Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

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

25.05.2018 № 05/02-1644

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

Щодо погодження проекту
постанови КМУ

Направляємо на погодження проект постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури», розроблений Адміністрацією Державної служби спеціального зв'язку та захисту інформації України на виконання вимог частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України».

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

Додатки:
1. Проект постанови Кабінету Міністрів України на 23 арк., тільки на адресу.
2. Пояснювальна записка до проекту постанови Кабінету Міністрів України на 3 арк., тільки на адресу.
3. Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України на 10 арк., тільки на адресу.
4. Повідомлення про оприлюднення проекту нормативно-правового акта на 1 арк., тільки на адресу.

Голова Служби Л.О. Євдоченко

виконавець Грошевий Р.А.
521-43-34

0.1

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 дня її опублікування.

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. Ці 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 Вимогах терміни вживаються у такому значенні:

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

Інші терміни вживаються у значенні, наведеному в 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 29.03.2006 № 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) Системи, порушення функціонування компонентів Системи тощо.

4. Кіберзахист ОКІ забезпечується впровадженням на ОКІІ сукупності організаційних та технічних заходів, а також засобів і методів захисту інформації.

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 відповідно до Переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації, затвердженого постановою Кабінету Міністрів України від 4 лютого 1998 № 121.

6. Кіберзахист об'єкта критичної інфраструктури забезпечується власником та/або керівником ОКІ відповідно до цих Вимог 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 цього документу 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.

Технічне завдання на створення комплексної системи захисту інформації ОКІІ підлягає погодженню з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (далі – Адміністрацією Держспецзв'язку).

У складі комплексної системи захисту інформації ОКІІ повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.

У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент проектування комплексної системи захисту інформації ОКІІ, відповідне оцінювання проводиться під час її державної експертизи комплексної системи захисту інформації ОКІІ в сфері технічного захисту інформації.

8. У випадку, якщо в ОКІІ не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вимоги цього документу повинні бути враховані під час створення (модернізації) системи інформаційної безпеки об'єкта критичної інфраструктури, а їх відповідність 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 загроз ОКІІ та ризиків, які викладаються в звіті за результатами оцінки ризиків в Системі. Методичною основою для оцінки ризиків в ОКІІ може слугувати стандарт ДСТУ ISO/IEC 27005.

Технічне завдання на створення системи інформаційної безпеки ОКІІ підлягає погодженню з Адміністрацією Держспецзв'язку.

Власник та/або керівник ОКІ організовує проведення незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури у порядку, який визначається Кабінетом Міністрів України.

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, у порядку встановленому Адміністрацією Держспецзв'язку.

10. З метою оперативного виявлення та реагування на кібератаки, моніторингу подій, які відносяться до мережевої безпеки, на ОКІІ державних органів влади, а також на ОКІІ підприємств, установ та організацій різних форм власності, перелік яких визначається Кабінетом Міністрів України, встановлюються засоби Системи кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури Держспецзв'язку, які взаємодіють з Центром реагування на кіберінциденти. Порядок встановлення та використання цих засобів визначається Адміністрацією Держспецзв'язку.

11. Для запобігання кібератакам державні органи можуть отримувати доступ до мережі Інтернет через Систему захищеного доступу державних органів до Інтернету (далі – СЗДІ) у порядку встановленому Адміністрацією Держспецзв'язку.

12. З метою забезпечення захищеного обміну та зберігання державних інформаційних ресурсів, підключення до СЗДІ, державні органи можуть використовувати засоби Національної телекомунікаційної мережі у встановленому Кабінетом Міністрів України порядку.

13. З метою забезпечення відмовостійкості компонентів ОКІІ, власник та/або керівник ОКІ забезпечує створення резервних копій своїх інформаційних ресурсів, для оперативного відновлення у разі їх пошкодження або знищення.

Органи державної влади для збереження резервних копій своїх інформаційних ресурсів використовують основний та резервний захищений дата-центр збереження інформації і відомостей державних інформаційних ресурсів Держспецзв'язку. Порядок використання ресурсів захищеного дата-центру збереження інформації і відомостей державних інформаційних ресурсів визначається Адміністрацією Держспецзв'язку.

14. 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 наведений у додатку до цих 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, повинні 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, керівними документами з питань інформаційної безпеки.

15. При відсутності можливості реалізації окремих заходів з кіберзахисту, наведених в додатку до цих Вимог, і/або неможливості їх застосування до окремих об'єктів захисту чи суб'єктів доступу, в 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 виключення окремих заходів з мінімального складу заходів із забезпечення кіберзахисту ОКІ.

При цьому в ході розробки організаційних і технічних заходів щодо забезпечення кіберзахисту ОКІ повинно бути обґрунтовано застосування компенсуючих заходів або виключення окремих заходів, а при проведенні незалежного аудиту ОКІ оцінена достатність і адекватність компенсуючих заходів, які застосовані для блокування (нейтралізації) загроз ОКІІ 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 повинно оформлюватись окремим документом за підписом власника та/або керівника ОКІ.

16. Центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування ОКІ, 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 ОКІІ використовувати такі конкретизовані вимоги з кіберзахисту.

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.

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.

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. ОКІ зобов'язаний розробити та затвердити політику управління ризиками інформаційної безпеки, самостійно визначивши підходи (методики) їх оцінювання та оброблення. Методичною основою для вибору методики може слугувати стандарт ДСТУ ISO/IEC 27005.

5. ОКІ зобов'язаний не рідше одного разу на рік 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 можуть слугувати 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. ОКІ зобов'язаний забезпечити розробку та підтримання в актуальному стані технічної, проектної тощо документації на комплексну систему захисту інформації (систему інформаційної безпеки) ОКІІ (в електронному та 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.

7. ОКІ зобов'язаний розробити та затвердити політику інформаційної безпеки в організації, яка:

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 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 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.

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

9. ОКІ зобов'язаний впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль обізнаності.

10. ОКІ зобов'язаний створити та підтримувати в актуальному стані перелік програмного та апаратного забезпечення, що використовується в ОКІІ (в електронному та 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. ОКІ зобов'язаний забезпечити ідентифікацію обладнання (наприклад, за IP-адресою, MAC-адресою тощо), що підключається до системи управління технологічними процесами, та вжити заходів, 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. ОКІ повинен забезпечувати захист журналів реєстрації подій компонентів ОКІІ від несанкціонованого доступу, модифікації або руйнування. ОКІ зобов'язаний зберігати електронні журнали реєстрації подій не менше ніж рік.

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.

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.

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. ОКІ зобов'язаний забезпечити надання доступу адміністраторам до компонентів ОКІІ 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 та Системою повинні бути встановлені засоби мережевого захисту, що реалізують щонайменше такі функції захисту:

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. ОКІ зобов'язаний 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. 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, ОКІ зобов'язаний 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 цього документу або конкретизованих вимог з кіберзахисту відповідної сфери регулювання, до якої відноситься ОКІ.

37. У випадку підключення системи управління технологічними процесами ОКІ до мережі Інтернет, повинна бути впроваджена система проактивного захисту від атак «нульового дня», виявлення зловмисного коду та шкідливого програмного забезпечення.

38. ОКІІ повинні отримувати доступ до глобальних мереж передачі даних, зокрема до мережі Інтернет, 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 Вимог, які він надає ОКІ.

Забезпечення доступності та відмовостійкості компонентів
та інформаційних ресурсів ОКІІ

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

періодичне створення резервних копій всіх даних ОКІІ, включаючи інформацію, яка зберігається в системі, технологічну інформацію компонентів системи та образів серверів системи, та їх відновлення у випадку втрати або пошкодження;

резервування програмних та апаратних компонентів системи 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) 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.

40. 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

41. 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.

42. 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.

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

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

Умови використання програмного та апаратного забезпечення

45. 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.

46. 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.

47. 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.

48. 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.

49. 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

50. Компоненти та/або інформація ОКІІ 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 Вимог, які він надає ОКІ.

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 інформації і відомостей державних інформаційних ресурсів Держспецзв'язку. Порядок використання ресурсів захищеного дата-центру збереження інформації і відомостей державних інформаційних ресурсів визначається Адміністрацією Держспецзв'язку.

51. Забороняється розміщувати компоненти та/або інформацію (дані) системи управління технологічними процесами ОКІ в сторонньому (не власному) центрі обробки даних.

52. 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.

53. Робочі місця адміністраторів та операторів системи управління технологічними процесами ОКІ не повинні бути підключені до інших систем ОКІ та зовнішніх систем та використовуватися для інших потреб.

54. ОКІ зобов'язаний мати схеми (креслення) розміщення обладнання структурованої кабельної системи та кабельних каналів ОКІІ, схеми підключення обладнання та мати таблиці маркування кабелів структурованої кабельної системи та кабельних з'єднань.

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 підприємств, установ та організацій до об'єктів критичної інфраструктури (далі – ОКІ).

2. У цьому документі терміни вживаються у такому значенні:

акт несанкціонованого втручання – діяння, що створило загрозу безпечному функціонуванню об'єкта критичної інфраструктури та призвело до одного або декількох з таких наслідків: порушило його неперервність і стійкість; створило негативні наслідки для життя і здоров'я людей, соціально-економічного розвитку держави, її обороноздатності та національної безпеки;

безпека об'єкта критичної інфраструктури – стан об'єкта критичної інфраструктури за якого забезпечено функціональність, безперервність роботи, цілісність й стійкість 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 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;

захист критичної інфраструктури – це всі види діяльності, спрямованої на забезпечення безпеки об'єктів критичної інфраструктури з метою запобігання виникненню загроз, ризиків або уразливості, мінімізації та ліквідації їхніх можливих наслідків;

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;

кризова ситуація – ситуація, що склалася на елементі об'єкта критичної інфраструктури або у взаємопов'язаних сферах внаслідок настання надзвичайної 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;

критична інфраструктура – сукупність об'єктів критичної інфраструктури;

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

рівень критичності – відносна міра важливості об'єкта критичної інфраструктури, що враховує вплив раптового припинення його функціонування або функціонального збою на безпеку постачання, забезпечення суспільства важливими товарами і послугами;

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;

сектор критичної інфраструктури – сукупність об'єктів критичної інфраструктури, що належать до одного сектору економіки;

стійкість об'єкта критичної інфраструктури – стан об'єкта критичної інфраструктури, за якого забезпечується його спроможність надійно функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після реалізації загроз будь-якого виду;

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

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

3. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи, 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, охорони здоров'я;

є аварійними та рятувальними службами, службами екстреної допомоги населенню;

включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

є об'єктами, що підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;

є об'єктами потенційно небезпечних технологій і виробництв.

4. Ступінь ризиків щодо діяльності об'єкта критичної інфраструктури, визначається Методикою оцінки ризиків на об'єктах критичної інфраструктури, яка затверджується Кабінетом Міністрів України.

5. Віднесення об'єктів до об'єктів критичної інфраструктури визначається за сукупністю критеріїв, що визначають їх важливість для реалізації життєво-важливих функцій та надання життєво-важливих послуг, свідчать про існування ризиків і загроз для них, можливість 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, а саме:

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

уразливості цих об'єктів, тяжкості настання можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода: здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); економіці (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного значення; обороноздатності; іміджу країни;

масштабності негативних наслідків для держави, які: вплинуть на діяльність стратегічно важливих об'єктів для кількох секторів економіки чи призведуть до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаються на діяльності ряду інших секторів;

тривалості ліквідації таких наслідків та дією подальшого негативного впливу на інші сектори держави;

впливу на функціонування суміжних секторів критичної інфраструктури.

6. Критерієм віднесення об'єктів до об'єктів критичної інфраструктури також є наслідки порушення сталого функціонування об'єкта критичної інфраструктури, які можуть спричинити:

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

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

негативний вплив на стан економічної безпеки держави (Н3);

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

негативний вплив на систему управління державою (Н5);

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

негативний вплив на імідж держави (Н7);

порушення сталого функціонування фінансової системи держави (Н8);

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

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

7. Для визначення рівня вимог до забезпечення захисту об'єктів критичної інфраструктури, здійснюється категоризація об'єктів критичної інфраструктури:

I категорія критичності – критично-важливі об'єкти – об'єкти, порушення функціонування яких призведе (може при звести) до великої кількості людських жертв, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру. Зазначені об'єкти включаються до переліку об'єктів критичної інфраструктури, щодо яких на державному рівні формуються вимоги щодо забезпечення їх захисту та регламентується використання державних ресурсів та сил;

II категорія критичності – життєво-важливі об'єкти, порушення функціонування яких призведе до кризової ситуації регіонального значення. Зазначені об'єкти включаються до переліку об'єктів критичної інфраструктури, щодо яких формуються вимоги розмежування завдань й повноважень органів державної влади та операторів критичної інфраструктури за забезпечення їх захисту та відновлення їх функціонування;

III категорія критичності – важливі об'єкти. Пріоритетом захисту такої інфраструктури є забезпечення швидкого відновлення функцій за рахунок диверсифікації та резервів. Відповідальність за стійкість функціонування об'єктів несуть оператори при встановлених законодавством вимогах щодо взаємодії із органами державної влади;

IV категорія критичності – необхідні об'єкти. Об'єкти інфраструктури, безпосередній захист яких є відповідальністю оператора, який має мати план реагування на кризову ситуацію.

Порядок віднесення до категорій критичності об'єктів критичної інфраструктури визначається Кабінетом Міністрів України.

8. Перелік об'єктів критичної інфраструктури формується на базі галузевих переліків об'єктів критичної інфраструктури, які надаються до

уповноваженого органу, який забезпечує формування і реалізацію державної політики у сфері захисту критичної інфраструктури уповноваженими органами, які забезпечують формування і реалізацію державної політики у відповідній галузі або сфері діяльності.

9. Галузеві переліки об'єктів критичної інфраструктури формуються та ведуться уповноваженими органами, які забезпечують формування і реалізацію державної політики у відповідній галузі або сфері діяльності та відповідно до законодавства у сфері захисту критичної інфраструктури визначає об'єкти критичної інфраструктури, що знаходяться у його власності чи розпорядженні.

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

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

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.

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

щодо призначення і складу об'єкта критичної інфраструктури, відомості, про відповідальних осіб;

відомості щодо 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;

можливі загрози щодо об'єкта критичної інфраструктури, наявні відомості, у т.ч. статистичні щодо інцидентів, які мали місце на об'єкті критичної інфраструктури.

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

зміни відомостей, визначених у пункті 13 цього документу;

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

зміни категорії значущості об'єкта критичної інфраструктури.

15. 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 переліку об'єктів критичної інфраструктури, у разі:

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

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

зміни категорії значущості об'єкта критичної інфраструктури.

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

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»

1. Обґрунтування необхідності прийняття законопроекту

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 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.

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 критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури.

На сьогодні, результатом кібератак є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування об'єктів критичної інфраструктури, які безпосередньо впливають на стан

національної безпеки і оборони. У зв'язку з цим, існуючі кіберзагрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки. Тому, важливим також є розроблення загальних вимог з кіберзахисту об'єктів критичної інфраструктури.

2. Мета і шляхи її досягнення

Метою 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.

3. Правові аспекти

Правовими підставами розроблення проекту постанови є вимоги частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» та завдання передбачене абзацом 3 пункту 1 Плану 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.

4. Фінансово-економічне обґрунтування

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

5. Позиція заінтересованих органів

Проект постанови потребує погодження 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.

6. Регіональний аспект

Проект постанови не стосується питання розвитку адміністративно-територіальних одиниць.

6[1]. Запобігання дискримінації

Проект постанови не містить положень, які мають ознаки дискримінації.

7. Запобігання корупції

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

8. Громадське обговорення

Проект постанови розміщено на офіційному веб-сайті Держспецзв'язку за адресою: www.dsszzi.gov.ua.

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

Проект постанови не стосується сфери наукової та науково-технічної діяльності, на розгляд до Наукового комітету Національної ради України з питань розвитку науки і технологій не надсилався.

9. Позиція соціальних партнерів

Проект постанови не стосується питань соціально-трудової сфери.

10. Оцінка регуляторного впливу

Проект постанови є регуляторним актом.

10[1]. Вплив реалізації акта на ринок праці

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

11. Прогноз результатів

Прийняття 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.

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

«18» 05 2018 року

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту Постанови Кабінету Міністрів України «Про затвердження 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 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.

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 критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури.

На сьогодні, результатом кібератак є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування

об'єктів критичної інфраструктури, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку з цим, існуючі кіберзагрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки. 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 призведе до неможливості визначення об'єктів критичної інфраструктури та, як наслідок, завадить запровадженню системного підходу до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури	Додаткових витрат не потребує
Альтернатива 2	Високі, оскільки прийняття Постанови дозволить визначити об'єкти критичної інфраструктури та, як наслідок, запровадити системний підхід до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури, зокрема шляхом висування до таких об'єктів вимог із кіберзахисту	Оцінити витрати з державного бюджету на реалізацію регуляторного акта буде можливо після визначення об'єктів критичної інфраструктури
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	Додаткових витрат не потребує

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні, оскільки такий підхід призведе до неможливості визначення об'єктів критичної інфраструктури, зокрема тих, що мають вплив на здоров'я та безпеку громадян, та висування до них вимог із	Додаткових витрат не потребує

	кіберзахисту, що може призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави	
Альтернатива 2	Високі, оскільки прийняття проекту Постанови дозволить визначити об'єкти критичної інфраструктури, зокрема ті, що мають вплив на здоров'я та безпеку громадян, та висунути до них вимоги із кіберзахисту, що може завадити виникненню надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави	Додаткових витрат не потребує
Альтернатива 3	Відсутні	Додаткових витрат не потребує

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	На поточний час оцінити кількість великих та середніх суб'єктів господарювання, що підпадають під дію регулювання неможливо		Дія регуляторного акта не буде розповсюджуватися на малі та мікро суб'єктів господарювання		–
Питома вага групи у загальній кількості, відсотків	Питома вага великих та середніх суб'єктів господарювання у загальній кількості може бути визначена тільки після віднесення об'єктів до об'єктів критичної інфраструктури, 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 призвести до виникнення надзвичайних	Додаткових витрат не потребує

	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	Оцінити витрати на реалізацію регуляторного акта буде можливо після визначення об'єктів критичної інфраструктури
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	Оцінити витрати на реалізацію регуляторного акта буде можливо після визначення об'єктів критичної інфраструктури

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	Додаткових витрат не потребує
Альтернатива 2	Оцінити витрати на реалізацію регуляторного акта буде можливо після оцінити визначення об'єктів критичної інфраструктури
Альтернатива 3	Оцінити витрати на реалізацію регуляторного акта буде можливо після оцінити визначення об'єктів критичної інфраструктури

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 вимог із кіберзахисту, що може завадити виникненню надзвичайних ситуацій техногенного характеру та/або негативного впливу на	Витрати на реалізацію регуляторного акта буде можливо оцінити після визначення об'єктів критичної інфраструктури	Проблема більше існувати не буде

	стан екологічної безпеки держави у випадку здійснення терористичних актів по відношенню до таких об'єктів		
Альтернатива 3	Відсутні	Витрати на реалізацію регуляторного акта буде можливо оцінити після визначення об'єктів критичної інфраструктури	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 порядок віднесення 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.

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:

– 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
«18» 05 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.

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

«18» травня 2018 р.