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 06.11.18 №10770/0/20-18

на №_____від_____

Рішення №_____ від _____2018 р.
про відмову в погодженні проекту регуляторного акта

Державна регуляторна служба України (далі – ДРС) 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), а також документи, що додаються до проекту постанови, подані листом Державної служби спеціального зв'язку та захисту інформації України від 27.09.2018 № 11/01/02-1714.

За результатами розгляду проекту постанови та аналізу регуляторного впливу на відповідність вимогам статей 4, 5, 8 і 9 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності»

встановлено:

проект постанови, як вбачається зі змісту аналізу регуляторного впливу, доданого до нього, розроблено з метою створення правових засад отримання об'єктивної інформації щодо стану інформаційної безпеки об'єктів критичної інфраструктури шляхом проведення незалежного аудиту інформаційної безпеки.

Для реалізації зазначеної мети проектом постанови пропонуються 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 (далі – проект Вимог та проект Порядку).

Однак, проект регуляторного акта не може бути погоджений у поданій редакції з огляду на таке.

У ході опрацювання проекту постанови у ДРС було проведено дві узгоджувальні наради, під час яких розробника було повідомлено, що редакція

проекту Вимог та проекту Порядку потребує суттєвого доопрацювання, зокрема з урахуванням таких зауважень.

Щодо редакції проекту Вимог

Частиною третьою статті 6 Закону України «Про основні засади забезпечення кібербезпеки України», на яку посилається розробник у вступній частині до проекту постанови, передбачено, що вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

Натомість, проект Вимог не містить посилань на зазначені міжнародні стандарти, стандарти Європейського Союзу та НАТО, що не дає можливості зрозуміти, яким самим вимогам має відповідати проведення незалежного аудиту.

Крім того, сама редакція проекту Вимог є не чіткою, не прозорою, містить вимоги до аудиторів інформаційної безпеки та аудиторських фірм у сфері інформаційної безпеки та не містить жодних вимог до процедури проведення незалежного аудиту.

Щодо проекту Порядку.

У пункті 1 проекту Порядку зазначено, що цей Порядок визначає процедуру організації та здійснення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, крім банківської системи України.

Згідно з Порядком подання нормативно-правових актів на державну реєстрацію до Міністерства юстиції України та проведення їх державної реєстрації, затвердженого наказом Міністерства юстиції України від 12.04.2005 №34/5, порядок - це акт, який встановлює механізм реалізації прав та обов'язків фізичних і юридичних осіб, процедуру застосування нормативно-правового акта та умови провадження певної діяльності.

Натомість редакція проекту Порядку не містить чіткого механізму реалізації прав та обов'язків фізичних і юридичних осіб при проведенні незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, а, містить, зокрема, принципи проведення незалежного аудиту, які не є предметом даного Порядку, права та обов'язкі аудиторів, які повинні визначатися у Договорі з проведення аудиту тощо.

Таким чином, редакція проекту регуляторного акта порушує статтю 5 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» в частині викладення положень регуляторного акта у спосіб, який є доступним та однозначним для розуміння особами, які повинні проваджувати або виконувати вимоги цього регуляторного акта.

Крім того, відповідно до прикінцевих та перехідних положень Закону України «Про основні засади забезпечення кібербезпеки України» на Державну службу спеціального зв'язку та захисту інформації України покладається обов'язок забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури та встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації).

Таким чином, для забезпечення принципу передбачуваності державної регуляторної політики - послідовності регуляторної діяльності, відповідності її цілям державної політики, а також планам з підготовки проектів регуляторних актів, що дозволяє суб'єктам господарювання здійснювати планування їхньої діяльності, розробнику необхідно чітко визначити Перелік об'єктів критичної інфраструктури, встановити Вимоги до аудиторів інформаційної безпеки, їх атестації (переатестації), а також доопрацювати Порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та вимоги до його проведення.

Вважаємо за доцільне, зазначені проекти розробляти комплексно з метою недопущення прийняття регуляторних актів, які є непослідовними або не узгоджуються чи дублюють діючі регуляторні акти.

Щодо підготовки АРВ до проекту постанови

У другому розділі АРВ розробником визначена мета державного регулювання проекту постанови - створення правових засад отримання об'єктивної інформації щодо стану інформаційної безпеки об'єктів критичної інфраструктури шляхом проведення незалежного аудиту інформаційної безпеки, а також зазначено, що проведення періодичного незалежного аудиту інформаційної безпеки стане обов'язковим до виконання підприємствами, установами та організаціями, які згідно із законодавством віднесені до об'єктів критичної інфраструктури.

Оскільки Перелік об'єктів критичної інфраструктури на разі не розроблений, то і АРВ до проекту постанови розробити правильно практично неможливо.

Враховуючи зазначене, повідомляємо, що АРВ до проекту постанови не відповідає вимогам Методики проведення аналізу впливу регуляторного акта, затвердженої постановою Кабінету Міністрів України від 11.03.2004 № 308 із змінами, внесеними постановою Кабінету Міністрів України від 16.12.2015 № 1151.

З огляду на вказане, розробка проекту постанови не узгоджується з одним з принципів державної регуляторної політики, встановлених статтею 4 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності», а саме, принципом передбачуваності, під яким розуміється послідовність регуляторної діяльності, відповідність її цілям державної політики, а також планам з підготовки проектів регуляторних актів, що дозволяє суб'єктам господарювання здійснювати планування їхньої діяльності та статтею 5 цього Закону, якою визначено, що забезпечення здійснення державної регуляторної політики включає, серед іншого,

недопущення прийняття регуляторних актів, які є непослідовними або не узгоджуються чи дублюють діючі регуляторні акти.

Ураховуючи викладене, керуючись частиною п'ятою статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності», Державна регуляторна служба України

вирішила:

відмовити в погодженні проекту 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 Державної регуляторної служби України **Ксенія ЛЯПІНА**

Кривошей О.В. 2545825