



ДЕРЖАВНА РЕГУЛЯТОРНА СЛУЖБА УКРАЇНИ

вул. Арсенальна, 9/11, м. Київ, 01011, тел./факс (044) 239-76-40
E-mail: inform@drs.gov.ua, Сайт: www.drs.gov.ua, код згідно з ЄДРПОУ 39582357

від _____ № _____ на № _____ від _____ 20__ р.

РІШЕННЯ

про погодження проекту регуляторного акта

Державна регуляторна служба України відповідно до Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» розглянула доопрацьований проект постанови Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» (далі – проект постанови), а також документи, що додаються до проекту постанови, подані листами Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.07.2020 № 11/01/01-1191 та від 26.08.2020 № 11/01/01-1337.

За результатами проведеного аналізу проекту постанови та його аналізу регуляторного впливу на відповідність вимогам статей 4, 5, 8 і 9 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності», керуючись частиною четвертою статті 21 цього Закону, Державна регуляторна служба України

вирішила:

погодити проект постанови Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури».

Т. в. о. Голови

Олег МІРОШНІЧЕНКО





КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2020 р. №

Київ

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

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

1. Затвердити такі, що додаються:

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

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

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

ведення переліку атестованих аудиторів інформаційної безпеки;

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

у разі успішного проходження незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури, організувати проведення наступного аудиту, не рідше ніж один раз на три роки;

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

Прем'єр-міністр України

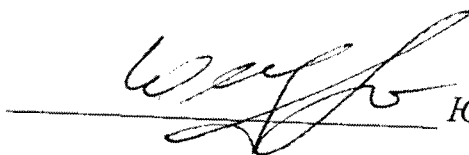
Д. ШМИГАЛЬ

Юрій ШИГОЛЬ

14. Звіт незалежного аудиту складається з двох частин:

- 1) огляду, що містить загальну інформацію про цілі, предмет проведення аудиту, яка зазначена у підпунктах 1-7 пункту 13 цих Вимог та стислу оцінку стану інформаційної безпеки, основні (стратегічні) рекомендації щодо обробки (уникнення, зменшення, перекладання чи прийняття) ризиків;
- 2) основної частини, що містить відомості, зазначені в підпунктах 8-11 пункту 13 цих Вимог, їх аналіз та детальні рекомендації.

15. Аудитор несе відповідальність за конфіденційність, повноту, достовірність, об'єктивність відомостей, зазначених у Звіті незалежного аудиту, а також за інші зобов'язання згідно умов договору.



Юрій ЩИГОЛЬ

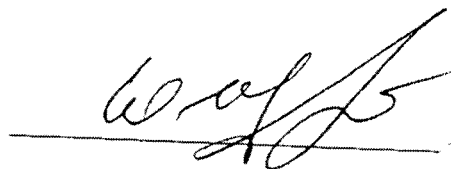
2) отримувати необхідну інформацію від власника та/або керівника і працівників об'єктів критичної інфраструктури, на яких проводиться аудит, в усній чи письмовій формі;

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

10. Власник та/або керівник об'єкта критичної інфраструктури має право самостійно обирати аудитора 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 та договору, зазначеного у пункті 5 цього Порядку.



Юрій ЩИГОЛЬ