Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

24.04.2020 № 11/01/04-710 На № _____ від _____

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

Щодо погодження проєкту постанови
Кабінету Міністрів України

Відповідно до §§ 33 і 37, пункту 2 § 40 Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 18.07.2007 № 950, Адміністрація Держспецзв'язку надсилає на повторне погодження проєкт постанови Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури", який було погоджено Державною регуляторною службою України рішенням від 17.01.2020 № 24.

Просимо повторно погодити проєкт постанови у п'ятиденний термін у встановленому порядку.

Додатки:
1. Проєкт постанови на 8 арк., тільки на адресу.
2. Пояснювальна записка до проєкту постанови на 9 арк., тільки на адресу.
3. Аналіз регуляторного впливу проєкту постанови на 8 арк., тільки на адресу.
4. Повідомлення про оприлюднення проєкту нормативно-правового акта (скріншот) на 1 арк., тільки на адресу.

Голова Служби Валентин ПЕТРОВ

Олег Шикер 281 88 37

Проєкт

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2020 р. №

Київ

Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури

Відповідно до частини третьої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" Кабінет Міністрів України **постановляє:**

1. Затвердити такі, що додаються:

Вимоги щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

Порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

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

ведення переліку атестованих аудиторів інформаційної безпеки;

проведення узагальненого аналізу звітів незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

3. Власникам та/або керівникам об'єктів критичної інфраструктури:

організувати проведення не рідше ніж один раз на два роки незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

за результатами проведеного аудиту протягом 30 робочих днів з дати отримання від аудиторів звіту аудиту інформаційної безпеки, надсилати його до Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

Прем'єр-міністр України **Д. ШМИГАЛЬ**

Валентин ПЕТРОВ

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України
від 2020 р. №

ВИМОГИ
щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури

1. Ці Вимоги встановлюють основи проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, крім об'єктів критичної інфраструктури у банківській системі України.

2. Дія цих Вимог не поширюється на діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення.

3. У цих Вимогах терміни вживаються в такому значенні:

1) аудитор інформаційної безпеки (далі — аудитор) — фізична особа, яка підтвердила кваліфікаційну придатність для проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури відповідно до порядку атестації (переатестації) аудиторів інформаційної безпеки;

2) аудиторська фірма у сфері інформаційної безпеки (далі — аудиторська фірма) — юридична особа, яка провадить діяльність, пов'язану з аудитом інформаційної безпеки, на підставах та в порядку, що передбачені цими Вимогами, Порядком проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, затвердженим постановою Кабінету Міністрів України від 2020 р. № , національними та міжнародними стандартами аудиту інформаційної безпеки;

3) вразливість — нездатність комунікаційної або технологічної системи протистояти реалізації певної загрози чи сукупності загроз;

4) звіт за результатами незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (далі — звіт) — офіційний документ, який складається в установленому порядку за результатами проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури і містить якісну та/або кількісну оцінку ступеня відповідності стану інформаційної безпеки на об'єктах критичної інфраструктури встановленим вимогам національних та рекомендаціям міжнародних стандартів інформаційної безпеки. Звіт є документом, який містить інформацію з обмеженим доступом;

5) незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури (далі — незалежний аудит) — систематизований, незалежний і документований процес отримання оцінки стану інформаційної безпеки на об'єктах критичної інфраструктури та його відповідності встановленим вимогам національних стандартів і рекомендаціям міжнародних стандартів інформаційної безпеки;

6) ризик — ймовірність виникнення негативних наслідків від провадження діяльності та можливий розмір втрат від них, що вимірюється у кількісних та якісних показниках;

7) тестування на проникнення — метод оцінювання захищеності комунікаційної або технологічної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу).

Інші терміни вживаються у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки".

4. Незалежний аудит проводиться згідно з нормами законодавства, національних стандартів та з урахуванням міжнародних стандартів аудиту та специфіки об'єкта критичної інфраструктури.

5. Аудитор (аудиторська фірма) проводить незалежний аудит за умови дотримання цих Вимог.

6. Проведення незалежного аудиту є обов'язковим для об'єктів критичної інфраструктури.

7. Організація проведення незалежного аудиту покладається на власників та/або керівників об'єктів критичної інфраструктури.

8. Проводити незалежний аудит можуть аудитори (аудиторські фірми).

9. Під час незалежного аудиту обов'язково проводиться тестування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на проникнення з використанням програмо-апаратних засобів пошуку та аналізу вразливостей. Програма та методика такого тестування погоджуються власником та/або керівником об'єкта критичної інфраструктури до початку незалежного аудиту.

10. У випадках надзвичайних ситуацій на об'єкті критичної інфраструктури, що призвели або можуть призвести до людських або значних матеріальних втрат, власник та/або керівник об'єкта критичної інфраструктури повинен розглянути питання щодо проведення незалежного аудиту, а Адміністрація Держспецзв'язку може провести незалежний аудит та видати рекомендації, виконання яких є обов'язковим.

11. Власник та/або керівник об'єкта критичної інфраструктури немає права залучати до проведення незалежного аудиту інформаційної безпеки одного і того самого аудитора (аудиторську фірму) двічі поспіль.

12. Аудитор може залучати для проведення незалежного аудиту інших аудиторів за погодженням з власником та/або керівником об'єкта критичної інфраструктури. Група аудиторів повинна формуватися з урахуванням компетентностей, необхідних для проведення незалежного аудиту.

13. Звіт незалежного аудиту повинен бути конкретним, об'єктивним, повним, точним, записи щодо незалежного аудиту чітко сформульовані та зрозумілі. Формулювання огляду, аналізу та рекомендацій у звіті повинні тлумачитися однозначно.

Звіт незалежного аудиту повинен містити:

1) найменування виду аудиту із зазначенням назви об'єкта критичної інфраструктури, на якому проводиться аудит;

2) відомості про аудиторів: прізвище, ім'я, по батькові, посаду аудитора (членів групи аудиторів або аудиторської фірми);

3) дані про власника та/або керівника об'єкта критичної інфраструктури, працівників об'єкта критичної інфраструктури, які брали участь у незалежному аудиті та перелік об'єктів аудиту;

4) дату та місце проведення незалежного аудиту;

5) перелік національних та/або міжнародних стандартів інформаційної безпеки, на відповідність яким проведено незалежний аудит, та обґрунтування можливості застосування стандартів інформаційної безпеки до сфери діяльності об'єкта критичної інфраструктури;

6) застосовані процедури та методики проведення незалежного аудиту;

7) план-графік проведення незалежного аудиту;

8) результати проведення незалежного аудиту;

9) опис вразливостей, виявлених за результатами тестування на проникнення;

10) оцінка достатності і адекватності компенсуючих заходів, які застосовані для блокування (нейтралізації) загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та зменшення ризиків об'єкта критичної інфраструктури;

11) рекомендації щодо обробки (уникнення, зменшення, перекладання чи прийняття) ризиків.

Звіт незалежного аудиту підписується усіма аудиторами, які його проводили.

Аудитор (аудиторська фірма) надає власнику та/або керівнику об'єкта критичної інфраструктури звіт незалежного аудиту у двох примірниках, по одному для об'єкта критичної інфраструктури та для подання до Адміністрації Держспецзв'язку.

14. Звіт незалежного аудиту складається з двох частин:

1) огляду, що містить загальну інформацію про предмет проведення аудиту, зазначену у пунктах 1-7 пункту 13 цих Вимог та стислу оцінку поточної ситуації, основні (стратегічні) рекомендації із зазначенням пов'язаних прогнозованих ризиків, у тому числі наслідків реалізації певної загрози, визначення можливих видів і розмірів завданих збитків;

2) основної частини, що містить відомості, зазначені в підпунктах 8-11 пункту 13 цих Вимог, їх аналіз та детальні рекомендації.

15. Аудитор (аудиторська фірма) несе відповідальність за повноту, достовірність та об'єктивність відомостей, зазначених у звіті незалежного аудиту.

Валентин ПЕТРОВ

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2020 р. №

ПОРЯДОК
проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури

1. Цей Порядок визначає процедуру організації та проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, крім об'єктів критичної інфраструктури у банківській системі України.

Дія цього Порядку не поширюється на діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення.

2. У цьому Порядку під терміном "відомості незалежного аудиту" слід розуміти записи та іншу інформацію, отриману під час проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Інші терміни вживаються у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", у Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19.06.2019 № 518, та Вимогах щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 2020 р. № .

3. Метою проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (далі — незалежний аудит) є оцінка аудитором інформаційної безпеки відповідності стану інформаційної безпеки на об'єктах критичної інфраструктури встановленим вимогам національних та рекомендаціям міжнародних стандартів інформаційної безпеки, які регламентують порядок дотримання та забезпечення інформаційної безпеки.

4. Основними етапами проведення незалежного аудиту є:

1) організація проведення незалежного аудиту, що включає вибір аудитора інформаційної безпеки, визначення переліку національних та міжнародних стандартів, на відповідність яким буде проводитися незалежний аудит, переліку питань, які будуть перевірятися, визначення процедур і методик проведення незалежного аудиту;

2) підготовка та погодження плану-графіку проведення незалежного аудиту;

3) збір необхідних відомостей незалежного аудиту та їх аналіз;

4) підготовка та погодження звіту незалежного аудиту.

5. Між власником та/або керівником об'єкта критичної інфраструктури та аудитором інформаційної безпеки (далі – аудитор) або аудиторською фірмою у сфері інформаційної безпеки (далі – аудиторська фірма) укладається договір з проведення незалежного аудиту (далі — договір).

6. Відповідно до плану-графіку проведення незалежного аудиту аудитор (аудиторська фірма) надає власнику та/або керівнику об'єкта критичної інфраструктури звіт незалежного аудиту.

7. Для отримання відомостей незалежного аудиту аудитор (аудиторська фірма):

1) проводить інтерв'ю (анкетування) та спостереження за діями персоналу;

2) використовує загальне чи спеціалізоване аудиторське програмне забезпечення для аналізу вмісту файлів та файлів налаштувань програмного і програмно-апаратного забезпечення;

3) переглядає та аналізує налаштування комунікаційних та технологічних систем безпосередньо під час зустрічей з відповідальними співробітниками;

4) використовує попередні аудиторські звіти та аналізує системні журнали, журнали реєстрації подій та логи програмного і програмно-апаратного забезпечення (за наявності);

5) аналізує технічну документацію та документацію користувача, рекомендації постачальника компонентів комунікаційних та технологічних систем;

6) аналізує налаштування компонентів комунікаційних та технологічних систем;

7) узагальнює отримані фактичні дані про стан інформаційної безпеки на об'єкті критичної інфраструктури і перевіряє їх на відповідність вимогам національних стандартів та рекомендаціям міжнародних стандартів інформаційної безпеки.

8. Аудитори (аудиторські фірми) під час проведення незалежного аудиту зобов'язані:

1) дотримуватися вимог цього Порядку та інших нормативно-правових актів, національних та міжнародних стандартів аудиту;

2) повідомляти власникам та/або керівникам об'єкта критичної інфраструктури, уповноваженим ними особам про виявлені під час проведення незалежного аудиту вразливості комунікаційних та технологічних систем та/або критичних бізнес/операційних процесів;

3) не розголошувати та не використовувати у своїх інтересах або інтересах третіх осіб інформацію, отриману під час проведення незалежного аудиту.

9. Аудитор (аудиторська фірма) має право:

1) спільно із власником та/або керівником об'єкта критичної інфраструктури визначати процедури і методики проведення незалежного

аудиту, користуючись нормами законодавства, національних та міжнародних стандартів аудиту, відповідно до умов договору;

2) отримувати необхідні пояснення від власника та/або керівника і працівників об'єктів критичної інфраструктури, що перевіряються, в усній чи письмовій формі;

3) ознайомлюватись з необхідними документами з предмета перевірки, які знаходяться у власника та/або керівника об'єкта критичної інфраструктури. Звертатись за необхідною інформацією до третіх осіб, які мають у своєму розпорядженні документи стосовно питань перевірки, за погодженням з власником та/або керівником об'єкта критичної інфраструктури.

10. Власник та/або керівник об'єкта критичної інфраструктури має право самостійно обирати аудитора (аудиторську фірму) для проведення незалежного аудиту, крім випадків, передбачених пунктом 10 Вимог щодо проведення незалежного аудиту на об'єктах критичної інфраструктури.

11. Доступ аудиторам (аудиторським фірмам) до інформації з обмеженим доступом надається власником та/або керівником об'єкта критичної інфраструктури відповідно до законодавства.

12. За незаконне розголошення інформації, отриманої під час проведення незалежного аудиту, та неналежне виконання своїх обов'язків аудитор (аудиторська фірма) несе відповідальність відповідно до закону та договору, зазначеного у пункті 5 цього Порядку.

Валентин ПЕТРОВ

Прим. №__

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту постанови Кабінету Міністрів України
"Деякі питання проведення незалежного аудиту інформаційної безпеки
на об'єктах критичної інфраструктури"

1. Резюме

Проєкт постанови Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури" (далі – проєкт постанови) розроблено з метою визначення основних вимог та механізму впровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

2. Проблема, яка потребує розв'язання

Необхідність прийняття постанови зумовлена відсутністю відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури, що унеможливлює системний підхід до розв'язання проблеми захисту критичної інфраструктури на загальнодержавному рівні. Проблеми забезпечення належного рівня інформаційної безпеки на об'єктах критичної інфраструктури не можуть бути розв'язані без наявності систематизованого підходу до аналізу стану захисту інформації, який базувався би на реальних показниках, отриманих під час проведення незалежного аудиту інформаційної безпеки.

3. Суть проєкту акта

Проєктом постанови пропонується затвердити Вимоги щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та Порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

4. Вплив на бюджет

Реалізація постанови потребуватиме постійних витрат з державного бюджету України.

Реалізація постанови не потребує відкриття нової бюджетної програми та буде здійснюватися в межах видатків споживання загального фонду державного бюджету України, передбачених для кожного державного органу відповідно. Для цього державні органи, віднесені до об'єктів критичної інфраструктури, під час складання бюджетних запитів повинні передбачати кошти на проведення незалежного аудиту інформаційної безпеки.

Фінансово-економічні розрахунки до проєкту постанови додаються.

5. Позиція заінтересованих сторін

Проєкт постанови потребує консультацій із суб'єктами господарювання, у зв'язку з чим розміщений на офіційному вебсайті Держспецзв'язку (https://www.dsszzi.gov.ua).

Проєкт постанови матиме вплив на ключові інтереси заінтересованих сторін, про що зазначено в прогнозі впливу, що додається.

Проєкт постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери.

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

6. Прогноз впливу

Проєкт постанови за предметом правового регулювання впливає на інтереси суб'єктів господарювання та держави шляхом запровадження обов'язковості проведення періодичного незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Проєкт постанови не впливає на ринкове середовище, забезпечення прав та інтересів суб'єктів господарювання, громадян.

Реалізація постанови не впливатиме на розвиток регіонів, прав та інтересів територіальних громад, ринок праці, рівень зайнятості населення, громадське здоров'я, екологію та навколишнє природне середовище, інші сфери суспільних відносин.

7. Позиція заінтересованих органів

Проєкт постанови потребує погодження Міністерством цифрової трансформації України, Міністерством фінансів України, Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством внутрішніх справ України, Міністерством оборони України, Міністерством інфраструктури України, Міністерством енергетики та захисту довкілля України, Службою безпеки України, Службою зовнішньої розвідки України та Державною регуляторною службою України.

Проєкт постанови потребує проведення правової експертизи Мін'юстом.

8. Ризики та обмеження

У проєкті постанови немає положень, що порушують права та свободи, які гарантовані Конвенцією про захист прав людини і основоположних свобод.

У проєкті постанови немає положень, які порушують принцип забезпечення рівних прав та можливостей жінок і чоловіків.

У проєкті постанови немає норм, які можуть містити ризики вчинення корупційних правопорушень.

У проєкті постанови немає положень, які містять ознаки дискримінації. Громадська антикорупційна та громадська антидискримінаційна експертизи не проводилися.

9. Підстава розроблення проєкту акта

Проєкт постанови розроблено на виконання частини третьої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" щодо впровадження системи незалежного аудиту інформаційної безпеки та абзацу четвертого пункту 1 Плану організації підготовки проєктів актів, необхідних для забезпечення реалізації Закону України "Про основні засади забезпечення кібербезпеки України", схваленого на засіданні Кабінету Міністрів України 22 листопада 2017 року (протокол № 66).

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

24.04 2020 р.

ПРОГНОЗ ВПЛИВУ
реалізації акта на ключові інтереси заінтересованих сторін

1. Суть проєкту акта

Проєктом постанови пропонується затвердити вимоги щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

2. Вплив на ключові інтереси усіх заінтересованих сторін

Заінтересована сторона	Ключовий інтерес	Очікуваний (позитивний чи негативний) вплив на ключовий інтерес із зазначенням передбачуваної динаміки змін основних показників (у числовому або кількісному вимірі)		Пояснення (чому саме реалізація акта призведе до очікуваного впливу)
		Короткостроковий вплив (до року)	Середньостроковий вплив (більше року)	
Держава	Забезпечення існування систематизованого підходу до аналізу стану захисту інформації на об'єктах критичної інфраструктури, який буде базуватися на реальних показниках, отриманих під час проведення незалежного аудиту інформаційної безпеки	Приведення нормативно-правових актів у відповідність до вимог чинного законодавства України	Забезпечення існування систематизованого підходу до аналізу стану захисту інформації на об'єктах критичної інфраструктури	Прийняття постанови надасть можливість отримувати актуальну інформацію щодо стану інформаційної безпеки на об'єктах критичної інфраструктури держави шляхом проведення заходів аудиту інформаційної безпеки, дотримуватися принципів

Суб'єкти господарювання	Запровадження обов'язковості проведення періодичного незалежного аудиту інформаційної безпеки на підприємствах, в установах та організаціях, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури	Приведення нормативно-правових актів у відповідність до вимог чинного законодавства України	Забезпечення належного рівня кіберзахисту та кібероборони підприємств, установ та організацій, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури	плановості й системності аудиту інформаційної безпеки та гарантувати державні інтереси в зазначених галузях; у межах повноважень виявляти та запобігати виникненню порушень вимог законодавства у зазначеній сфері об'єктами критичної інфраструктури та забезпечувати інтереси суспільства, зокрема належну якість кіберзахисту та кібероборони

ФІНАНСОВО-ЕКОНОМІЧНІ РОЗРАХУНКИ ДО ПРОЄКТУ ПОСТАНОВИ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ

"Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури"

Рівень бюджету

Державний бюджет України.

Початок реалізації проєкту, період необхідний для його реалізації

Проєкт акта починає діяти після затвердження переліку об'єктів критичної інфраструктури.

Аналіз проблеми

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

Водночас Закон України "Про основні засади забезпечення кібербезпеки України" визначає, що до переліку 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.

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.

Так, протягом останніх 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 кібератак, 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 більше ніж 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго;

4) 06 грудня 2016 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, що 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 із Санкт-Петербурга здійснили DDOS-атаку на сайт Укрзалізниці, внаслідок чого протягом дня була повністю заблокована його робота. Атака була націлена на крадіжку даних про пассажироперевезення;

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

7) у першій половині дня 27 червня 2017 року розпочалася масова кібератака на український державний та комерційний сектор із застосування шкідливого програмного забезпечення – вірусу-шифрувальника файлів Petya Ransomware. Її жертвами стали інформаційно-телекомунікаційні системи "Укрпошти", аеропорту "Бориспіль", "Укренерго", ДТЕК, багатьох банків, ЗМІ, телеканалів, АЗС та інших компаній. Якщо порахувати збитки, за оцінками експертів Україна втратила близько 0.4% ВВП, що становить близько 10 мільярдів гривень.

У зв'язку з цим з урахуванням потреб національної безпеки і необхідності системного підходу до розв'язання проблеми на загальнодержавному рівні отримання відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Необхідність прийняття постанови зумовлена відсутністю відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури та, як наслідок, унеможливлює системний підхід до розв'язання проблеми захисту критичної інфраструктури на загальнодержавному рівні.

Проблеми забезпечення належного рівня інформаційної безпеки на об'єктах критичної інфраструктури не можуть бути розв'язані без існування систематизованого підходу до аналізу стану захисту інформації, який базувався би на реальних показниках, отриманих під час проведення незалежного аудиту інформаційної безпеки.

Основною ціллю проєкту постанови є створення правових засад для отримання об'єктивної інформації щодо стану інформаційної безпеки об'єктів

критичної інфраструктури шляхом проведення незалежного аудиту інформаційної безпеки.

Проведення періодичного незалежного аудиту інформаційної безпеки стане обов'язковим до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури.

Прийняття постанови дозволить значно підвищити рівень кіберзахисту об'єктів критичної інфраструктури, а також мінімізувати збитки за результатами кібератак.

Шляхи реалізації проєкту акта та очікувані результати реалізації проєкту

Розрахунки проводились на основі очікуваної кількості об'єктів критичної інфраструктури, які будуть включені до переліку об'єктів критичної інфраструктури після прийняття постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об'єктів критичної інфраструктури, внесення об'єктів критичної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування».

Цільовою аудиторією є підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури.

Оцінити витрати на реалізацію постанови буде можна після визначення об'єктів критичної інфраструктури. 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 НАТО в Україні на сьогодні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних. Понад чверть з них ідентифіковані як об'єкти підвищеної небезпеки.

Частку об'єктів критичної інфраструктури, які є державними органами можна буде визначити лише після затвердження переліку об'єктів критичної інфраструктури. Тому для розрахунків використовувалось прогнозована кількість об'єктів критичної інфраструктури, які є державними органами – 100.

Через відсутність даних щодо вартості послуг незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури України середня вартість проведення незалежного аудиту інформаційної безпеки розраховувалась для об'єкта, який має 50 мережевих ресурсів (середня вартість аудиту одного мережевого ресурсу в Україні — 20000 грн. Орієнтовні сумарні витрати становлять 100 000 тис. грн.

Реалізація проєкту акта не потребує відкриття нової бюджетної програми та буде здійснюватись в межах видатків споживання загального фонду державного бюджету України, передбачених для кожного державного органу відповідно. Для цього державні органи, віднесені до об'єктів критичної інфраструктури, під час складання бюджетних запитів повинні передбачати кошти на проведення незалежного аудиту інформаційної безпеки.

Зведені фінансово-економічні розрахунки до проєкту постанови Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури"

(тис. грн.)

Показники	2019 рік			щорічно починаючи з 2020 року		
	загальний фонд	спеціальний фонд	усього	загальний фонд	спеціальний фонд	усього
1. Витрати бюджету згідно з проєктом акта, усього (підпункт.1.1 + підпункт.1.2)	-	-	-	100 000,0	-	100 000,0
у тому числі:	-	-	-	-	-	-
1.1. Збільшення витрат (+), усього	-	-	-	100 000,0	-	100 000,0
з них: за бюджетними програмами (КПКВК або ТПКВКМБ/ ТКВБМС) та напрямами використання	-	-	-	-	-	-
1.2. Зменшення витрат (-), усього	-	-	-	-	-	-
з них: за бюджетними програмами (КПКВК або ТПКВКМБ/ТКВБМС) та напрямами використання	-	-	-	-	-	-
2. Надходження до бюджету згідно з проєктом акта, усього (підпункт 2.1 + підпункт 2.2)	-	-	-	-	-	-
у тому числі:	-	-	-	-	-	-
2.1. Збільшення надходжень (+), усього	-	-	-	-	-	-
з них за видами:	-	-	-	-	-	-
2.2. Зменшення надходжень (-), усього	-	-	-	-	-	-
з них за видами:	-	-	-	-	-	-
2.2. Зменшення надходжень (-), усього	-	-	-	-	-	-
з них за видами:	-	-	-	-	-	-
3. Витрати бюджету згідно з проєктом	-	-	-	-	-	-

акта, які враховані у бюджеті, усього						
з них: за бюджетними програмами (КПКВК або ТПКВКМБ/ ТКВКБМС) та напрямами використання	-	-	-	-	-	-
4. Надходження бюджету згідно з проєктом акта, які враховані у бюджеті, усього	-	-	-	-	-	-
з них за видами:	-	-	-	-	-	-
5. Загальна сума додаткових бюджетних коштів, необхідна згідно з проєктом акта (пункт 1 - пункт 2 - пункт 3 – пункт 4)	-	-	-	-	-	-
6. Джерела покриття загальної суми додаткових бюджетних коштів (пункт 5), необхідних згідно з проєктом акта, усього (підпункт 6.1 + підпункт 6.2)	-	-	-	-	-	-
у тому числі за рахунок:	-	-	-	-	-	-
6.1. Зменшення витрат бюджету (-), усього	-	-	-	-	-	-
з них: за бюджетними програмами (КПКВК або ТПКВКМБ/ ТКВКБМС) та напрямами використання	-	-	-	-	-	-
Збільшення надходжень бюджету (+), усього	-	-	-	-	-	-
з них за видами:	-	-	-	-	-	-

Директор Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку Олег БОНДАРЕНКО

Розширений пошук

- Про Держспецзв`язку
- Телекомунікації і користування радіочастотним ресурсом
- НОВИНИ
- Нормативно-правова база
- Регуляторна діяльність
- Міжнародна діяльність
- Діяльність
- Стандартизація, оцінка відповідності (сертифікація) та метрологія
- Оголошення
- Державні закупівлі
- Фінансово-економічна діяльність
- Ветеранська організація
- Зв'язки з громадськістю
- Галузева наука
- Консультаційний центр
- Контактна інформація
- Запобігання проявам корупції
- Прес-служба
- Вакансії
- Доступ до публічної інформації
- Звернення громадян
- Відкриті дані

14 квітня 2020

Повідомлення про оприлюднення
проекту постанови Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»

1. Стислий виклад змісту проекту акта

Проект постанови Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури" розроблено на виконання частини третьої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" щодо впровадження системи незалежного аудиту інформаційної безпеки та абзацу четвертого пункту 1 Плану організації підготовки проектів актів, необхідних для забезпечення реалізації Закону України "Про основні засади забезпечення кібербезпеки України", схваленого на засіданні Кабінету Міністрів України 22 листопада 2017 року (протокол № 66).

Документ визначає основні вимоги та механізм впровадження незалежного аудиту інформаційної безпеки на об'єктах 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) 281-88-51;

електронна: info@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 «Оприлюднення проектів регуляторних актів» 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 Держспецзв'язку Валентин Петров
Офіційна сторінка Держспецзв'язку
Офіційний твіттер Держспецзв'язку

Допоможи нам стати кращими
Повідом на new@dsszzi.gov.ua
Пряма лінія зв'язку з Головою Служби

CERT-UA
Цифрова грамотність держслужбовців

Аналіз регуляторного впливу

проєкту постанови Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури"

1. Визначення проблеми

Відповідно до частини третьої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" Адміністрацією Держспецзв'язку розроблено проєкт постанови Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури" (далі – проєкт постанови).

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії їм та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для вчинення терористичних актів.

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

Так, протягом останніх 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 кібератак, 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 більше ніж 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго;

4) 6 грудня 2016 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, що 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 із Санкт-Петербурга здійснили DDOS-атаку на сайт Укрзалізниці,

внаслідок чого протягом дня була повністю заблокована його робота. Атака була націлена на крадіжку даних про пассажироперевезення;

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

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

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 з урахуванням потреб національної безпеки і необхідності системного підходу до розв'язання проблеми на загальнодержавному рівні отримання відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Необхідність прийняття постанови зумовлена відсутністю відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури та, як наслідок, унеможливлює системний підхід до розв'язання проблеми захисту критичної інфраструктури на загальнодержавному рівні.

Проблеми забезпечення належного рівня інформаційної безпеки на об'єктах критичної інфраструктури не можуть бути розв'язані без існування систематизованого підходу до аналізу стану захисту інформації, який базувався би на реальних показниках, отриманих під час проведення незалежного аудиту інформаційної безпеки.

Метою проєкту постанови є визначення основних вимог та механізму впровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Основні групи (підгрупи), на які проблема впливає:

Групи (підгрупи)	Так	Ні
Громадяни		+
Держава	+	
Суб'єкти господарювання,	+	
У тому числі суб'єкти малого підприємництва	+	

Проблема не може бути розв'язана за допомогою ринкових механізмів, оскільки на сьогодні відсутні вимоги щодо передачі інформації стосовно стану інформаційної безпеки об'єктами критичної інфраструктури державі.

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

2. Цілі державного регулювання

Основною ціллю проєкту постанови є створення правових засад отримання об'єктивної інформації щодо стану інформаційної безпеки об'єктів критичної інфраструктури шляхом проведення незалежного аудиту інформаційної безпеки.

Проведення періодичного незалежного аудиту інформаційної безпеки стане обов'язковим до виконання підприємствами, установами та організаціями, які згідно до законодавства віднесені до об'єктів критичної інфраструктури.

3. Визначення та оцінка альтернативних способів досягнення цілей

3.1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Збереження чинного законодавства, що призведе до відсутності об'єктивної інформації щодо стану інформаційної безпеки на об'єктах критичної інфраструктури та до відсутності (неадекватності) вимог з кіберзахисту, що поставить під загрозу населення, стале функціонування цих об'єктів та існування держави як інституту в цілому. Такий спосіб є неприйнятним та не відповідає вимогам Закону. Це не забезпечить досягнення поставленої цілі регулювання.
Альтернатива 2	Прийняття проєкту постанови Кабінету Міністрів України

3.2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	**Вигоди**	**Витрати**
Альтернатива 1	**Відсутні** (такий підхід призведе до відсутності об'єктивної інформації щодо стану інформаційної безпеки на об'єктах критичної інфраструктури держави та, як наслідок, унеможливлює системний підхід до розв'язання проблеми захисту критичної інфраструктури на загальнодержавному рівні)	Додаткових витрат не потребує

Альтернатива 2	**Висока** (надасть можливість отримувати актуальну інформацію щодо стану інформаційної безпеки на об'єктах критичної інфраструктури держави шляхом проведення заходів аудиту інформаційної безпеки, дотримуватися принципів плановості й системності аудиту інформаційної безпеки та гарантувати державні інтереси в зазначених галузях; у межах повноважень виявляти та запобігати виникненню порушень вимог законодавства у зазначеній сфері об'єктами критичної інфраструктури та забезпечувати інтереси суспільства, зокрема належної якості кіберзахисту та кібероборони)	Оцінити витрати з державного бюджету на реалізацію регуляторного акта буде можна після визначення об'єктів критичної інфраструктури.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	Відповідно до Зеленої книги з питань захисту критичної інфраструктури в Україні, підготовленої Національним інститутом стратегічних досліджень із залученням українських та зарубіжних експертів, і за підтримки Офісу зв'язку НАТО в Україні на сьогодні в Україні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних				0 %
Питома вага групи у загальній кількості, відсотків	Питома вага великих, середніх, малих та мікро суб'єктів господарювання у загальній кількості може бути визначена тільки після віднесення об'єктів до об'єктів критичної інфраструктури, 100				100 %

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає (процедура проведення планових заходів аудиту ІБ не зможе застосуватися у зв'язку з невідповідністю вимог її проведення чинному законодавству, призведе до відсутності (висування неадекватних) вимог із кіберзахисту, що може призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави у випадку здійснення терористичних актів по відношенню до таких об'єктів)	Додаткових витрат не потребує
Альтернатива 2	Високі (узгодження інтересів бізнесу та держави, чіткий порядок та плановість проведення заходів аудиту ІБ Адміністрації Держспецзв'язку)	Оцінити витрати на реалізацію регуляторного акта неможливо через відсутність переліку об'єктів критичної інфраструктури держави. Орієнтовні щорічні витрати — 100 000 тис. грн. *

* вартість є орієнтовною. Оцінити витрати на реалізацію регуляторного акта буде можна після визначення об'єктів критичної інфраструктури. 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 на сьогодні в Україні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних. Через відсутність даних щодо вартості послуг незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури України середня вартість проведення незалежного аудиту інформаційної безпеки розраховувалась для об'єкта, який має 50 мережевих ресурсів (середня вартість аудиту одного мережевого ресурсу в Україні — 20 тис. грн. Орієнтовні сумарні витрати становлять 100 млн грн.

3.3. Сумарні витрати за альтернативами

Вид альтернативи	Сума витрат, гривень
Альтернатива 1	Додаткових витрат не потребує
Альтернатива 2	Оцінити витрати з державного бюджету на реалізацію регуляторного акта буде можна після визначення об'єктів критичної інфраструктури. Орієнтовні сумарні витрати становлять 100 000 тис. грн.

4. Вибір найбільш оптимального альтернативного способу досягнення цілей

Враховуючи вищенаведені позитивні та негативні сторони альтернативних способів досягнення мети, доцільно прийняти розроблений проєкт постанови. 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	Зазначений спосіб повністю відповідає вимогам сучасності, є найбільш доцільним та дасть змогу врегулювати проведення заходів аудиту інформаційної безпеки на об'єктах критичної інфраструктури держави

Вид альтернативи	Вигоди (підсумок)	Витрати (Підсумок)	Обґрунтування альтернативи
Альтернатива 1	Немає	Додаткових витрат не потребує	Проблема продовжує існувати
Альтернатива 2	Надасть можливість отримувати актуальну інформацію щодо стану інформаційної безпеки на об'єктах критичної інфраструктури держави шляхом вжиття заходів аудиту інформаційної безпеки, дотримуватися принципів плановості й системності аудиту інформаційної безпеки та гарантувати державні інтереси в зазначених галузях; у межах повноважень виявляти та запобігати виникненню порушень вимог законодавства у зазначеній сфері об'єктами критичної інфраструктури та забезпечувати інтереси суспільства, зокрема належної якості кіберзахисту та кібероборони	Оцінити витрати з державного бюджету та витрати суб'єктів господарювання на реалізацію регуляторного акта буде можна після визначення переліку об'єктів критичної інфраструктури. Орієнтовні щорічні витрати — 100 000 тис. грн. *	Проблема більше існувати не буде

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

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

Адміністрацією Держспецзв'язку підготовлено проєкт постанови, яким пропонується затвердити вимоги щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, що визначає:

обов'язковість проведення періодичного незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

вимоги до організаційних заходів та порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

відповідальність відповідних сторін при проведенні незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Для досягнення цієї цілі проєктом постанови передбачається:

затвердити вимоги щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

затвердити порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Заходи, що пропонуються для розв'язання проблеми:

погодити проєкт постанови з Міністерством оборони України, Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством фінансів України, Міністерством внутрішніх справ України, Міністерством інфраструктури України, Міністерством енергетики та захисту довкілля України, Міністерством цифрової трансформації України, Службою безпеки України та Службою зовнішньої розвідки України.

надіслати проєкт постанови на правову експертизу до Міністерства юстиції України;

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

Реалізація положень проєкту постанови:

Дозволить отримувати актуальну інформацію щодо стану інформаційної безпеки на об'єктах критичної інфраструктури, визначити об'єкти критичної інформаційної інфраструктури, які мають першочергово (пріоритетно) захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки.

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

6. 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

Оцінити витрати з державного бюджету на реалізацію регуляторного акта буде можна після визначення об'єктів критичної інфраструктури.

Питома вага суб'єктів малого підприємництва (малих та мікропідприємств разом) у загальній кількості суб'єктів господарювання, на яких поширюється регулювання, може бути визначена тільки після віднесення об'єктів до об'єктів критичної інфраструктури, тому розрахунок витрат на запровадження державного регулювання для суб'єктів малого підприємництва (Тест малого підприємництва) не проводився.

7. Обгрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується.

Строк набрання чинності регуляторним актом настає з дня затвердження переліку об'єктів критичної інфраструктури.

8. Визначення показників результативності дії регуляторного акта

Прогнозні значення показників результативності регуляторного акта будуть встановлюватися після набрання ним чинності.

Прогнозними значеннями показників результативності регуляторного акта є:

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

розмір коштів і час, що витрачатимуться суб'єктами господарювання та/або фізичними особами, пов'язаними з виконанням вимог акта, оцінити неможливо до затвердження переліку об'єктів критичної інфраструктури. Додаткові витрати від суб'єктів господарювання, пов'язані з виконанням вимог акта, – орієнтовно 100 000 тис. грн;

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

кількість порушень, виявлених підчас проведення аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

кількість наданих рекомендацій щодо підвищення рівня захищеності;

оцінка рівня кіберзахисту (кіберзагрози) за результатами проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

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

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

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

Базове відстеження результативності регуляторного акта буде здійснюватися через один рік після набрання чинності цим регуляторним актом

шляхом збирання статистичних даних, одержання пропозицій до нього, їх аналізу.

Повторне відстеження результативності регуляторного акта буде 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
24 04 2020 року

Валентин ПЕТРОВ