Прим. № 6

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

22.04.2020 № 11/01/01-782 На № _____ від _____

Голові Правління Інтернет Асоціації України

Анатолію ПЯТНІКОВУ

вул. О. Гончара, буд. 15/3, офіс 22, м.Київ, 04053

Шановний пане Анатолію!

В Адміністрації Держспецзв'язку опрацьовано листа Інтернет Асоціації України від 28.04.2020 № 53/2 щодо проєкту постанови Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» (далі – проєкт постанови).

За результатами опрацювання повідомляємо про позицію Адміністрації Держспецзв'язку щодо наданих зауважень та пропозицій до проєкту постанови.

1. Щодо непоширення дії проєкту постанови на мікро- та малі підприємства (зауваження відхилено).

Питання щодо непоширення дії проєкту постанови на мікро- та малі підприємства, які надають телекомунікаційні послуги було враховано у попередній редакції проєкту постанови, після чого НАЗК провело його антикорупційну експертизу та надало висновок, в якому зазначено, що проєкт постанови містить корупціогенні фактори та потребує доопрацювання з урахуванням наданих рекомендацій:

https://nazk.gov.ua/uk/documents/vysnovok-antykoruptsijnoyi-ekspertyzy-proyektu-postanovy-kabinetu-ministriv-ukrayiny-deyaki-pytannya-provedennya-nezalezhnogo-audytu-informatsijnoyi-bezpeky-na-ob-yektah-krytychnoyi-infrastruktury/

Одним з корупціогенних факторів в проєкті постанови, виявлених НАЗК, були положення про незастосування вимог щодо проведення аудиту до мікро-

та малих підприємств, які надають телекомунікаційні послуги, зокрема як такі, що не відповідають вимогам Закону України «Про основні засади забезпечення кібербезпеки України».

У зв'язку з чим, відповідно до рекомендацій, зазначених у висновку НАЗК, Адміністрація Держспецзв'язку виключила положення про незастосування вимог щодо проведення аудиту до мікро- та малих підприємств, які надають телекомунікаційні послуги з проєкту Порядку проведення незалежного аудиту на об'єктах критичної інфраструктури та проєкту Вимог щодо проведення незалежного аудиту кібербезпеки на об'єктах критичної інфраструктури, як такі, що є джерелами корупційних ризиків.

2. Щодо фінансово-економічного обгрунтування та аналізу регуляторного впливу до проєкту поставнови.

Питання фінансового забезпечення заходів кібербезпеки визначено статтею 13 Закону України «Про основні засади забезпечення кібербезпеки України».

Фінансово-економічні розрахунки та аналіз регуляторного впливу до проєкту постанови з доопрацьованим за результатами громадського обговорення проєктом постанови, будуть розміщені на офіційному вебсайті Держспецзв'язку (https://www.dsszzi.gov.ua).

3. Щодо визначення переліку об'єктів критичної інфраструктури та поняття «незалежний аудит інформаційної безпеки», а також формування відповідних положень на рівні законів (зауваження відхилено).

Відповідно до частини третьої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» Порядок формування переліку об'єктів критичної інформаційної інфраструктури, перелік таких об'єктів та порядок їх внесення до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

На даний час, постановою Кабінету Міністрів України від 09.10.2020 № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» затверджено Порядок формування переліку об'єктів критичної інформаційної інфраструктури, порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

Також, постановою Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури» затверджено Порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік секторів (підсекторів), основних послуг критичної інфраструктури держави та Методику категоризації об'єктів критичної інфраструктури.

Термін «незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури» пропонується визначити у проєкті Вимог щодо проведення аудиту інформаційної безпеки на об'єктах критичної інфраструктури, які затверджуватимуться проєктом постанови.

Крім того, вимога щодо прийняття Порядку проведення незалежного аудиту на об'єктах критичної інфраструктури та Вимог щодо проведення незалежного аудиту кібербезпеки на об'єктах критичної інфраструктури встановлена нормами Закону України «Про основні засади забезпечення кібербезпеки України» та не потребує формування відповідних положень додатковим законом.

4. Щодо пункту 4 проєкту Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (зауваження враховано).

Зауваження Інтернет Асоціації України стосовно пункту 4 проєкту Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури враховано шляхом виключення пункту 4 з проєкту Порядку.

5. Щодо прав та обов'язків власників та/або керівників об'єктів критичної інфраструктури (зауваження відхилено).

Проєктом Вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури передбачено, що аудитор здійснює оцінку поточного стану інформаційної безпеки на об'єктах критичної інфраструктури та його відповідності вимогам, процедурам та методикам, визначеним у договорі між власником та/або керівником об'єкта критичної інфраструктури та аудитором. Так, в зазначеному договорі визначатимуться, зокрема, й права та обов'язки власника та/або керівника об'єкта критичної інфраструктури.

6. Щодо визначення переліку актів законодавства та стандартів на відповідність, яких здійснюється оцінка відповідності стану інформаційної безпеки на об'єктах критичної інфраструктури (зауваження відхилено).

Відповідно до підпункту 5 пункту 13 проєкту Вимог щодо проведення незалежного аудиту кібербезпеки на об'єктах критичної інфраструктури звіт незалежного аудиту повинен містити необхідну інформацію згідно з умовами договору, зокрема перелік національних та міжнародних стандартів інформаційної безпеки, на основі яких проведено незалежний аудит та обґрунтування можливості застосування переліку вимог зі стандартів інформаційної безпеки до сфери діяльності об'єкта критичної інфраструктури.

Крім того, відповідно до частини другої статті 23 Закону України «Про стандартизацію» національні стандарти та кодекси усталеної практики застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами.

В свою чергу, вимоги щодо обов'язковості застосування відповідних національних стандартів під час впровадження заходів інформаційної безпеки, як і самі вимоги щодо впровадження заходів інформаційної безпеки на об'єктах критичної інфраструктури повинні бути визначені нормативно-правовими

актами, що регулюють питання саме впровадження заходів інформаційної безпеки на об'єктах критичної інфраструктури, а не перевірки стану їх дотримання (незалежного аудиту).

Так, організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури визначено Загальними вимогами до кіберзахисту об'єктів критичної інфраструктури, затвердженими постановою Кабінету Міністрів України від 19.06.2019 № 518, абзацом першим пункту 7 яких передбачено, що виконання Загальних вимог до кіберзахисту перевіряється під час незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури.

З повагою

Голова Служби Юрій ЩИГОЛЬ

Олег Шикер 281 88 37