ПРОЄКТ
Прим. №__

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УРАЇНИ

Н А К А З

м. Київ

__ _____ 20__ року № _____

Про затвердження Вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації)

Відповідно до пункту 90 частини першої статті 14 Закону України “Про Державну службу спеціального зв’язку та захисту інформації України”, пункту 1 частини другої статті 8 Закону України “Про основні засади забезпечення кібербезпеки України”, підпункту 95^5 пункту 4, пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, пункту 2 постанови Кабінету Міністрів України від 24 березня 2023 року № 257 “Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури”, з метою врегулювання питань забезпечення впровадження системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки та порядку їх атестації (переатестації)

НАКАЗУЮ:

1. Затвердити Вимоги до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядок їх атестації (переатестації), що додаються.

2. Директору Департаменту державного контролю у сфері захисту інформації Адміністрації Державної служби спеціального зв’язку та захисту інформації України забезпечити подання цього наказу в установленому порядку на державну реєстрацію до Міністерства юстиції України.

3. Контроль за виконанням цього наказу покласти на заступника Голови Державної служби спеціального зв’язку та захисту інформації України відповідно до розподілу обов’язків.

4. Цей наказ набирає чинності з дня його офіційного опублікування.

Голова Служби
майор Юрій МИРОНЕНКО

Прим. №__

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)»

1. Мета

Метою прийняття наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)» (далі – проєкт наказу) є визначення основних вимог до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури, а також визначення порядку їх атестації (переатестації).

2. Обґрунтування необхідності прийняття акта

Проєкт наказу розроблено відповідно до пункту 90 частини першої статті 14 Закону України "Про Державну службу спеціального зв'язку та захисту інформації України", пункту 1 частини другої статті 8 Закону України "Про основні засади забезпечення кібербезпеки України", підпункту 95^5 пункту 4, пункту 10 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, пункту 2 постанови Кабінету Міністрів України від 24 березня 2023 року № 257 "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури".

Необхідність прийняття наказу зумовлена відсутністю кваліфікованих аудиторів для проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, що унеможливлює збір відомостей щодо реального стану їх інформаційної безпеки та перешкоджає впровадженню системного підходу до врегулювання питання захисту критичної інфраструктури на загальнодержавному рівні. Питання забезпечення належного рівня кваліфікації аудиторів інформаційної безпеки на об'єктах критичної інфраструктури не можуть бути вирішені без наявності чітких вимог до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури, а також визначеного порядку їх атестації (переатестації) з подальшим формуванням та оприлюдненням Переліку аудиторів інформаційної безпеки на об'єктах критичної інфраструктури, куди будуть внесені особи, що мають право проводити

незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури.

3. Основні положення проєкту акта

Проєктом наказу пропонується затвердити Вимоги до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядок їх атестації (переатестації).

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-комунікаційних системах»;

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

Закон України «Про основні засади забезпечення кібербезпеки України»;

Закон України «Про критичну інфраструктуру»;

Закон України «Про електронні комунікації»;

Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затверджене постановою Кабінету Міністрів України від 03 вересня 2014 року № 411;

Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19 червня 2019 року № 518;

постанова Кабінету Міністрів України від 09 жовтня 2020 року № 1109 «Деякі питання об’єктів критичної інфраструктури»;

постанова Кабінету Міністрів України від 24 березня 2023 року № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури».

5. Фінансово-економічне обґрунтування

Реалізація наказу не потребує фінансування з державного та місцевого бюджетів.

6. Позиція заінтересованих сторін

Проєкт наказу потребує консультацій з громадськістю, у зв’язку з чим розміщений на офіційному вебсайті Держспецзв’язку (https://cip.gov.ua). Отримані пропозиції громадськості від Інтернет Асоціації України та Української асоціації операторів зв'язку «ТЕЛАС» були обговорені на робочій зустрічі. За результатами доопрацювання проєкту наказу були надіслані листи до Інтернет Асоціації України від 31.10.2023 № 11/07-8088/СЕД та до Української асоціації операторів зв'язку «ТЕЛАС» від 31.10.2023 № 11/07-8089/СЕД щодо врахування пропозицій, а також обґрунтування не врахованих позицій. Зауважень та пропозицій до позицій,

викладених в зазначених листах після проведення громадського обговорення до Адміністрації Держспецзв'язку не надходило.

Проєкт наказу 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, уповноваженими представниками всеукраїнських профспілок, їх об'єднань та всеукраїнських об'єднань організацій роботодавців, Урядовим уповноваженим з прав осіб з інвалідністю та всеукраїнськими громадськими організаціями осіб з інвалідністю, їх спілками, Уповноваженим із захисту державної мови.

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

7. Оцінка відповідності

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

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

У проєкті наказу немає положень, які впливають на забезпечення рівних прав та можливостей жінок і чоловіків.

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

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

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

8. Прогноз результатів

Реалізація наказу дозволить встановити чіткі вимоги до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та налагодити процес їх атестації (переатестації), що дасть можливість сформувати Перелік аудиторів інформаційної безпеки на об'єктах критичної інфраструктури, куди будуть внесені тільки особи, що мають достатній рівень знань, вмінь та навичок. Це забезпечить проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури на високому рівні з урахуванням існуючих вимог, норм і законів у сфері кіберзахисту об'єктів критичної інфраструктури, що сприятиме якісному моніторингу стану захищеності інформаційних ресурсів об'єктів критичної інфраструктури.

Реалізація наказу 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 формування Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури, до якого входитимуть аудитори інформаційної безпеки, які підтвердили свою компетентність, відповідають вимогам та пройшли всі необхідні перевірки в установленому порядку, що унеможливить доступ до об’єктів критичної інфраструктури сторонніх неперевірених осіб.	Прийняття наказу надасть можливість об’єктам критичної інфраструктури отримувати якісні послуги з проведення аудиту інформаційної безпеки, на основі якого основні суб’єкти національної системи кібербезпеки отримають актуальну інформацію щодо стану інформаційної безпеки на об’єктах критичної інфраструктури держави, зокрема інформацію про рівень кіберзахисту та кібероборони. Також це дозволить у межах повноважень виявляти та запобігати виникненню порушень вимог законодавства у зазначеній сфері на об’єктах критичної інфраструктури.
Суб’єкти господарювання	Об’єкти критичної інфраструктури матимуть змогу обирати кваліфіковану, перевірену особу для проведення аудиту інформаційної безпеки.	

Голова Державної служби спеціального
зв’язку та захисту інформації України Юрій МИРОНЕНКО

___ _____ 2023 р.

Аналіз регуляторного впливу
до проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)»

I. Визначення проблеми

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)» (далі – проєкт наказу) розроблено з метою встановлення критеріїв та вимог до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури, а також визначення порядку їх атестації (переатестації).

Проєкт наказу розроблено відповідно до пункту 2 постанови Кабінету Міністрів України від 24 березня 2023 року № 257 "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури", яким передбачено, що Адміністрація Державної служби спеціального зв'язку та захисту інформації повинна забезпечити затвердження вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації).

Необхідність прийняття наказу зумовлена відсутністю кваліфікованих аудиторів для проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, що унеможливлює збір відомостей щодо реального стану їх інформаційної безпеки та перешкоджає впровадженню системного підходу до врегулювання питання захисту критичної інфраструктури на загальнодержавному рівні.

Затвердження наказу дозволить вирішити питання забезпечення належного рівня кваліфікації аудиторів інформаційної безпеки на об'єктах критичної інфраструктури шляхом встановлення чітких вимог до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури, а також визначення порядку їх атестації (переатестації) з подальшим формуванням та оприлюдненням Переліку аудиторів інформаційної безпеки на об'єктах критичної інфраструктури (далі – Перелік), куди будуть внесені особи, що мають право проводити незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури.

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

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

Проблема не може бути розв’язана за допомогою ринкових механізмів, оскільки на сьогодні відсутній регуляторний акт, який би врегульовував вимоги до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури, а також визначення порядку їх атестації (переатестації).

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

II. Цілі державного регулювання

Основною ціллю державного регулювання є виконання вимог постанови Кабінету Міністрів України від 24 березня 2023 року № 257 “Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури” щодо затвердження вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації).

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Збереження нормативно-правової бази без змін. Така альтернатива є неприйнятною, оскільки це унеможливить досягнення поставленої цілі та не створить відповідних умов для нормативного-правового врегулювання питання встановлення вимог до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури, а також визначення порядку їх атестації (переатестації) з подальшим формуванням та оприлюдненням Переліку. За відсутності Переліку та атестованих аудиторів інформаційної безпеки на об’єктах критичної інфраструктури, проведення незалежного аудиту інформаційної безпеки на об’єктах критичої інфраструктури неможливо, адже це суперечить Порядку проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 24 березня 2023 року № 257 “Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури”. Такий спосіб не сприятиме досягненню цілей державного регулювання.

Альтернатива 2	Затвердження наказу. Зазначений альтернативний спосіб досягнення цілей є найбільш прийнятним і ефективним, оскільки він відповідає потребам у розв’язанні визначених проблем та принципам державної регуляторної політики. Реалізація наказу дозволить встановити чіткі вимоги до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та налагодити процес їх атестації (переатестації), що дасть можливість сформувати Перелік, куди будуть внесені тільки особи, що мають достатній рівень знань, вмінь та навичок. Це забезпечить проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури на високому рівні з урахуванням існуючих вимог, норм і законів у сфері кіберзахисту об’єктів критичної інфраструктури, що сприятиме якісному моніторингу стану захищеності інформаційних ресурсів об’єктів критичної інфраструктури. Такий спосіб сприятиме досягненню цілей державного регулювання.

Інші способи є неприйнятними, оскільки їх реалізація не вирішить порушену проблему.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає	Немає
Альтернатива 2	Формування Переліку, до якого входитимуть аудитори інформаційної безпеки, які підтвердили свою компетентність, відповідають вимогам та пройшли всі необхідні перевірки в установленому порядку, що забезпечить якісне проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури та унеможливить доступ до об’єктів критичної інфраструктури сторонніх неперевірених осіб.	Немає

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Ситуація залишається на рівні, що існує. Ймовірне виникнення загроз безпеці	Немає

	життєдіяльності громадян, можливості втрати ними життєво важливих ресурсів, послуг та функцій, які виконують та надають об'єкти критичної інфраструктури.	
Альтернатива 2	Вигоди опосередковані. Сприятиме захисту життєдіяльності громадян, забезпечить безперервність надання життєво важливих ресурсів, послуг та функцій для населення.	Немає

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	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%	100%

* 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, орієнтована 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.

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає	Немає
Альтернатива 2	Оператори критичної інфраструктури матимуть змогу обирати кваліфіковану, перевірену особу для проведення незалежного аудиту інформаційної безпеки.	63117,6*

* відповідно до додатку до Аналізу регуляторного впливу, витрати на ознайомлення суб'єктів господарювання з вимогами регуляторного акту.

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	–
Альтернатива 2	63117,6

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 2	4	Максимальний бал, який свідчить про можливість максимального досягнення мети державного регулювання.
Альтернатива 1	1	Мінімальний бал, який свідчить про неможливість досягнення мети державного регулювання. Цілі прийняття регуляторного акта не можуть бути досягнуті, проблема продовжує існувати.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 2	Затвердження наказу надасть можливість об’єктам критичної інфраструктури отримувати якісні послуги з проведення незалежного аудиту інформаційної безпеки, на основі якого основні суб’єкти національної системи кібербезпеки отримають актуальну інформацію щодо стану інформаційної безпеки на об’єктах критичної інфраструктури держави, зокрема інформацію про рівень кіберзахисту та кібероборони. Також це дозволить у межах повноважень виявляти та запобігати виникненню порушень вимог	63117,6*	Цілі державного регулювання можуть бути досягнуті повною мірою, проблема більше існувати не буде

	законодавства у зазначеній сфері на об’єктах критичної інфраструктури.		
Альтернатива 1	Немає	Немає	Цілі державного регулювання не можуть бути досягнуті, проблема продовжує існувати

* відповідно до додатку до Аналізу регуляторного впливу, витрати на ознайомлення суб’єктів господарювання з вимогами регуляторного акту.

Рейтинг	Аргументи щодо переваги обраної альтернативи/причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 1	Відсутність встановлених вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації) унеможливить проведення незалежного аудиту інформаційної безпеки на об’єктах критичої інфраструктури. Проблема інформаційної безпеки на об’єктах критичної інфраструктури залишиться актуальною.	Х
Альтернатива 2	Прийняття наказу дозволить залучати до проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури кваліфікованих перевірених осіб, що надасть можливість значно підвищити рівень кіберзахисту об’єктів критичної інфраструктури, а також мінімізувати збитки за результатами кібератак.	Ризику впливу зовнішніх чинників на дію запропонованого регуляторного акта немає.

V. Механізм та заходи, які забезпечать розв’язання визначеної проблеми

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

Адміністрацією Держспецзв’язку підготовлено проєкт наказу, яким пропонується затвердити вимоги до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядок їх атестації (переатестації), що визначає:

суб'єкти відносин, пов'язаних з оцінюванням кваліфікації аудиторів, та їх функції;

вимоги до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури;

порядок атестації (переатестації) осіб, що мають намір проводити незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури;

причини для прийняття рішення щодо виключення особи з Переліку.

Заходи, що пропонуються для розв’язання проблеми:

інформування громадськості про вимоги регуляторного акта шляхом оприлюднення його проєкту на офіційному вебсайті Держспецзв’язку;

погодження проєкту регуляторного акта із заінтересованими органами;

проведення атестації (переатестації) осіб з подальшим прийняттям рішення щодо включення їх до Переліку.

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

Реалізація наказу не потребує додаткових матеріальних, фінансових та інших ресурсів державного та місцевих бюджетів.

За результатами введення в дію запропонованого регуляторного акта не передбачається нанесення шкоди суб’єктам господарювання, тому механізм повної або часткової компенсації можливої шкоди у разі настання очікуваних наслідків дії акта не розроблявся.

Витрати для великих, середніх та малих суб’єктів господарювання пов’язані з ознайомленням з прийнятим актом і складають 161,84 грн. на 1 суб’єкта господарювання.

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	–	–
2	Витрати пов’язані з розглядом 1 заяви від особи, що претендує на внесення в Перелік	648 грн.	3240 грн.
3	РАЗОМ(сума рядків 1 і 2), гривень	648 грн.	3240 грн.
4	Кількість очікуваних заяв заявників, одиниць	100	950
6	Сумарні витрати ((648 грн) х (рядок 4)), гривень	64800 грн.	615600 грн.

[1] Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 40,46 грн/год відповідно до Закону України «Про Державний бюджет України на 2023 рік»; кількість днів на проведення розгляду заяви від 1 особи - 2, 8-годинний робочий день.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії регуляторного акта не обмежується у часі. Регуляторний акт набирає чинності з дня його офіційного опублікування. Зміна строку дії акта можлива в разі зміни законодавства, на вимогах якого базується проєкт регуляторного акта.

VIII. Визначення показників результативності дії регуляторного акта

Показниками результативності запропонованого регуляторного акта є:

кількість суб'єктів господарювання, на яких поширюється дія акта, становить близько 390 – це кількість об'єктів критичної інфраструктури, які в результаті реалізації наказу зможуть отримувати послуги з проведення незалежного аудиту інформаційної безпеки, залучаючи осіб з Переліку;

кількість осіб в Переліку (прогнозована кількість: за перший рік – 50, за п'ять років – близько 200);

кількість укладених договорів з проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (прогнозована кількість: за перший рік – 390, за п'ять років – близько 1000);

кількість наданих рекомендацій щодо підвищення рівня захищеності;

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

кількість впроваджених заходів щодо підвищення рівня кіберзахисту на об'єктах критичної інфраструктури.

Розмір надходжень до державного і місцевих бюджетів та державних цільових фондів, пов'язаних з дією акта, не передбачається, оскільки цей акт не регулює цих надходжень і не має впливу на них.

Прийняття регуляторного акта не передбачає витрат коштів суб'єктів господарювання.

Рівень поінформованості державних органів, органів місцевого самоврядування, суб'єктів господарювання та/або фізичних осіб – достатній: проєкт наказу розміщено на офіційному вебсайті Державної служби спеціального зв'язку та захисту інформації України.

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

Відстеження результативності цього регуляторного акта буде здійснюватися Адміністрацією Державної служби спеціального зв'язку та захисту інформації України 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.

Вид даних для базового, повторного та періодичного відстеження – статистичні дані про кількість осіб, внесених до Переліку, кількість укладених договорів з проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури, кількість наданих рекомендацій щодо підвищення рівня захищеності.

Голова Державної служби спеціального
зв’язку та захисту інформації України Юрій МИРОНЕНКО

«___» _____ 2023 року

Додаток
до Аналізу регуляторного впливу

ВИТРАТИ
на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта за альтернативою 2

№ з/п	Витрати	За перший рік	За п'ять років
1	2	3	4
1	Процедури отримання первинної інформації про вимоги регулювання – 1 година ***(одноразово)*** *Формула: витрати часу на отримання інформації про регулювання, отримання необхідних форм Х, вартість часу суб'єкта підприємництва (заробітна плата)* 40,46 грн * 1 год	40,46	40,46
2	Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів), гривень	-	-
3	Витрати, пов'язані з наданням органу державного ринкового нагляду за його запитами інформації, що дає змогу ідентифікувати суб'єкта господарювання – 1 год	-	-
4	Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/приписів тощо), гривень	-	-
5	Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень	-	-
6	Витрати на оборотні активи (матеріали, канцелярські товари тощо), гривень, витрати, пов'язані із приведенням у відповідність необхідних документів та інструкцій: 3 год * 40,46 грн	121,38	121,38
7	Витрати, пов'язані з наймом додаткового персоналу, гривень	-	-
8	Інше (уточнити), гривень	-	-
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень	161,84	161,84
10	Кількість суб'єктів господарювання великого, середнього та малого підприємництва, на яких буде поширено регулювання, одиниць	390	390
11	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва на виконання регулювання (вартість регулювання) (рядок 9 * рядок 10), гривень	63117,6	63117,6

ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної
служби спеціального зв’язку та
захисту інформації України
___ _____ 20__ року № ___

Вимоги
до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядок їх атестації (переатестації)

I. Загальні положення

1. Ці Вимоги встановлюють критерії та вимоги до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури, а також визначають порядок їх атестації (переатестації), включення до Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та виключення з нього.

2. У цих Вимогах терміни вживаються в такому значенні:

Перелік аудиторів інформаційної безпеки на об’єктах критичної інфраструктури (далі – Перелік) – список атестованих аудиторів інформаційної безпеки, який містить дані про прізвище, власне ім’я, по батькові (за наявності)/назву аудитора інформаційної безпеки, кваліфікацію (для фізичних осіб-аудиторів), контактні дані, кількість проведених аудитів, рейтинг аудитора інформаційної безпеки за результатами проведених аудитів і розміщується на сайті Держспецзв’язку в розділі «Незалежний аудит інформаційної безпеки»;

заявник – юридична або фізична особа, що має намір провадити діяльність аудитора інформаційної безпеки на об’єктах критичної інфраструктури, пройти атестацію (переатестацію) аудиторів інформаційної безпеки та бути включеною до Переліку;

атестація аудиторів інформаційної безпеки (далі – атестація) – процедура розгляду та перевірки на відповідність цим Вимогам документів заявників з метою отримання ними права проводити незалежні аудити інформаційної безпеки на об’єктах критичної інфраструктури;

Кваліфікаційний центр – суб’єкт, уповноважений Національним агентством кваліфікацій здійснювати оцінювання і визнання результатів навчання, здобутих особами шляхом формальної, неформальної або інформальної освіти, присвоєння та/або підтвердження відповідних професійних кваліфікацій, визнання відповідних професійних кваліфікацій,

здобутих у інших країнах, на підставі сертифіката про акредитування такого кваліфікаційного центру і включений до Реєстру кваліфікаційних центрів у складі Реєстру кваліфікацій;

Орган із сертифікації персоналу – суб'єкт, який має атестат про акредитацію, виданий Національним агентством з акредитації України, та надає послуги із сертифікації персоналу згідно з вимогами кваліфікацій «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» та «Керівник команди з аудиту систем менеджменту інформаційної безпеки», визначених у професійному стандарті «Аудитор інформаційних технологій (з кібербезпеки)».

Інші терміни вживаються у значенні, наведеному в Законах України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, затвердженому постановою Кабінету Міністрів України від 24 березня 2023 року № 257.

3. Суб'єктами відносин, пов'язаних з атестацією (переатестацією) аудиторів інформаційної безпеки, є:

Адміністрація Держспецзв'язку;

заявники;

Кваліфікаційні центри;

Органи із сертифікації персоналу;

Служба безпеки України.

4. Адміністрація Держспецзв'язку:

здійснює ведення та оприлюднення Переліку на сайті Держспецзв'язку в розділі «Незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури»;

отримує, розглядає та перевіряє документи, подані заявниками;

приймає рішення про успішне проходження атестації та включення заявника до Переліку або про не проходження атестації заявником;

приймає рішення про скасування права на проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та виключення аудитора інформаційної безпеки з Переліку.

5. Підтвердженням проходження заявником атестації є відповідне рішення Адміністрації Держспецзв'язку та наявність відомостей про нього в Переліку.

6. Рішення Адміністрації Держспецзв'язку та наявність відомостей про юридичну особу в Переліку підтверджує право юридичної особи проводити незалежний аудит інформаційної безпеки на об'єктах критичної

інфраструктури, залучаючи до нього виключно аудиторів інформаційної безпеки, які пройшли атестацію в порядку, що встановлений цими Вимогами, і з якими вона має договірні відносини.

II. Вимоги до заявників

1. Вимоги до заявника, який є фізичною особою:

бути громадянином України;

не мати не погашеної або не знятої судимості в установленому законом порядку;

мати довідку встановленого законодавством зразка про відсутність психіатричних протипоказань;

мати допуск до державної таємниці;

мати документи, що підтверджують досвід роботи у сфері інформаційної безпеки та/або інформаційних систем;

мати чинний сертифікат «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки» відповідно до вимог професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)», виданий Кваліфікаційним центром або Органом із сертифікації персоналу.

2. Підтвердженням досвіду роботи у сфері інформаційної безпеки та/або інформаційних систем є відомості про виконання не менше ніж 4 проєктів з внутрішнього або незалежного аудиту інформаційної безпеки за останні 2 роки.

3. Вимоги до заявника, який є юридичною особою:

перебувати у трудових відносинах не менше ніж з 3 аудиторами інформаційної безпеки, які пройшли атестацію згідно з цими Вимогами та включені до Переліку;

мати дозвіл на провадження діяльності, пов’язаної з державною таємницею;

не бути включеним до переліку осіб, щодо яких застосовано спеціальні економічні та інші обмежувальні заходи (санкції) відповідно до Закону України «Про санкції»;

мати атестат про акредитацію, виданий Національним агентством з акредитації відповідно до ДСТУ EN ISO/IEC 17021-1:2017 та ДСТУ EN ISO/IEC 27006.

III. Порядок атестації (переатестації) заявників

1. З метою проходження атестації (переатестації) та включення до Переліку заявник, який є фізичною особою, надсилає до Адміністрації Держспецзв’язку такі документи:

1) заповнену заяву за формою згідно з додатком 1 до цих Вимог;

2) документи, що підтверджують відповідність заявника вимогам, визначеним у пункті 1 розділу ІІ цих Вимог, а саме:

копію витягу про відсутність судимості або обмежень;

довідку встановленого законодавством зразка про проходження психіатричних оглядів, у тому числі на предмет вживання психоактивних речовин;

копії 4 контрактів на проведення робіт з аудиту інформаційної безпеки, що були проведені протягом двох календарних років до дати подання заяви;

копію допуску до державної таємниці;

копію сертифіката «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки» відповідно до вимог професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)», виданого Кваліфікаційним центром або Органом із сертифікації персоналу.

2. З метою проходження атестації (переатестації) та включення до Переліку заявник, який є юридичною особою, надсилає такі документи:

1) заповнену заяву за формою згідно з додатком 2 до цих Вимог;

2) документи, що підтверджують відповідність заявника вимогам, визначеним у пункті 3 розділу ІІ цих Вимог, а саме:

копії чинних сертифікатів «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки» та трудових договорів заявника з аудиторами, яким належать ці сертифікати;

копію дозволу на провадження діяльності, пов’язаної з державною таємницею;

інформацію (довідку у довільній формі) про те, що до заявника не застосовані спеціальні економічні та інші обмежувальні заходи (санкції) відповідно до Закону України «Про санкції»;

копію атестата про акредитацію, виданого Національним агентством з акредитації відповідно до ДСТУ EN ISO/IEC 17021-1:2017 та ДСТУ EN ISO/IEC 27006.

3. Заява з відповідними документами подаються заявником до Адміністрації Держспецзв’язку в паперовій або електронній формі. Електронна пошта для надсилання документів заявником вказана на сайті Держспецзв’язку в розділі «Незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури».

4. Документи, які надаються заявником на розгляд, повинні відповідати таким вимогам:

заява має бути викладена державною мовою;

документи, викладені іноземною мовою, повинні бути перекладені на державну мову із засвідченням правильності перекладу з однієї мови на іншу в установленому законодавством порядку;

заява та документи повинні містити повну та достовірну інформацію, передбачену цими Вимогами.

5. Адміністрація Держспецзв'язку погоджує зі Службою безпеки України у межах компетенції атестацію (переатестацію) заявника шляхом надання до Служби безпеки України копій документів, передбачених пунктами 1 та 2 розділу III цих Вимог, для перевірки заявника на предмет його сприяння діяльності іноземної держави, іноземної організації чи їх представників, що може завдати шкоди інтересам національної безпеки України, або інші його дії, які створюють реальні та/або потенційні загрози національним інтересам та безпеці.

Про прийняте рішення Служба безпеки України повідомляє Адміністрацію Держспецзв'язку протягом десяти робочих днів з дня отримання відповідного листа.

6. Підставами для прийняття рішення щодо не проходження атестації заявником є:

подання документів або відомостей, визначених цими Вимогами, не в повному обсязі;

невідповідність документів вимогам, які встановлені цими Вимогами;

невідповідність заявника зазначеним вище вимогам;

не підтверджена (не може бути підтверджена) достовірність наданих документів;

отримання від Служби безпеки України повідомлення про прийняте рішення щодо не погодження атестації заявника.

IV. Прийняття рішення про успішне проходження атестації заявника та включення його до Переліку

1. У разі відповідності поданої заяви та документів вимогам, що встановлені цими Вимогами, та з урахуванням повідомлення Служби безпеки України щодо погодження атестації (переатестації) заявника Адміністрація Держспецзв'язку протягом 15 робочих днів з моменту отримання заяви приймає рішення про успішне проходження атестації та включення заявника до Переліку та вносить відповідні зміни до Переліку на основі цього рішення протягом 5 робочих днів з моменту прийняття рішення.

Повідомлення заявника про успішне проходження атестації та включення його до Переліку відбувається протягом 5 робочих днів з моменту прийняття рішення шляхом надсилання листа на електронну пошту заявника.

2. У випадку прийняття рішення щодо не проходження атестації заявником Адміністрація Держспецзв'язку протягом 5 робочих днів з моменту прийняття

такого рішення повідомляє йому причини, з яких йому було відмовлено, шляхом надсилання листа на його електронну пошту.

Після усунення причин, що були підставою для прийняття рішення щодо не проходження атестації заявником, він може повторно подати документи до Адміністрації Держспецзв'язку відповідно до порядку атестації, що встановлений цими Вимогами.

3. Після успішного проходження атестації та включення фізичної особи до Переліку вона зобов'язана щороку до 1 лютого надсилати до Адміністрації Держспецзв'язку інформацію про чинний допуск до державної таємниці, чинний сертифікат «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки».

4. Після успішного проходження атестації та включення юридичної особи до Переліку вона зобов'язана щороку до 1 березня надсилати до Адміністрації Держспецзв'язку інформацію про чинний дозвіл на провадження діяльності, пов'язаної з державною таємницею, чинні сертифікати аудиторів інформаційної безпеки та трудові договори з аудиторами, яким належать ці сертифікати.

5. У разі зміни інформації, що міститься в документах, які аудитор інформаційної безпеки подав до Адміністрації Держспецзв'язку для проходження атестації відповідно до пунктів 1 та 2 розділу III цих Вимог, він зобов'язаний надати інформацію про зміни до Адміністрації Держспецзв'язку впродовж 30 календарних днів з моменту виникнення такої зміни.

V. Виключення аудиторів інформаційної безпеки з Переліку та їх переатестація

1. Рішення про скасування права на проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та виключення фізичної особи з Переліку приймається у разі:

ведення кримінального провадження та в разі висунення обвинувального вироку за вчинення умисного кримінального правопорушення. Дані про фізичну особу в Переліку відновлюються у разі закриття кримінального провадження з виправдовувальним вироком або без оголошення вироку;

порушення аудитором інформаційної безпеки законодавства у сфері захисту інформації та кібербезпеки, що підтверджено рішенням суду або рішенням органу державної влади;

зміни особистої інформації, інформації щодо чинного сертифіката «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки», «Керівник команди з аудиту систем менеджменту інформаційної безпеки», що призвели до невиконання вимог, визначених пунктом 1 розділу II цих Вимог;

позбавлення допуску до державної таємниці;

отримання від Служби безпеки України повідомлення з аргументованою пропозицією щодо виключення аудитора інформаційної безпеки з Переліку у зв'язку зі його сприянням діяльності іноземної держави, іноземної організації чи їх представників, що може завдати шкоди інтересам національної безпеки України, або іншими діями аудитора інформаційної безпеки, які створюють реальні та/або потенційні загрози національним інтересам та безпеці;

отримання заяви у довільній формі від аудитора інформаційної безпеки про припинення діяльності аудитора інформаційної безпеки на об'єктах критичної інфраструктури за власним бажанням.

2. Рішення про скасування права на проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та виключення юридичної особи з Переліку приймається у разі:

порушення юридичною особою вимог законодавства у сфері захисту інформації та кібербезпеки, що підтверджено рішенням суду або рішенням органу державної влади;

зміни інформації щодо трудових відносин з аудиторами інформаційної безпеки, що призвели до невиконання юридичною особою вимог до заявників, визначених пунктом 3 розділу II цих Вимог;

скасування або закінчення дії атестата про акредитацію, виданого Національним агентством з акредитації відповідно до ДСТУ EN ISO/IEC 17021-1:2017 та ДСТУ EN ISO/IEC 27006;

скасування або закінчення дії дозволу на провадження діяльності, пов'язаної з державною таємницею;

отримання від Служби безпеки України повідомлення з аргументованою пропозицією щодо виключення аудитора інформаційної безпеки з Переліку у зв'язку зі його сприянням діяльності іноземної держави, організації чи їх представникам, що може завдати шкоди інтересам національної безпеки України, або іншими діями аудитора інформаційної безпеки, які створюють реальні та/або потенційні загрози національним інтересам та безпеці;

отримання заяви у довільній формі від аудитора інформаційної безпеки про припинення діяльності аудитора інформаційної безпеки на об'єктах критичної інфраструктури за власним бажанням.

3. У разі виключення аудитора інформаційної безпеки з Переліку для проходження переатестації, поновлення права на проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та включення його до Переліку він повинен подати до Адміністрації Держспецзв'язку документи відповідно до положень розділу III цих Вимог.

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

Додаток 1
до Вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації)
(пункт 1 розділу III)

Заява
про проходження атестації та включення до Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури (для фізичних осіб)

1. Заявник _____
(прізвище, власне ім'я, по батькові (у разі наявності))

2. Дата народження _____

3. Реквізити документа, що підтверджує особу _____

_____
(найменування документа, серія, номер, ким виданий і коли)

4. Ідентифікаційний код _____

5. Адреса для листування _____

_____
(поштовий індекс, область/Автономна Республіка Крим, район, населений пункт, вулиця/провулок, площа тощо, № будинку/корпусу, № квартири/офісу)

6. Контактний телефон _____, електронна пошта _____

7. До заяви додаю:

_____
(повний перелік документів, що додаються до заяви, із зазначенням для кожного: копія чи оригінал, найменування, номер, дата видачі документа)

_____
_____
_____
_____
_____

_____ _____
(дата) *(підпис)*

* Примітка. Документи, що додаються до заяви, визначені у Вимогах до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації).

Додаток 2
до Вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації) (пункт 2 розділу III)

Заява
про проходження атестації та включення до Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури (для юридичних осіб)

1. Заявник _____
(повне найменування юридичної особи)

_____
(код платника податків згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб - підприємців та громадських формувань або податковий номер)

_____
(код Класифікації видів економічної діяльності (КВЕД))

має намір провадити діяльність у сфері аудиту інформаційної безпеки на об’єктах критичної інфраструктури і просить включити його до Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури.

2. Місцезнаходження заявника _____

_____

3. Адреса для листування _____

_____
(поштовий індекс, область/Автономна Республіка Крим, район, населений пункт, вулиця/провулок, площа тощо, № будинку/корпусу, № квартири/офісу)

4. Контактний телефон _____, електронна пошта _____

5. Адреса вебсайту у мережі Інтернет (URL) _____

6. Прізвище, власне ім'я, по батькові (у разі наявності) керівника _____

7. Номер і дата видачі атестата про акредитацію, виданого Національним агентством з акредитації

_____

Керівник _____ _____
(підпис) (власне ім’я, прізвище)

«___» _____ 20__ року

М.П.

_____

Прим. № ___

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

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-93-08, факс: (044) 281-94-83,
e-mail: info@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

_____ № _____ На № _____ від _____

Державна регуляторна служба
України

Адміністрація Державної служби спеціального зв'язку та захисту інформації України відповідно до статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» надсилає на погодження проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)» (далі – проєкт наказу).

Додатки: 1. Проєкт наказу на 11 арк.
2. Пояснювальна записка до проєкту наказу на 4 арк.
3. Аналіз регуляторного впливу до проєкту наказу на 10 арк.
4. Повідомлення про оприлюднення проєкту наказу на 1 арк.

Голова Служби Юрій МИРОНЕНКО

Катерина Барсукова 067 424 15 92

Повідомлення про оприлюднення проєкту наказу Адміністрації Держспецзв'язку «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)»

Регуляторна діяльність | Проєкти регуляторних актів | 10.07.2023 12:15

1. Стислий виклад змісту проєкту акта

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)» розроблено відповідно до пункту 2 постанови Кабінету Міністрів України від 24 березня 2023 року № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури», яким передбачено, що Адміністрація Державної служби спеціального зв'язку та захисту інформації повинна забезпечити затвердження вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації).

Необхідність прийняття наказу зумовлена відсутністю кваліфікованих аудиторів для проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, що унеможливлює збір відомостей щодо реального стану їх інформаційної безпеки та перешкоджає впровадженню системного підходу до врегулювання питання захисту критичної інфраструктури на загальнодержавному рівні.

Документ визначає основні вимоги до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури, а також порядок їх атестації (переатестації).

2. Адреси для зауважень та пропозицій до проєкту акта

Адміністрації Державної служби спеціального зв'язку та захисту інформації України:
поштова: вул. Солом'янська, 13, м. Київ, 03110;
електронна: info@cip.gov.ua
електронна відповідального підрозділу: audit@cip.gov.ua

Державної регуляторної служби України:
поштова: вул. Арсенальна, 9/11, м. Київ, 01011;
електронна: inform@drs.gov.ua

3. Обраний спосіб оприлюднення проєкту акта

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

4. Строк, протягом якого приймаються зауваження та пропозиції

Пропозиції та зауваження до проєкту наказу просимо надсилати протягом місяця з дати його оприлюднення.

5. Спосіб надання зауважень та пропозицій

Зауваження та пропозиції до проєкту акта надсилати на адреси, зазначені у пункті 2.

АРВ наказ.doc | Проєкт наказу та Вим ...