонується затвердити Порядок формування переліку об'єктів критичної інформаційної інфраструктури та Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

Порядок формування переліку об'єктів критичної інформаційної інфраструктури визначає:

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

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

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

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

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

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

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

– повноваження розпорядника Реєстру;

– мету формування Реєстру та його склад;

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

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

Для досягнення цієї цілі проектом постанови передбачається:

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

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

– визнати такою, що втратила чинність, постанову Кабінету Міністрів України від 23 серпня 2016 року № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

Заходи, що пропонуються для розв'язання проблеми:

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

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

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

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

Реалізація положень проекту Постанови:

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

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

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

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується.

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

VIII. Визначення показників результативності дії регуляторного акта

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

– 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 проекту 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 проекту 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 – проект акта розміщено на веб-сайті Держспецзв'язку (електронна адреса: www.dsszzi.gov.ua) у підрозділі «Повідомлення про оприлюднення та проекти» розділу «Регуляторна діяльність»;

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

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

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

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

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

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

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

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

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

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

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

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

1. Стислий виклад змісту проекту акта

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

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

2. Адреси для зауважень та пропозицій до проекту акта

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

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

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

електронна: cyber@dsszzi.gov.ua;

- Державної регуляторної служби України:

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

факс (044) 254-43-93;

електронна: inform@dkrp.gov.ua

3. Обраний спосіб оприлюднення проекту акта

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

4. Строк, протягом якого приймаються зауваження та пропозиції

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

Доопрацьований проект акта та аналіз його регуляторного впливу.

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

___.___ 2018 р.

Інформація щодо врахування зауважень Інтернет Асоціації України

Проект ПОСТАНОВИ КМУ **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**			
ПОРЯДОК **формування переліку об'єктів критичної інформаційної інфраструктури**			
Попередня редакція	**Зауваження ІнАУ**	**Враховано/відхилено**	**Нова редакція**
1. Цей Порядок визначає механізм формування переліку об'єктів критичної інформаційної інфраструктури України (далі – Перелік), а також основні засади організації діяльності суб'єктів забезпечення кібербезпеки критичної інфраструктури при його формуванні.	Після слів «суб'єктів забезпечення кібербезпеки» виключити слова «критичної інфраструктури», що відповідатиме розумінню поняття «суб'єкти забезпечення кібербезпеки», даного у статті 5 Закону України «Про основні засади забезпечення кібербезпеки України».	враховано	1. Цей Порядок визначає механізм формування переліку об'єктів критичної інформаційної інфраструктури України (далі – Перелік), а також основні засади організації діяльності суб'єктів забезпечення кібербезпеки при його формуванні.
суб'єкт критичної інформаційної інфраструктури – державний орган, підприємство, установа та організація, юридична та (або) фізична особа, якому (якій) на правах власності, оренди або на інших законних підставах належать інформаційні та інформаційно-телекомунікаційні системи, системи управління технологічними процесами, що функціонують задля забезпечення функціонування об'єктів критичної інфраструктури у штатному режимі у відповідній галузі або сфері;	вираз «інформаційні та інформаційно-телекомунікаційні системи» замінити на вираз «комунікаційні або технологічні системи». Також, у визначенні даного терміну не зовсім зрозуміло понятті «функціонування у штатному режимі». Визначення терміну «суб'єкт критичної інформаційної інфраструктури» доопрацювати, зокрема, зазначивши, що під дію даного визначення підпадають юридичні особи незалежно від форми власності.	враховано	суб'єкт (оператор) критичної інформаційної інфраструктури - державний орган, підприємство, установа або організація, юридична та/або фізична особа, який (яка) на правах власності, оренди або на інших законних підставах має право розпоряджатися об'єктом критичної інформаційної інфраструктури, що використовується для виконання життєво-важливих функцій або надання життєво-важливих послуг за призначенням у відповідних секторах (галузях) економіки або сферах діяльності;
3. До Переліку включаються об'єкти критичної інформаційної інфраструктури об'єктів критичної	викласти в такій редакції: «До Переліку включаються об'єкти критичної інформаційної	враховано	3. До Переліку включаються об'єкти критичної інформаційної інфраструктури тих

інфраструктури, які: провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами потенційно небезпечних технологій і виробництв.	інфраструктури об'єктів критичної інфраструктури, включених до Переліку об'єктів критичної інфраструктури».		інфраструктурних об'єктів, що включені до переліку об'єктів критичної інфраструктури.
4. Визначення необхідності включення об'єкта критичної інформаційної інфраструктури до Переліку здійснюється з урахуванням категорії:	у пункті 4 проекту визначитись з категорією «значущість», тобто, це обсяги, територіальність тощо.	Враховано	виключено
значущості об'єкта критичної інформаційної інфраструктури для правоохоронної сфери, національної безпеки і оборони України;	«значущості об'єкта критичної інформаційної інфраструктури для правоохоронних органів військових формувань, утворених відповідно до закону, та національної безпеки України».	Враховано	виключено
політичного значущості, яка виражається оцінкою можливого	виключити останній абзац, в якому зазначено, як категорію визначення	Враховано	виключено

нанесення втрат Україні у внутрішній і зовнішній політиці.	необхідності включення об'єкта критичної інфраструктури до Переліку, «політичну значущість, яка виражається оцінкою можливого нанесення втрат Україні у внутрішній і зовнішній політиці», як такий, що не узгоджується із метою Закону, а також із положеннями статей 4,6 Закону, якими, саме політичні інтереси держави не визначаються як об'єкт захисту в кіберпросторі. Частиною першою статті 4 Закону визначено, що об'єктами кібербезпеки, зокрема, є держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність, національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави. Зазначене положення Закону доповнюється статтями 1,5, 17 Конституції України, нормами Закону України «Про основи національної безпеки України», іншими актами законодавства		
5. Критерієм включення об'єкта критичної інформаційної інфраструктури до Переліку є порушення сталого функціонування об'єкта критичної інформаційної інфраструктури через здійснені на них кібератаки та кіберінциденти, що може спричинити:			5. Критерієм включення об'єкта критичної інформаційної інфраструктури до Переліку є порушення сталого функціонування об'єкта критичної інформаційної інфраструктури через здійснені на них кібератаки та кіберінциденти, що може спричинити:
негативний вплив на суспільно-	виключити «негативний вплив на	Відхилено	негативний вплив на суспільно-

політичну ситуацію в державі (Н6);	суспільно-політичну ситуацію в державі» В противному разі, необхідно розробити та зазначити про це в проекті постанови певні індикатори, які вказуватимуть на наявність зазначених критеріїв та їх вплив на кіберпростір.	зважаючи на роль комунікаційних систем для формування громадської думки, зокрема у ході виборів	політичну ситуацію в державі (Н6);
негативний вплив на імідж держави (Н7);	виключити «негативний вплив на імідж держави». В противному разі, необхідно розробити та зазначити про це в проекті постанови певні індикатори, які вказуватимуть на наявність зазначених критеріїв та їх вплив на кіберпростір.	Відхилено зважаючи на роль комунікаційних технологій для формування позитивного образу держави як усередині країни, так і на міжнародній арені.	негативний вплив на імідж держави (Н7);
6. Правила категоріювання об'єктів критичної інформаційної інфраструктури, а також переліки і показники критеріїв віднесення до об'єктів критичної інформаційної інфраструктури інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, які забезпечують управлінські, технологічні, виробничі, фінансово-економічні, інші процеси в рамках виконання функцій (повноважень) або здійснення видів діяльності суб'єктів критичної інфраструктури встановлюються Кабінетом Міністрів України.	з тексту проекту Порядку виключити положення, якими пропонується встановити додаткові повноваження Кабінету Міністрів України щодо встановлення правил категоріювання об'єктів критичної інформаційної інфраструктури, а також переліки і показники критеріїв віднесення до об'єктів критичної інформаційної інфраструктури інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, які забезпечують управлінські, технологічні, виробничі, фінансово-економічні, інші процеси в рамках виконання функцій (повноважень) або здійснення видів діяльності суб'єктів критичної інфраструктури.	Враховано	виключено

8. Відомості про об'єкт критичної інформаційної інфраструктури для внесення до Переліку подаються уповноваженими органами до Адміністрації Держспецзв'язку у паперовому та електронному вигляді за формою згідно з додатком.	У пункті 8 проекту Порядку запропоновано передбачити, що, для подання до Адміністрації Держспецзв'язку відомостей про об'єкт критичної інформаційної інфраструктури використовується лише електронна форма.	Взято до уваги і буде враховано частково при підготовці остаточної редакції. У разі підключення до СЕВ можна подавати або в електронному вигляді, або у паперовому	8. Відомості про об'єкт критичної інформаційної інфраструктури для внесення до Переліку подаються уповноваженими органами до Адміністрації Держспецзв'язку у паперовому та (або) електронному вигляді за формою згідно з додатком.
9. Відомості про об'єкти критичної інформаційної інфраструктури вносяться до державного реєстру об'єктів критичної інформаційної інфраструктури.	необхідно зазначити, хто (який державний орган) є власником державного реєстру об'єктів критичної інформаційної інфраструктури.	Відхилено пунктом 3 Порядку ведення Реєстру визначено, що Розпорядником Реєстру є Адміністрація Держспецзв'язку.	9. Відомості про об'єкти критичної інформаційної інфраструктури вносяться до державного реєстру об'єктів критичної інформаційної інфраструктури.
12. Галузеві переліки об'єктів критичної інформаційної інфраструктури формуються на підставі відомостей, отриманих від суб'єктів критичної інформаційної інфраструктури відповідних галузей або сфер діяльності.	пункти 11 та 12 проекту Порядку викласти в редакції: «Галузеві переліки об'єктів критичної інформаційної інфраструктури формуються та ведуться державним органом, який забезпечує формування і реалізацію державної політики у відповідній галузі або сфері діяльності, на підставі даних, об'єктів критичної інфраструктури, що знаходяться у його власності чи розпорядженні та відомостей, отриманих від інших суб'єктів критичної інформаційної інфраструктури відповідних галузей або сфер діяльності».	Враховано	8. Секторальні (галузеві) переліки об'єктів критичної інформаційної інфраструктури формуються та ведуться уповноваженими органами на підставі відомостей про об'єкти критичної інформаційної інфраструктури, що знаходяться у їх власності чи розпорядженні, та відомостей, отриманих від суб'єктів (операторів) критичної інформаційної інфраструктури.
15. Для формування галузевого переліку об'єктів критичної інформаційної			15. Для формування секторального (галузевого) переліку об'єктів

інфраструктури суб'єкти критичної інформаційної інфраструктури збирають та подають до уповноваженого органу відомості:			критичної інформаційної інфраструктури суб'єкти (оператори) критичної інформаційної інфраструктури збирають та подають до уповноваженого органу відомості:
щодо призначення і архітектури об'єкта критичної інформаційної інфраструктури, наявність доступу до телекомунікаційних мереж;	виключити необхідність подання інформації про відомості «щодо призначення і архітектури об'єкта критичної інформаційної інфраструктури, сервіси з управління, контролю або моніторингу, які здійснюються об'єктом критичної інформаційної інфраструктури», оскільки, частково, ці дані схожі з інформацією про «взаємодію об'єкта критичної інформаційної інфраструктури з іншими об'єктами критичної інформаційної інфраструктури», яка також буде надаватись з метою формування галузевого переліку.	Враховано	щодо назви (призначення) об'єкта критичної інформаційної інфраструктури, форми власності, наявність доступу до телекомунікаційних мереж;
17. Уповноважені органи подають відомості про об'єкт критичної інформаційної інфраструктури до Адміністрації Держспецзв'язку та здійснюють заходи щодо актуалізації відомостей, що містяться у Переліку, у разі:	передбачити обов'язковість заходів з ідентифікації осіб, які передають інформацію про об'єкти критичної інформаційної інфраструктури. Доповнити положеннями про персональну відповідальність осіб, винних у розголошені інформації стороннім особам з порушенням процедури та підстав надання інформації.	Відхилено Передача інформації здійснюється відповідно до порядку поводження з інформацією з обмеженим доступом	14. Уповноважені органи подають відомості про об'єкти критичної інформаційної інфраструктури до Адміністрації Держспецзв'язку у паперовому та електронному вигляді за формою згідно з додатком та здійснюють заходи щодо актуалізації відомостей, що містяться у Переліку, у разі: