



**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

08.09.2021 № 11/01/02 - 1532

На № _____ від _____

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

В Адміністрації Держспецзв'язку опрацьовано рішення про відмову в погодженні проекту регуляторного акта від 28.07.2021 № 350, в частині підготовки аналізу регуляторного впливу проекту постанови Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури" з урахуванням вимог Методики проведення аналізу регуляторного впливу регуляторного акта, затвердженої постановою Кабінету Міністрів України від 11.03.2004 (із змінами).

Ураховуючи зазначене, керуючись § 37 Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 18.07.2007 № 950, Адміністрація Держспецзв'язку надсилає на повторне погодження проект постанови Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури".

- Додатки: 1. Проект постанови на 8 арк., тільки на адресу.
2. Пояснювальна записка до проекту постанови на 9 арк., тільки на адресу.
3. Аналіз регуляторного впливу проекту постанови на 10 арк., тільки на адресу.
4. Повідомлення про оприлюднення проекту нормативно-правового акта (скріншот) на 1 арк., тільки на адресу.

Голова Служби

Юрій ЩИГОЛЬ



КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від

2021 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 забезпечити:

ведення переліку атестованих аудиторів інформаційної безпеки;

проведення узагальненого аналізу звітів незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та інформування Ради національної безпеки і оборони України про стан інформаційної безпеки на об'єктах критичної інфраструктури.

3. Власникам та/або керівникам об'єктів критичної інфраструктури організувати проведення незалежного аудиту інформаційної безпеки з урахуванням встановлених категорій критичності об'єктів критичної інфраструктури:

для об'єктів I та II категорій критичності – не рідше ніж один раз на два роки;

для об'єктів III та IV категорій критичності – не рідше ніж один раз на три роки.

4. За результатами проведеного аудиту власникам та/або керівникам об'єктів критичної інфраструктури протягом 30 робочих днів з дати отримання від аудиторів звіту аудиту інформаційної безпеки копію звіту надіслати до Адміністрації Державної служби спеціального зв'язку та захисту інформації.

Прем'єр-міністр України

Д. ШМИГАЛЬ

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 або юридична особа, яка пройшла атестацію відповідно до порядку, встановленого Адміністрацією Держспецзв'язку, та дані про яку внесені до переліку аудиторів;

2) вразливість – слабкість ресурсу системи управління інформаційною безпекою або заходів безпеки, якою можуть скористатися одна чи більше загроз;

3) звіт за результатами незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (далі – звіт) – офіційний документ, який складається аудитором за результатами проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури і містить відомості щодо ступеня відповідності стану інформаційної безпеки на об'єкті критичної інфраструктури вимогам законодавства та національних стандартів, а також рекомендаціям міжнародних стандартів інформаційної безпеки. Звіт може містити інформацію з обмеженим доступом;

4) 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, який базується на вимогах законодавства, національних стандартів і рекомендаціях міжнародних стандартів інформаційної безпеки;

5) перелік атестованих аудиторів – список, який містить інформацію щодо аудиторів інформаційної безпеки об'єктів критичної інфраструктури, які мають право проводити аудит інформаційної безпеки на об'єктах критичної інфраструктури;

6) ризик – ефект невизначеності щодо досягнення цілей;

7) тестування на проникнення – метод оцінювання захищеності комунікаційної або технологічної системи чи мережі шляхом часткового імітування дій зовнішніх злоумисників 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 Кодексі цивільного захисту України, Законах України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки», «Про основні засади забезпечення кібербезпеки України», постанові Кабінету Міністрів України від 09 жовтня 2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» (Офіційний вісник України, 2020 р., № 84, ст. 2709), та Порядку віднесення об'єктів до об'єктів критичної інфраструктури, затвердженому постановою Кабінету Міністрів України від 09 жовтня 2020 р. № 1109 (Офіційний вісник України, 2020 р., № 93, ст. 2994).

4. Незалежний аудит проводиться відповідно до умов договору, укладеного між власником та/або керівником об'єкта критичної інфраструктури і аудитором, норм законодавства та вимог національних стандартів, а також з урахуванням рекомендацій міжнародних стандартів аудиту інформаційної безпеки.

5. Аудитор 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 мають право аудитори, які в установленому порядку внесені до переліку атестованих аудиторів інформаційної безпеки.

9. Під час незалежного аудиту проводиться тестування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на проникнення з використанням спеціалізованих ліцензійних програмо-апаратних засобів пошуку та аналізу вразливостей. Програма та методика такого тестування розробляються з урахуванням безпечного режиму функціонування об'єкта критичної інфраструктури та погоджуються власником та/або керівником об'єкта критичної інфраструктури до початку проведення незалежного аудиту.

10. У випадках настання надзвичайних ситуацій на об'єкті критичної інфраструктури, що призвели до порушення сталого функціонування об'єкта критичної інфраструктури, власник та/або керівник об'єкта критичної інфраструктури повинен після виконання першочергових заходів з мінімізації наслідків надзвичайної ситуації організувати проведення позачергового незалежного аудиту.

11. Власник та/або керівник об'єкта критичної інфраструктури не має права залучати до проведення незалежного аудиту інформаційної безпеки одного і того самого аудитора двічі поспіль.

12. За погодженням з власником та/або керівником об'єкта критичної інфраструктури аудитор може залучати до проведення незалежного аудиту інших аудиторів, відомості про яких занесені до переліку атестованих аудиторів інформаційної безпеки.

До залучених аудиторів застосовуються всі правила, передбачені цими Вимогами, Порядком проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

13. Інформація у звіті незалежного аудиту, формулювання висновків, аналізу та рекомендацій повинні тлумачитися однозначно. Звіт незалежного аудиту повинен містити інформацію згідно з умовами договору, а також:

1) відомості про аудитора (аудиторів): прізвище, власне ім'я, по батькові (за потреби) та посада;

2) відомості про власника та/або керівника об'єкта критичної інфраструктури, працівників об'єкта критичної інфраструктури, які брали участь у незалежному аудиті (прізвище, власне ім'я, по батькові (за потреби), посада), а також перелік об'єктів аудиту;

3) відомості про строки та місце проведення незалежного аудиту;

4) перелік національних та/або міжнародних стандартів інформаційної безпеки, на основі яких проведено незалежний аудит, та обґрунтування можливості застосування переліку вимог із стандартів інформаційної безпеки до сфери діяльності об'єкта критичної інфраструктури;

5) відомості про застосовані процедури та методики проведення незалежного аудиту;

6) програму проведення незалежного аудиту;

7) результати проведення незалежного аудиту;

8) опис та класифікацію вразливостей, виявлених за результатами тестування на проникнення;

9) опис заходів, які рекомендується застосувати для мінімізації загроз, та опис ризиків інформаційної безпеки об'єкта критичної інфраструктури;

10) рекомендації щодо обробки (уникнення, зменшення, перекладання чи прийняття) ризиків інформаційної безпеки (за наявності).

Аудитор надає власнику та/або керівнику об'єкта критичної інфраструктури звіт незалежного аудиту, підписаний усіма аудиторами, що його проводили.

14. Звіт незалежного аудиту складається з двох частин:

1) огляду, що містить загальну інформацію про цілі та предмет проведення аудиту, яка зазначена у підпунктах 1 – 6 пункту 13 цих Вимог, та стислу оцінку стану інформаційної безпеки;

2) основної частини, що містить відомості, зазначені в підпунктах 7 – 10 пункту 13 цих Вимог, їх аналіз та детальні рекомендації.

15. Аудитор несе відповідальність за конфіденційність, повноту, достовірність, об'єктивність відомостей, зазначених у звіті, а також за інші зобов'язання згідно з умовами договору.

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 інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 (Офіційний вісник України, 2019 р., № 50, ст. 1697), постанові Кабінету Міністрів України від 09 жовтня 2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» (Офіційний вісник України, 2020 р., № 84, ст. 2709), Порядку віднесення об'єктів до об'єктів критичної інфраструктури, затвердженому постановою Кабінету Міністрів України від 09 жовтня 2020 р. № 1109 (Офіційний вісник України, 2020 р., № 93, ст. 2994), та Вимогах щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 2021 р. № (Офіційний вісник України, 2021 р., № , ст.).

3. Метою проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (далі – незалежний аудит) є оцінка аудитором інформаційної безпеки стану інформаційної безпеки на об'єктах критичної інфраструктури, що має відповідати вимогам законодавства, національних стандартів та рекомендаціям міжнародних стандартів інформаційної безпеки.

4. Основними етапами проведення незалежного аудиту є:

1) організація проведення незалежного аудиту, що передбачає вибір аудитора інформаційної безпеки (далі – аудитор), визначення переліку національних та міжнародних стандартів інформаційної безпеки, на основі яких буде проводитися незалежний аудит, переліку питань, які будуть перевірятися, визначення процедур і методик проведення незалежного аудиту;

- 2) підготовка аудитором програми проведення незалежного аудиту та її погодження з власником та/або керівником об'єкта критичної інфраструктури;
- 3) збір необхідних відомостей незалежного аудиту та їх аналіз;
- 4) підготовка звіту незалежного аудиту.

5. Між власником та/або керівником об'єкта критичної інфраструктури та аудитором укладається договір з проведення аудиту інформаційної безпеки (далі – договір) та угода про нерозголошення конфіденційної інформації.

6. Враховуючи особливості об'єкта критичної інфраструктури, аудитор використовує критерії оцінки захищеності інформації, передбачені національними або міжнародними стандартами з інформаційної безпеки та узгоджені з власником та/або керівником об'єкта критичної інфраструктури.».

7. Для отримання відомостей незалежного аудиту аудитор:

1) використовує попередні звіти незалежного аудиту та аналізує системні журнали, журнали реєстрації подій програмного і програмно-апаратного забезпечення (за наявності);

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

3) використовує загальне чи спеціалізоване ліцензійне програмне забезпечення для пошуку вразливостей в комунікаційних та/або технологічних системах;

4) аналізує технічну документацію та документацію користувача, рекомендації постачальника компонентів комунікаційних та технологічних систем (за наявності);

5) аналізує налаштування компонентів комунікаційних і технологічних систем;

6) узагальнює отримані фактичні дані про стан інформаційної безпеки на об'єкті критичної інфраструктури і перевіряє їх на відповідність вимогам законодавства, національних стандартів, а також рекомендаціям міжнародних стандартів інформаційної безпеки.

8. Аудитори під час проведення незалежного аудиту зобов'язані:

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

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, а також надавати рекомендації щодо їх усунення та рекомендації щодо компенсуючих заходів мінімізації впливу вразливостей;

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

9. Аудитор має право:

1) спільно із власником та/або керівником об'єкта критичної інфраструктури визначати процедури і методики проведення незалежного аудиту, користуючись нормами законодавства, національних і міжнародних стандартів аудиту інформаційної безпеки;

2) отримувати від власника та/або керівника, а також працівників об'єкта критичної інфраструктури необхідну інформацію, що стосується незалежного аудиту, в усній чи письмовій формі;

3) ознайомлюватися з необхідними документами, що стосуються питань перевірки, які знаходяться у власника та/або керівника об'єкта критичної інфраструктури. Звертатися 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 з переліку атестованих аудиторів інформаційної безпеки для проведення незалежного аудиту.

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

12. За розголошення інформації з обмеженим доступом, отриманої під час проведення незалежного аудиту, та неналежне виконання своїх обов'язків аудитор несе відповідальність відповідно до закону.

ПОЯСНЮВАЛЬНА ЗАПИСКА

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

1. Мета

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

2. Обґрунтування необхідності прийняття акта

Проект 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).

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

3. Основні положення проєкту акта

Проектом 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. Правові аспекти

У цій сфері правового регулювання діють такі основні нормативно-правові акти:

Закон України «Про інформацію»;

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

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

Закон України «Про основні засади забезпечення кібербезпеки України»;

постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;

постанова Кабінету Міністрів України від 09 жовтня 2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури»;

постанова Кабінету Міністрів України від 09 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури».

5. Фінансово-економічне обґрунтування

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 проекту постанови додаються.

6. Позиція заінтересованих сторін

Проект постанови 19.03.2021 та 01.06.2021 було розміщено на офіційному вебсайті Держспецзв'язку (<https://cpr.gov.ua>) для проведення консультацій з громадськістю. Зауваження і пропозиції, отримані від Української асоціації операторів зв'язку “Телас”, ПАТ “Укртелеком” та Інтернет Асоціації України, враховано частково (№№ 11/01/01-878 від 19.05.2021, 11/01/01-879 від 19.05.2021, 11/01/01-782 від 29.04.2021, 11/01/02-1115 від 24.06.2021).

Проект постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери, прав осіб з інвалідністю, функціонування і застосування української мови як державної, тому не потребує погодження з уповноваженими представниками всеукраїнських асоціацій органів місцевого самоврядування чи відповідних органів місцевого самоврядування, уповноважених представників всеукраїнських профспілок, їх об'єднань та всеукраїнських об'єднань організацій роботодавців, Уповноваженим Президента України з прав людей з інвалідністю, Урядовим уповноваженим з прав осіб з інвалідністю та всеукраїнськими громадськими організаціями осіб з інвалідністю, їх спілками, Уповноваженим із захисту державної мови.

Проект постанови не стосується сфери наукової та науково-технічної діяльності, тому не потребує погодження з Науковим комітетом Національної ради з питань розвитку науки і технологій.

Проект постанови погоджено без зауважень Міністерством фінансів України, Міністерством інфраструктури України, Міністерством енергетики України та Міністерством захисту довкілля та природних ресурсів України.

Проект постанови погоджено із зауваженнями Міністерством оборони України, Міністерством внутрішніх справ України, Міністерством розвитку

економіки, торгівлі та сільського господарства України, Службою зовнішньої розвідки України та Службою безпеки України, які було частково враховано в проєкті постанови.

З метою врегулювання розбіжностей проведено узгоджувальні процедури, зокрема з представниками Міністерства оборони України проведено робочу нараду.

Проєкт постанови потребує погодження Державною регуляторною службою України, проведення цифрової експертизи Міністерством цифрової трансформації України та правової експертизи Міністерством юстиції України.

У зв'язку з висновком антикорупційної експертизи, підготовленим Національним агентством з питань запобігання корупції, доопрацьований проєкт постанови потребує проведення повторної антикорупційної експертизи Національним агентством з питань запобігання корупції.

7. Оцінка відповідності

У проєкті постанови немає положень, що стосуються зобов'язань України у сфері європейської інтеграції.

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 впливають на забезпечення рівних прав та можливостей жінок і чоловіків.

У проєкті постанови немає норм, які містять ризики вчинення корупційних правопорушень та правопорушень, пов'язаних з корупцією.

У проєкті постанови немає положень, які створюють підстави для дискримінації.

Національним агентством з питань запобігання корупції проведено антикорупційну експертизу, висновок якої надіслано листом від 05.10.2020 № 21-03/53017/20, за результатами опрацювання якого надіслано листа від 01.12.2020 № 11/01/02-1959 щодо проведення узгоджувальної наради та листа від 11.12.2020 № 11/01/02-2045 з доопрацьованим проєктом постанови. У відповідь від НАЗК отримано листа від 24.12.2020 № 21-03/68424/20.

Громадська антикорупційна, громадська антидискримінаційна та громадська гендерно-правова експертизи не проводилися.

8. Прогноз результатів

Прийняття постанови дозволить налагодити моніторинг стану захищеності інформаційних ресурсів об'єктів критичної інфраструктури, що дасть можливість отримувати відомості в реальному часі про стан інформаційної безпеки як на окремих об'єктах критичної інфраструктури і в регіонах, так і в державі в цілому. Зазначене сприятиме проведенню централізованого аналізу стану інформаційної безпеки, наданню рекомендацій щодо усунення вразливостей у системах інформаційної безпеки та застосовуванню вимог національних та міжнародних стандартів інформаційної безпеки.

Показниками, за якими буде оцінюватися ефективність реалізації постанови, є:

- кількість недоліків, виявлених під час проведення аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

кількість наданих рекомендацій щодо підвищення рівня захищеності об'єктів критичної інфраструктури;

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

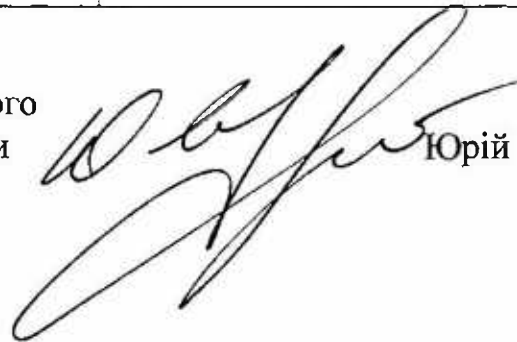
Реалізація постанови не матиме впливу на ринкове середовище, забезпечення захисту прав та інтересів громадян, розвиток регіонів, підвищення чи зниження спроможності територіальних громад; ринок праці, рівень зайнятості населення; громадське здоров'я, покращення чи погіршення стану здоров'я населення або його окремих груп; екологію та навколишнє природне середовище, обсяг природних ресурсів, рівень забруднення атмосферного повітря, води, земель, зокрема забруднення утвореними відходами, інші суспільні відносини.

Вплив на інтереси заінтересованих сторін:

Заінтересована сторона	Вплив реалізації акта на заінтересовану сторону	Пояснення очікуваного впливу
Держава	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 плановості й системності аудиту інформаційної безпеки та гарантувати державні інтереси в зазначених галузях, зокрема належну якість кіберзахисту та кібероборони; у межах повноважень виявляти та запобігати виникненню порушень вимог законодавства у зазначеній сфері об'єктами критичної інфраструктури.
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.	

Голова Державної служби спеціального зв'язку та захисту інформації України

07 09 2021 р.

 Юрій ШИГОЛЬ

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 кібершпionaжем. 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 пасажироперевезення;

6) 17 грудня 2016 року кібератака на підстанцію "Північна" компанії "Укренерго" призвела до збою в автоматичній управлінні, 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 поррахувати 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, унеможливорює 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 проекту 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	2021 рік			щорічно починаючи з 2022 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 напрямками використання	-	-	-	-	-	-
1.2. Зменшення витрат (-), усього	-	-	-	-	-	-
з них: за бюджетними програмами (КПКВК або ТПКВКМБ/ТКВБМС) та напрямками 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 проектом акта, які враховані у бюджеті, усього	-	-	-	-	-	-
з них за видами:	-	-	-	-	-	-
5. Загальна сума додаткових бюджетних коштів, необхідна згідно з проектом акта (пункт 1 - пункт 2 - пункт 3 – пункт 4)	-	-	-	-	-	-
6. Джерела покриття загальної суми додаткових бюджетних коштів (пункт 5), необхідних згідно з проектом 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

Аналіз регуляторного впливу

проекту постанови Кабінету Міністрів України “Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури”

I. Визначення проблеми

Останніми роками в Україні відбувається зростання загроз тероризму, сепаратизму, збільшення кількості надзвичайних ситуацій техногенного та природного характеру та кібератак на державні установи, компанії, підприємства. Зазначене відбувається на тлі процесів подальшого ускладнення і розгалуження взаємозв’язків і взаємовпливів при забезпеченні життєдіяльності сучасної держави, її національної безпеки і оборони. Вплив перерахованих чинників значно підвищує уразливість об’єктів і систем, життєво-важливих для забезпечення повсякденного функціонування держави.

Готовність до реагування на комплексні загрози та ризики до цього часу забезпечується за умов наявності, зокрема аудиту інформаційної безпеки об’єктів критичної інфраструктури.

Аналіз кіберзагроз свідчить, що кібератаки на комунікаційні системи та системи управління технологічними процесами об’єктів критичної інфраструктури держави таких галузей, як енергетика, хімічна промисловість та інші можуть призвести до виникнення надзвичайних ситуацій техногенного характеру.

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) у червні 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 поррахувати збитки, за оцінками експертів Україна втратила близько 0.4% ВВП, що становить близько 10 мільярдів гривень.

2) у ході президентських виборів 2019 року відбулися DDoS-атаки на сервер Центральної виборчої комісії.

3) у першому півріччі 2021 року на державні інформаційні ресурси здійснено 1,7 млн мережових кібератак, зокрема на сайт ЦВК, сайт Президента України, сайт НАБУ, сайт СБУ. Також, у 2021 році збільшилася кількість кібератак з використанням шкідливого програмного забезпечення Pterodo до організацій, які використовують програмне забезпечення «АСКОД».

Відповідно до Порядку віднесення об'єктів до об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 09.10.2020 № 1109 наразі формується Перелік об'єктів критичної інфраструктури, орієнтовна кількість об'єктів критичної інфраструктури – 490, з яких 390 об'єктів – суб'єкти господарювання (110 – великі, 250 – середні, 30 – малі) та 100 об'єктів критичної інфраструктури, які є державними органами.

На сьогодні в Україні відсутній перелік атестованих аудиторів інформаційної безпеки, орієнтовно – 50 аудиторів інформаційної безпеки.

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 та 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).

Основні групи (підгрупи), на які проблема впливає:

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

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

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

II. Цілі державного регулювання

Основною ціллю проекту постанови є встановлення єдиних вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та уніфікованого порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Альтернативний спосіб обрано під час зустрічей та обговорень з представниками громадськості та посадовими особами державних органів.

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, стає 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	Обраний спосіб (прийняття проекту постанови) Зазначений альтернативний спосіб досягнення цілей є найбільш прийнятним і ефективним, оскільки він відповідає потребам у розв'язанні визначених проблем та принципам державної регуляторної політики. Прийняття проекту постанови дозволить: встановити уніфікований порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, як результат цього - підвищити рівень кіберзахисту об'єктів критичної інфраструктури.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Вигоди відсутні. Ситуація залишиться на рівні, що існує, що може створити загрози національній безпеці України	Проблема інформаційної безпеки на об'єктах критичної інфраструктури залишиться актуальною Можливо зменшення надходження коштів до державного бюджету у випадку реалізації загроз об'єктам критичної інфраструктури, а також збільшення видатків з держбюджету на необхідні заходи щодо відновлення порушених об'єктів критичної інфраструктури.

Альтернатива 2	Надасть можливість забезпечувати інтереси держави шляхом підвищення захисту об'єктів критичної інфраструктури до загроз будь-якого походження, що, у свою чергу, забезпечить національну безпеку.	Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів. Водночас, організація належного захисту об'єктів критичної інфраструктури сприятиме зменшенню додаткового навантаження на державний бюджет щодо усунення наслідків порушення у роботі об'єктів критичної інфраструктури та відновлення їх функціонування.
----------------	---	--

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Ситуація залишиться на рівні, що існує. Ймовірне виникнення загроз безпеці життєдіяльності громадян, можливості втрати ними життєво-важливих послуг та функцій, які виконують об'єкти критичної інфраструктури.	Не передбачаються
Альтернатива 2	Вигоди опосередковані. Сприятиме захисту життєдіяльності громадян, забезпечить безперервність надання життєво-важливих послуг та функцій для населення.	Реалізація не потребує додаткових матеріальних та інших витрат з боку громадян

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	110	250	30	-	390
Питома вага групи у загальній кількості, відсотків	28%	64%	8%	0%	100 %

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає	Будуть виникати надзвичайні ситуації
Альтернатива 2	Узгодження інтересів бізнесу та держави, чіткий порядок та плановість проведення заходів аудиту ІБ Адміністрації Держспецзв'язку.	Оцінити точні витрати на реалізацію регуляторного акта буде можливо після визначення переліку об'єктів критичної інфраструктури держави

Розрахунки проводились на основі очікуваної кількості об'єктів критичної інфраструктури, які будуть включені до переліку об'єктів критичної інфраструктури відповідно до Порядку віднесення об'єктів до об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 09.10.2020 № 1109.

Зараз питома вага суб'єктів малого підприємництва (малих та мікропідприємств разом) у загальній кількості суб'єктів господарювання, на яких може поширюватися регулювання складає 8 %.

Оцінити точні витрати на реалізацію постанови буде можна після визначення переліку об'єктів критичної інфраструктури.

Витрати одного аудитора, які виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати на складання договору між власником та/або керівником об'єкта критичної інфраструктури і аудитором	—	—
2	Витрати, пов'язані з проведенням аудиту об'єкта критичної інфраструктури ¹	12133 грн. (42*8*36,11)	60665 грн.
3	Витрати, пов'язані з тестуванням об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на проникнення з використанням спеціалізованих ліцензійних програмно-апаратних засобів пошуку та аналізу вразливостей ²	1444 грн. (5*8*36,11)	7220 грн.
4	Витрати, пов'язані із залученням до проведення незалежного аудиту інших аудиторів, відомості про яких занесені до переліку атестованих аудиторів інформаційної безпеки	—	—
5	Витрати, пов'язані зі складанням звіту за результатами незалежного аудиту (канцелярські товари тощо), гривень ³	2889 грн. (10*8*36,11)	14445 грн.
5.1	Папір, гривень ⁴	26 грн.	130 грн.
5.2	Картриджі до принтеру, гривень ⁵	36 грн.	180 грн.
6	Інше (уточнити), гривень	—	—
7	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 5 ¹ + 5 ² + 6), гривень	16528 грн.	82640 грн.
8.	Сумарні витрати аудитора на виконання регулювання (вартість регулювання) (рядок 7 x кількість аудитів), гривень ⁶	66112 грн.	330560 грн.

¹ Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 36,11 грн/год відповідно до Закону України "Про Державний бюджет України на 2021 рік"; кількість днів на проведення аудиту – 42; 8-годинний робочий день

² Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 36,11 грн/год відповідно до Закону України "Про Державний бюджет України на 2021 рік"; кількість днів на проведення тестування – 5; 8-годинний робочий день

³ Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 36,11 грн/год відповідно до Закону України "Про Державний бюджет

України на 2021 рік"; кількість днів на підготовку звіту за результатами аудиту – 10; 8-годинний робочий день.

⁴Для обрахунку: вартість пачки паперу формату А4 становить 86 грн за 500 аркушів (0,17 грн 1 аркуш); орієнтовна кількість аркушів звіту аудиту складає – 150 аркушів.
Орієнтовна кількість коштів – 26 грн
https://rozetka.com.ua/ua/canon_8713878092269/p5002507/

⁵Для обрахунку: ціна картриджу до принтера для 2000 аркушів складає 429 грн. (0,21 грн. 1 аркуш паперу) орієнтовна кількість аркушів звіту 150 аркушів.

https://rozetka.com.ua/ua/hp_w1103a/p129985609/characteristics

⁵Для обрахунку 1 аудитор може провести за 1 рік 4 аудита (об'єкта, який має 20 АРМ)

Витрати
на одного суб'єкта господарювання великого і середнього підприємництва, які
виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати на складання договору між власником та/або керівником об'єкта критичної інфраструктури і аудитором	–	–
2	Витрати, пов'язані із наймом аудитора, гривень ¹	16466 грн. (57*8*36,11)	49398 грн.
3	Витрати, пов'язані із поданням копії звіту Адміністрації Держспецзв'язку, гривень	57 грн.	171 грн.
3.1	Папір, гривень ²	26 грн.	78 грн.
3.2	Картриджі до принтеру, гривень ³	31 грн.	93 грн.
4	Інше (уточнити), гривень	–	–
5	РАЗОМ (сума рядків: 1 + 2 + 3 + 4), гривень	16523 грн.	33046 грн.
6	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць ⁴	200	600
7	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 5 x рядок 6), гривень ⁴	3304600 грн.	9913800 грн.

¹ Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 36,11 грн/год відповідно до Закону України "Про Державний бюджет України на 2021 рік"; сумарна кількість днів на проведення аудиту, тестування та підготовку звіту – 57, 8-годинний робочий день

²Для обрахунку: вартість пачки паперу формату А4 становить 86 грн за 500 аркушів (0,17 грн 1 аркуш); орієнтовна кількість аркушів звіту аудиту складає – 150 аркушів
Орієнтовна кількість коштів – 26 грн
https://rozetka.com.ua/ua/canon_8713878092269/p5002507/

³Для обрахунку: ціна картриджу до принтера для 2000 аркушів складає 429 грн (0,21 грн. – 1 аркуш паперу) орієнтовна кількість аркушів звіту 150 аркушів
https://rozetka.com.ua/ua/hp_w1103a/p129985609/characteristics

⁴Для обрахунку. кількість суб'єктів господарювання з урахуванням встановлених категорій критичності об'єктів критичної інфраструктури:
для об'єктів I та II категорій критичності – не рідше ніж один раз на два роки;

для об'єктів III та IV категорій критичності – не рідше ніж один раз на три роки та наявності 50 аудиторів (1 аудитор може провести за 1 рік 4 аудита).

Сумарні витрати за альтернативами

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1.	Не має
Альтернатива 2.	16523 грн. у одного суб'єкта (33046 грн. за 5 років) 3304600 грн. у 200 суб'єктів (9913800 грн. у 600 суб'єктів за 5 років)

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

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

Рейтинг результативності	Вигоди (підсумок)	Витрати (Підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
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 з державного бюджету — 173400 грн. Орієнтовні щорічні витрати 200 суб'єктів господарювання — 3304600 грн.	Проблема більше існувати не буде

Рейтинг	Аргументи щодо переваги обраної альтернативи/причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 1	Ситуація залишиться на рівні, що існує, що може створити загрози національній безпеці України. Збільшення витрат на необхідні заходи щодо відновлення порушених об'єктів критичної інфраструктури.	
Альтернатива 2	Прийняття постанови дозволить значно підвищити рівень кіберзахисту об'єктів критичної інфраструктури, а також мінімізувати збитки за результатами кібератак.	Вплив зовнішніх чинників на дію регуляторного акта у разі його прийняття – відсутній

Враховуючи вищенаведені позитивні та негативні сторони альтернативного способу досягнення мети, доцільно прийняти розроблений проект постанови.

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 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 проектом постанови передбачається:

встановлення єдиних вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та уніфікованого порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Заходи, що пропонуються для розв'язання проблеми:

для впровадження цього регуляторного акта необхідно забезпечити інформування громадськості про вимоги регуляторного акта шляхом його оприлюднення у засобах масової інформації (на офіційному вебсайті Держспецзв'язку).

Реалізація положень проекту постанови:

дозволить отримувати актуальну інформацію щодо стану інформаційної безпеки на об'єктах критичної інфраструктури.

зазначене сприятиме підвищенню рівня кіберзахисту об'єктів критичної інфраструктури, а також мінімізувати збитки за результатами кібератак.

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

Відповідно до Порядку віднесення об'єктів до об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 09.10.2020 № 1109 рішення щодо категорії критичності об'єкта критичної інфраструктури приймається на основі узагальненої нормованої оцінки рівня критичності об'єкта критичної інфраструктури.

Зараз питома вага суб'єктів малого підприємництва (малих та мікропідприємств разом) у загальній кількості суб'єктів господарювання, на яких може поширюватися регулювання складає 8 %, але після проведення розрахунків узагальненої нормованої оцінки рівня критичності суб'єкти малого підприємництва (малих та мікропідприємств разом) будуть віднесені до не критичних об'єктів.

Тому розрахунок витрат на запровадження державного регулювання для суб'єктів малого підприємництва (Тест малого підприємництва) не проводився.

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

Витрати

Адміністрації Держспецзв'язку, які виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати, пов'язані з веденням переліку атестованих аудиторів інформаційної безпеки	—	—
2.	Витрати, пов'язані з проведенням аналізу звіту незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури	867 грн.	4335 грн.
3.	Інше, гривень	—	—
4.	РАЗОМ (сума рядків: 1 + 2 + 3), гривень	867 грн.	4335 грн.
5.	Кількість копій звітів аудитів , одиниць	200	600
6.	Сумарні витрати (рядок 4 x рядок 5), гривень	173400 грн.	2601000 грн.

¹ Для обрахунку приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 36,11 грн/год відповідно до Закону України "Про Державний бюджет України на 2021 рік", кількість днів на проведення аналізу звіту аудиту – 3, 8-годинний робочий день. (1 звіт – 150 аркушів.)

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується у часі.

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

VIII. 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 місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта;

кількість суб'єктів господарювання, на яких поширюватиметься дія акта;

розмір коштів і час, що витратимуться суб'єктами господарювання та/або фізичними особами, пов'язаними з виконанням вимог акта, оцінити неможливо до затвердження переліку об'єктів критичної інфраструктури;

рівень поінформованості суб'єктів господарювання та (або) фізичних осіб із основними положеннями регуляторного акта –середній, оскільки зі змістом акта та супровідних до нього документів можна ознайомитися на офіційному вебсайті Держспецзв'язку (<https://cip.gov.ua>);

кількість укладених договорів з проведення аудиту інформаційної безпеки;

кількість об'єктів критичної інфраструктури, з порушеннями виявленими під час проведення аудиту інформаційної безпеки;

кількість наданих рекомендацій щодо підвищення рівня захищеності;

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

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

Відстеження результативності цього регуляторного акта буде здійснюватися Адміністрацією Держспецзв'язку за допомогою статистичного методу шляхом проведення:

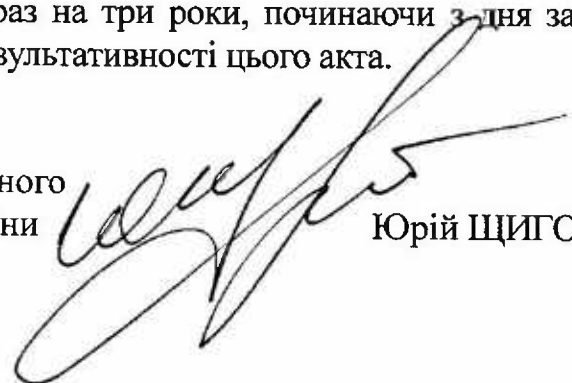
базового відстеження – через рік після набрання чинності регуляторним актом шляхом збирання статистичних даних, опрацювання пропозицій до нього, їх аналізу;

повторного відстеження – не пізніше двох років з дня набрання чинності шляхом аналізу статистичних даних;

періодичного відстеження – раз на три роки, починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Голова Державної служби спеціального зв'язку та захисту інформації України

07 09 2021 року



Юрій ЩИГОЛЬ

gov.ua
Державна служба спеціального зв'язку та захисту інформації України

Особистий кабінет
Люди із порушенням зору
In English

Про Службу Послуги Діяльність Документи Прес-центр Для громадянські Контакти Більше f t y v n Пошук



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

Держспецзв'язку Держспецзв'язку Держспецзв'язку

2021.06.23 15:12

1. Короткий 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 згідно четвертого пункту І Плану організації підготовки проекту актів, необхідних для забезпечення реалізації Закону України «Про основні засади забезпечення кібербезпеки України» схваленого на засіданні Кабінету Міністрів України 22 листопада 2017 року (протокол № 56).

Документ визначає основні вимоги та механізми впровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

2. Адреси для надання пропозицій до проекту акта

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

Адміністрація Державної служби спеціального зв'язку та захисту інформації України

пошта: вул. Солом'янська 13 м. Київ 03110 тел. (044) 281 88 46

електронна: info@dsszzi.gov.ua

Державної регуляторної служби України

пошта: вул. Арсенальна 9/11 м. Київ 01011 тел. (044) 254 56 75

факс: (044) 254 43 73

електронна: info@rds.gov.ua

3. Іншими способами надіслати проект акта

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