ДЕРЖАВНА РЕГУЛЯТОРНА СЛУЖБА УКРАЇНИ

вул. Арсенальна, 9/11 м. Київ 01011, тел. (044) 254-56-73, факс (044) 254-43-93
E-mail: inform@dkrp.gov.ua, Web: http://www.drs.gov.ua, код ЄДРПОУ 39582357

від _____ №_____

на №_____від_____

Рішення №_____ від _____2019 р.
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 «Про затвердження Вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» (далі - проект постанови) та документи, додані до проекту постанови, подані листом Державної служби спеціального зв'язку та захисту інформації України від 15.01.2019 № 11/01/01-69.

За результатами проведеного аналізу доопрацьованого 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» та керуючись частиною 5 статті 21 цього Закону, Державна регуляторна служба України

вирішила:

погодити проект постанови Кабінету Міністрів України «Про затвердження Вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури».

Голова **К. ЛЯПІНА**

Кривошей О.В. 2545825

Кривошей Олена Володимирівна

Проект

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

П О С Т А Н О В А

від _____ 2019 р. №____

Київ

Про затвердження Вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та Порядку 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:

вести перелік атестованих аудиторів інформаційної безпеки;

аналізувати звіти незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

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

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

за результатами проведеного аудиту інформаційної безпеки упродовж 30 робочих днів подавати до Адміністрації Держспецзв'язку звіт аудиту інформаційної безпеки та план уникнення (зменшення, перекладання чи прийняття) ризиків.

4. Ця постанова набирає чинності після затвердження переліку об'єктів критичної інфраструктури.

Прем'єр-міністр України **В. ГРОЙСМАН**

_____ Л.О. Євдоченко

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

2) повідомляти власників (розпорядників) та/або керівників об'єкта критичної інфраструктури, уповноважених ними осіб про виявлені під час проведення аудиту ІБ уразливості автоматизованих систем та/або критичних бізнес/операційних процесів;

3) надавати консультації щодо обробки (уникнення, зменшення, перекладання чи прийняття) ризиків;

4) не розголошувати та не використовувати в своїх інтересах або інтересах третіх осіб інформацію, отриману при проведенні аудиту ІБ;

5) відповідати перед власником (розпорядником) та/або керівником об'єкта критичної інфраструктури за порушення умов Договору та законодавства України відповідно до законодавства;

6) відповідати за незаконне розголошення інформації, отриманої при проведенні аудиту ІБ відповідно до законодавства;

13. Права аудиторів ІБ (фірм ІБ):

1) самостійно визначати процедури і методики проведення аудиту ІБ, користуючись нормами чинного законодавства України, національних та міжнародних стандартів аудиту ІБ, відповідно до умов Договору та особливостей об'єкта критичної інфраструктури;

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

14. Власник (розпорядник) та/або керівник об'єкта критичної інфраструктури має право самостійно обирати аудитора ІБ (фірму ІБ) для проведення аудиту ІБ крім випадків, передбачених Вимогами щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

15. За неналежне виконання своїх обов'язків аудитор ІБ (фірма ІБ) несе майнову та іншу відповідальність відповідно до Договору та законодавства України.

16. Усі спори стосовно невиконання умов Договору, а також спори майнового характеру між аудитором ІБ (фірмою ІБ) та власником та/або керівником об'єкта критичної інфраструктури вирішуються в установленому законом порядку.

Л.О. Євдоченко

12. У випадках надзвичайних ситуацій, що призвели або можуть призвести до людських або значних матеріальних втрат, власник (розпорядник) та/або керівник об'єкта критичної інфраструктури має організувати проведення аудиту ІБ, а Адміністрація Держспецзв'язку має право провести аудит ІБ за рахунок державних коштів та видати рекомендації, усунення яких є обов'язковим.

13. Аудитор ІБ (фірма ІБ) не має права проводити аудит ІБ одного і того самого об'єкта критичної інфраструктури більше ніж раз на два роки.

14. Аудитор ІБ для проведення аудиту ІБ може залучати інших аудиторів ІБ за погодженням із власником (розпорядником) та/або керівником об'єкта критичної інфраструктури. Група аудиторів ІБ повинна формуватися з урахуванням компетентностей, необхідних для проведення аудиту ІБ.

15. Для визначення кількості та складу групи аудиторів ІБ для конкретного аудиту ІБ необхідно враховувати:

1) загальну компетентність групи аудиторів ІБ, необхідну для проведення аудиту ІБ;

2) обрані методи аудиту ІБ;

3) можливість аудиторів ІБ ефективно взаємодіяти з працівниками об'єкта критичної інфраструктури та між собою.

16. Звіт аудиту ІБ повинен містити повні, точні, чітко сформульовані та зрозумілі записи щодо аудиту ІБ, а також:

1) перелік національних та/або міжнародних стандартів інформаційної безпеки, на відповідність яким був проведений аудит ІБ, та обґрунтування можливості застосування стандартів інформаційної безпеки до сфери діяльності об'єкта критичної інфраструктури;

2) цілі, межі та методи проведення аудиту ІБ;

3) ідентифікацію аудитора ІБ (членів групи аудиторів ІБ або фірми ІБ) та працівників об'єкта критичної інфраструктури, які брали участь в аудиті ІБ;

4) дати та місця проведення аудита ІБ;

5) план та графік аудиту ІБ;

6) відомості аудиту ІБ;

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

8) план уникнення (зменшення, перекладання чи прийняття) ризиків.

17. Звіт аудиту ІБ повинен складатися з кількох документів:

1) огляд для керівництва, що містить коротку оцінку поточної ситуації, основні рекомендації (стратегічні) з зазначенням прогнозованого ефекту, пов'язані ризики та визначення орієнтовної вартості (за можливості).

2) повний звіт – включає всі дані, їх аналіз та детальні рекомендації; призначається для ІТ спеціалістів.

Л.О. Євдоченко