



Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

22.12.17 № 04/03/03-5371

Державна регуляторна служба
України

вул. Арсенальна, 9/11, м. Київ, 01011

Щодо погодження
проекту постанови

Надсилаємо на погодження проект постанови Кабінету Міністрів України «Про внесення змін до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (далі – проект постанови).

Проект постанови розроблений на виконання «Плану організації виконання Указу Президента України від 30 серпня 2017 року № 254 «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32». Враховуючи встановлені стислі строки прийняття змін до постанови Кабінету Міністрів України та невеликий обсяг змін згідно зазначеного вище документу, просимо розглянути проект постанови у п'ятиденний строк.

Зауваження до проекту постанови пропонуємо опрацювати в робочому порядку (контактна особа Ільчов М.М., тел. 281-96-83).

- Додатки: 1. Проект постанови на 3 арк., прим. № 1.
2. Порівняльна таблиця до проекту постанови на 4 арк., прим. № 1.
3. Пояснювальна записка до проекту постанови на 3 арк., прим. № 1.
4. Аналіз регуляторного впливу на 6 арк., прим. № 1.
5. Копія оприлюдненого повідомлення про оприлюднення проекту постанови, на 5 арк., прим. № 1.

Додатки тільки на адресу.

Голова Служби

Д.О. Євдокенко

№ 14622/0/19-17 від 26.12.2017

0.31



КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від _____ 2017 р. № _____

Київ

**Про внесення змін до Правил забезпечення захисту інформації в
інформаційних, телекомунікаційних та інформаційно-телекомунікаційних
системах**

Кабінет Міністрів України постановляє:

1. Внести до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 (Офіційний вісник України, 2006 р., № 13, ст. 878, № 50, ст. 3324; 2011 р., № 69, ст. 2624) зміни, що додаються.

2. Установити, що:

протягом двох років з дня набрання чинності цієї постанови, за результатами додаткових експертиз у сфері технічного захисту інформації видаються/реєструються атестати відповідності на комплексні системи захисту інформації;

експертні висновки на засоби захисту інформації, атестати відповідності на комплексні системи захисту інформації, які чинні на момент набрання чинності цієї постанови зберігають чинність протягом терміну їх дії.

3. Ця постанова набирає чинності з дня її опублікування.

Прем'єр-міністр України

В. ГРОЙСМАН

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 2017 р. № _____

ЗМІНИ,

**що вносяться до Правил забезпечення захисту інформації в інформаційних,
телекомунікаційних та інформаційно-телекомунікаційних системах**

1. Пункт 3 після абзацу третього доповнити новим абзацом такого змісту:
«недокументовані функції – функції програмних засобів, які не прописані або не відповідають тим, які прописані в документації, при використанні яких можливе порушення конфіденційності, доступності або цілісності оброблюваної інформації;».

У зв'язку з цим абзац четвертий вважати абзацом п'ятим.

2. Абзац дев'ятий пункту 11 викласти в такій редакції:

«Реєстрація спроб несанкціонованих дій із службовою та таємною інформацією, а також конфіденційною інформацією про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.».

3. Абзац другий пункту 20 викласти в такій редакції:

«Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту, та підлягають погодженню з Адміністрацією.».

4. Пункт 21 викласти в такій редакції:

«21. У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.».

Для оброблення інформації в системі, у якій забезпечується захист від витоку технічними каналами, повинні використовуватись технічні засоби із захистом.

Програмні засоби захисту інформації повинні піддаватись дослідженню на наявність недокументованих функцій. Проведення такого дослідження здійснюється під час проведення державної експертизи.

У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент проектування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.».

5. Абзац другий пункту 22 викласти в такій редакції:

«Державні органи, військові формування, органи місцевого самоврядування, які мають дозвіл на проведення робіт з технічного захисту інформації для власних потреб, організують проведення державної експертизи систем захисту на підприємствах, в установах, організаціях, закладах, військових з'єднаннях та частинах, які належать до їх сфери управління або підпорядковані їм. Порядок проведення такої експертизи встановлюється державним органом, військовим формуванням або органом місцевого самоврядування за погодженням з Адміністрацією.».

7. Пункт 23 виключити.

ПОРІВНЯЛЬНА ТАБЛИЦЯ

до проекту постанови Кабінету Міністрів України «Про внесення змін до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»

Зміст положення (норми) чинного акта законодавства	Зміст положення (норми) проекту акта
<p>Правила забезпечення захисту інформації в інформаційних, телекомунікаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджені постановою Кабінету Міністрів України від 29 березня 2006 року № 373</p>	
<p>3. У правилах наведені нижче терміни вживаються у такому значенні:</p> <p>...</p>	<p>3. У правилах наведені нижче терміни вживаються у такому значенні:</p> <p>недокументовані функції – функції програмних засобів, які не прописані або не відповідають тим, які прописані в документації, при використанні яких можливе порушення конфіденційності, доступності або цілісності оброблюваної інформації;</p>
<p>11. У системі здійснюється обов'язкова реєстрація:</p> <p>...</p> <p>Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора</p>	<p>Реєстрація спроб несанкціонованих дій з службовою і таємною інформацією, а також конфіденційною інформацією про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.</p>

Зміст положення (норми) чинного акта законодавства	Зміст положення (норми) проекту акта
<p>безпечн.</p> <p>20. Вимоги та порядок створення системи захисту встановлюються Адміністрацією Держспецзв'язку (далі - Адміністрація).</p> <p>Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту.</p>	<p>20. Вимоги та порядок створення системи захисту встановлюються Адміністрацією Держспецзв'язку (далі - Адміністрація).</p> <p>Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту, та підлягають погодженню з Адміністрацією.</p>
<p>21. У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.</p> <p>У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент</p>	<p>21. У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.</p> <p>Для оброблення інформації в системі, у якій забезпечується захист від витоку технічними каналами, повинні використовуватись технічні засоби із захистом.</p> <p>Програмні засоби захисту інформації повинні надаватись дослідженню на наявність не документованих функцій. Проведення такого дослідження здійснюється під час проведення державної експертизи у сфері технічного захисту інформації.</p> <p>У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент проектування</p>

<p>Зміст положення (норми) чинного акта законодавства</p> <p>проектування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.</p>	<p>Зміст положення (норми) проекту акта</p> <p>системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.</p>
<p>22. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації технічного і криптографічного захисту інформації встановлюється Адміністрацією.</p> <p>Органи виконавчої влади, які мають дозвіл на провадження діяльності з технічного захисту інформації для власних потреб, вправі за згодою департаменту організувати проведення державної експертизи системи захисту на підприємствах, в установах та організаціях, які належать до сфери їх управління. Порядок проведення такої експертизи встановлюється органом виконавчої влади за погодженням з Адміністрацією.</p>	<p>22. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією.</p> <p>Державні органи, військові формування, органи місцевого самоврядування, які мають дозвіл на проведення робіт з технічного захисту інформації для власних потреб, організують проведення державної експертизи систем захисту на підприємствах, в установах, організаціях, закладах, військових з'єднаннях та частинах, які належать до їх сфери управління або підпорядковані їм. Порядок проведення такої експертизи встановлюється державним органом, військовим формуванням або органом місцевого самоврядування за погодженням з Адміністрацією.</p>
<p>23. Виконавцем робіт із створення системи захисту може бути суб'єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації, необхідність проведення якого визначено технічним завданням на створення системи захисту.</p>	<p>виключили</p>

Зміст положення (норми) чинного акта законодавства	Зміст положення (норми) проекту акта
<p>— Для проведення інших видів робіт з технічного захисту інформації, на провадження яких виконавець не має ліцензії (дозволу), залучається співвиконавці, що мають відповідні ліцензії.</p> <p>— Якщо для створення системи захисту необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензії на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.</p>	

Директор Департаменту захисту інформації
Адміністрації Державної служби
спеціального зв'язку та захисту інформації України

« » 2017 року



А.І. Пушкарьов

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту постанови Кабінету Міністрів України «Про внесення змін до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»

1. Обґрунтування необхідності прийняття акта

Проект постанови Кабінету Міністрів України «Про внесення змін до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (далі – проект постанови) розроблений на виконання «Плану організації виконання Указу Президента України від 30 серпня 2017 року № 254 «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32» (далі – План організації виконання Указу Президента України) та у зв'язку з прийняттям постанови Кабінету Міністрів України від 16 листопада 2016 року № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України» (далі – Постанова 821).

Проект постанови передбачає удосконалення вимог до нормативних документів із технічного захисту інформації, на відповідність яким проводиться державна експертиза у галузі технічного захисту інформації, а саме – удосконалення вимог до програмних засобів, призначених для захисту інформації, які використовуються в державних органах, на підприємствах, в установах та організаціях державної форми власності. Проект постанови також передбачає приведення «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373 (далі – Правила) у відповідність до норм Постанови 821.

Чинна редакція постанови потребує доповнення щодо: визначення додаткових вимог щодо програмних засобів захисту інформації; встановлення обов'язкового погодження з Адміністрацією Держспецзв'язку проектів технічних завдань на створення комплексної системи захисту інформації (далі – КСЗІ). Також чинна редакція постанови потребує приведення її у відповідність до норм Постанови 821.

2. Мета і шляхи її досягнення

Основною метою проекту постанови є виконання вимог Плану організації виконання Указу Президента України, приведення Правил у відповідність до Постанови 821.

Досягнення мети здійснюється шляхом:
введення нового терміну – «недокументовані функції»;

введення норми щодо обов'язкового погодження технічних завдань на створення КСЗІ, призначених для захисту державних інформаційних ресурсів Адміністрацією Держспецзв'язку;

введення норми щодо додаткової процедури перевірки програмних засобів на наявність недокументованих функцій в рамках проведення державної експертизи в галузі технічного захисту інформації;

доповнення шляхом уточнення права військових формувань та підрозділів, які належать до сфери їх управління, організувати проведення державної експертизи в сфері технічного захисту інформації для власних потреб;

виключення норми щодо наявності у виконавця робіт із створення КСЗІ ліцензії, оскільки дане питання регулюється Постановою 821.

Таким чином, з метою удосконалення нормативно-правових актів із захисту інформації, вирішення наявних проблем у сфері забезпечення кібербезпеки, пов'язаних із наслідками здійснення кібератак на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури, приведення Правил до вимог чинного законодавства, Адміністрацією Держспецзв'язку розроблено проект постанови.

3. Правові аспекти

Правові підстави для розроблення проекту постанови визначені частиною першою статті 3 Закону України «Про Державну службу спеціального зв'язку та захисту інформації в Україні», Законом України «Про наукову та науково-технічну експертизу».

Крім того, на сьогодні діяльність у сфері технічного захисту інформації регулюється такими нормативними актами:

Законами України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 року № 93, зареєстрованим в Міністерстві юстиції України 16 липня 2007 року за № 820/14087.

Реалізація наказу не потребує внесення змін до чинних актів або визнання їх такими, що втратили чинність, а також розроблення нових нормативно-правових актів.

4. Фінансово-економічне обґрунтування

Реалізація наказу не потребує додаткових матеріальних та інших витрат.

5. Позиція заінтересованих органів

Проект постанови потребує погодження з Державною регуляторною службою України, Міністерством фінансів України, Міністерством економічного розвитку і торгівлі України, Службою безпеки України.

6. Регіональний аспект

Проект постанови не стосується питання розвитку адміністративно-територіальних одиниць.

6¹. Запобігання дискримінації

У проекті постанови відсутні положення, що містять ознаки дискримінації.

7. Запобігання корупції

Проект постанови не містить правил і процедур, які можуть містити ризики вчинення корупційних правопорушень.

Проект постанови не потребує проведення громадської антикорупційної експертизи.

8. Громадське обговорення

Проект постанови розміщено на офіційному веб-сайті Держспецзв'язку за адресою: www.dsszzi.gov.ua.

9. Позиція соціальних партнерів

Проект постанови не стосується питань соціально-трудової сфери.

10. Оцінка регуляторного впливу

Нормативно-правовий акт є регуляторним актом. Прийняття наказу не передбачає встановлення будь-яких платежів чи витрат для суб'єктів господарювання і не вимагатиме витрат бюджетних коштів.

10¹. Вплив реалізації акта на ринок праці

Проект постанови не спрямований безпосередньо на регулювання трудових відносин, а тому реалізація його положень не вплине на ринок праці.

11. Прогноз результатів

Прийняття постанови забезпечить удосконалення нормативно-правових актів із захисту інформації, вирішення наявних проблем у сфері забезпечення кібербезпеки, пов'язаних із наслідками здійснення кібератак на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури та приведе до виконання вимог чинного законодавства.

Голова Державної служби спеціального зв'язку та захисту інформації України

«___» _____ 2017 року



Леонід Євдоченко

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ

проекту постанови Кабінету Міністрів України «Про внесення змін до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»

I. Визначення проблеми

Проект нормативно-правового акта розроблено за результатами повторного відстеження результативності «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373, на виконання «Плану організації виконання Указу Президента України від 30 серпня 2017 року № 254 «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32» (далі – Указ Президента України).

На виконання Указу Президента України в проект нормативно-правового акта :

введено новий термін – «не документовані функції»;

введено норми щодо обов'язкового погодження технічних завдань на створення КСЗІ, призначених для захисту державних інформаційних ресурсів Адміністрацією Держспецзв'язку;

введено норми щодо додаткової процедури перевірки програмних засобів на наявність не документованих функцій в рамках проведення державної експертизи в галузі технічного захисту інформації;

здійснено доповнення, шляхом уточнення права військових формувань та підрозділів, які належать до сфери їх управління, організувати проведення державної експертизи в сфері технічного захисту інформації для власних потреб.

Також проектом нормативно-правового акта виключено норми щодо наявності у виконавця робіт із створення КСЗІ ліцензії, оскільки дане питання регулюється постанови Кабінету Міністрів України від 16 листопада 2016 року № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України» (далі – Постанова 821).

II. Цілі державного регулювання

Основними цілями державного регулювання, які передбачається

досягнути введенням у дію регуляторного акта, є виконання Указу Президента України, а саме – удосконалення нормативно-правових актів із захисту інформації, вирішення наявних проблем у сфері забезпечення кібербезпеки, пов'язаних із наслідками здійснення кібератак на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури.

III. Визначення та оцінка альтернативних способів досягнення цілей

Вид альтернативи	Опис альтернативи
Альтернатива 1: залишення законодавства без змін	Альтернативним способом досягнення цілей є залишення законодавства без змін. Такий спосіб не зможе забезпечити досягнення поставленої мети, оскільки не буде виконано вимоги Указу Президента України.
Альтернатива 2: прийняття акта про внесення змін	З прийняттям акта чинна система норм буде відкоригована й залишиться прозорою та однаковою для всіх суб'єктів на яких поширюється регуляторний акт, а саме. Дія регуляторного акта поширюється на органи державної влади, військові формування, органи місцевого самоврядування, підприємства, установи та організації, які обробляють інформацію вимога щодо захисту якої визначена пунктом 4 «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373. Як найбільш ефективний приймається другий варіант.

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1: залишення законодавства без змін	відсутні	відсутні
Альтернатива 2: прийняття акта про внесення змін	відсутні	відсутні

Оцінка впливу на сферу інтересів громадян. Вплив відсутній, оскільки проект постанови не стосується громадян.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	—	—	—	—	—
Питома вага групи у загальній кількості, відсотків	—	—	—	—	—

Вид альтернативи	Вигоди	Витрати
Альтернатива 1: залишення законодавства без змін	відсутні	відсутні
Альтернатива 2: прийняття акта про внесення змін	відсутні	відсутні

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

За результатами реалізації регуляторного акта очікується виконання Указу Президента України.

Розв'язання зазначених проблем можливе лише шляхом прийняття проекту регуляторного акта.

Отже, на основі вищенаведеного аналізу будемо таблицю.

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
--	---	---

Альтернатива 1: залишення законодавства без змін	1	відсутні
Альтернатива 2: прийняття акта про внесення змін	4	відсутні

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 2: прийняття акта про внесення змін	відсутні.	відсутні	
Альтернатива 1: залишення законодавства без змін	вигода відсутня	відсутні	

Рейтинг	Аргументи щодо переваги обраної альтернативи/причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 2: прийняття акта про внесення змін	Таким чином при застосуванні другої альтернативи (прийняття акта про внесення змін): відбудеться виконання Указу Президента України	Зовнішні ризики відсутні
Альтернатива 1: залишення законодавства без змін		Зовнішні ризики відсутні

--	--	--

V. Механізми та заходи, які забезпечать розв'язання визначеної проблеми

Вносяться зміни до пунктів 3, 20, 21, 22, 23 регуляторного акта, які уточнюють термінологію, вводять норми щодо обов'язкового погодження технічних завдань на створення КСЗІ, призначених для захисту державних інформаційних ресурсів Адміністрацією Держспецзв'язку; щодо додаткової процедури перевірки програмних засобів на наявність не документованих функцій в рамках проведення державної експертизи в галузі технічного захисту інформації;

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

Виконання вимог регуляторного акта не призведе до додаткових витрат з боку держави.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Термін дії регуляторного акта не обмежений у часі, оскільки заходи щодо розроблення КСЗІ вживаються постійно.

VIII. Визначення показників результативності дії регуляторного акта

Показники результативності	з 2007 по 2015 роки	2016 рік	2017 рік
Кількість виданих атестатів відповідності	4330	897	1100
Кількість виданих декларацій відповідності	1165	600	800
Кількість виданих експертних висновків	512	79	105

Надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта не передбачається.

Кількість суб'єктів господарювання та/або фізичних осіб, на яких поширюватиметься дія акта не визначена, оскільки стосується державних інформаційних ресурсів.

Рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта високий, оскільки останній опубліковано на сайті Держспецзв'язку.

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

Відстеження результативності регуляторного акта буде проводитися Адміністрацією Держспецзв'язку у строки, визначені законодавством, шляхом аналізу статистичних даних щодо проведених державних експертиз у сфері ТЗІ.

Базове відстеження буде проведено через 1 рік після набрання чинності регуляторним актом.

Повторне відстеження буде проведено через 2 роки після набрання чинності регуляторним актом для визначення результатів його дії.

Періодичне відстеження результативності здійснюватиметься кожних три роки після проведення повторного відстеження.

Відстеження результативності дії регуляторного акта буде проводитися статистичним методом із застосуванням статистичних даних.

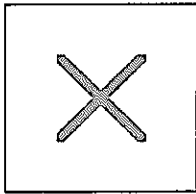
Директор Департаменту захисту інформації

Адміністрації Держспецзв'язку



А.І. Пушкарьов

«__» _____ 2017 року



24 листопада 2017



Розширений пошук

ПОВІДОМЛЕННЯ ПРО ОПРИЛЮДНЕННЯ

Про
Держспецзв'язк
у
Телекомунікації
і користування
радіочастотним
ресурсом

проекту постанови
Кабінету Міністрів
України «Про внесення
змін до Правил
забезпечення захисту
інформації в
інформаційних,
телекомунікаційних та
інформаційно-
телекомунікаційних
системах»

НОВИНИ

1. Стислий виклад змісту проекту акта

Нормативно-
правова база

Відповідно
до статті 3 Закону
України «Про
Державну службу
спеціального зв'язку
та захисту інформації
України» Адміністрація
Держспецзв'язку
повідомляє про
розроблення проекту
постанови Кабінету
Міністрів України «Про
внесення змін до
Правил забезпечення
захисту інформації в
інформаційних,
телекомунікаційних та
інформаційно-
телекомунікаційних
системах» (далі –
проект акта).

Регуляторна
діяльність

Міжнародна
діяльність

Діяльність

Стандартизація,
оцінка
відповідності
(сертифікація)
та метрологія

Оголошення

Державні
закупівлі

Проект акта
розроблено за
результатами
повторного
відстеження
результативності
Правил забезпечення
захисту інформації в
інформаційних,
телекомунікаційних та
інформаційно-

Фінансово-
економічна
діяльність

Ветеранська
організація

Зв'язки з



ГАРЯЧА ЛІНІЯ

з питань захисту прав інвесторів,
протидії незаконному
полюванню та захопленню
підприємств

044 281-92-83

УКРІНФОРМ

інформаційне агентство №1



Facebook

ВАЖЛИВА ІНФОРМАЦІЯ!

Держава турбується про тебе

Благодійна фінансова підтримка прикордонникам та
членам їх родин

ПРОВІСНИК

громадськістю [redacted] телекомунікаційних
системах,
Галузева наука [redacted] затверджених
постановою Кабінету
Консультаційни [redacted] Міністрів України від
й центр [redacted] 29 березня 2006 року
№ 373 (далі –
Правила), на
Контактна [redacted] виконання «Плану
інформація [redacted] організації виконання
Указу Президента
Запобігання [redacted] України від 30 серпня
проявам [redacted] 2017 року № 254 «Про
корупції [redacted] рішення Ради
національної безпеки і
Прес-служба [redacted] оборони України від 10
липня 2017 року «Про
Вакансії [redacted] стан виконання
рішення Ради
національної безпеки і
Доступ до [redacted] оборони України від 29
публічної [redacted] грудня 2016 року «Про
інформації [redacted] загрози кібербезпеці
держави та
невідкладні заходи з їх
Звернення [redacted] нейтралізації»,
громадян [redacted] введеного в дію
Указом Президента
України від 13 лютого
Центральна [redacted] 2017 року № 32», у
житлово- [redacted] зв'язку з прийняттям
побутова [redacted] постанови Кабінету
комісія [redacted] Міністрів України від
16 листопада 2016
Очищення влади [redacted] року № 821 «Деякі
питання ліцензування
null [redacted] господарської
діяльності з надання
послуг у галузі
криптографічного
захисту інформації
(крім послуг
електронного
цифрового підпису) та
технічного захисту
інформації за
переліком, що
визначається
Кабінетом Міністрів
України» (далі –
Постанова 821).

Чинна редакція
постанови потребує
доповнення щодо:
визначення
додаткових вимог
щодо програмних
засобів захисту

інформації;
встановлення
обов'язкового
погодження 3
Адміністрацією
Держспецзв'язку
проектів технічних
завдань на створення
комплексної системи
захисту інформації
(далі – КСЗІ). Також
чинна редакція
постанови потребує
приведення її у
відповідність до норм
Постанови 821.

Досягнення цієї мети
здійснюється шляхом:

введення нового
терміну – «не
документовані
функції»;

введення норми
щодо обов'язкового
погодження технічних
завдань на створення
КСЗІ, призначених для
захисту державних
інформаційних
ресурсів
Адміністрацією
Держспецзв'язку;

введення норми
щодо додаткової
процедури перевірки
програмних засобів на
наявність не
документованих
функцій в рамках
проведення державної
експертизи в галузі
технічного захисту
інформації;

доповнення
шляхом уточнення
права військових
формувань та
підрозділів, які
належать до сфери їх
управління,
організовувати
проведення державної
експертизи в сфері
технічного захисту

інформації для власних потреб;

виключення норми щодо наявності у виконавця робіт із створення КСЗІ ліцензії, оскільки дане питання регулюється Постановою 821.

Адреси для зауважень та пропозицій до проекту акта

Адреса розробника проекту акта:

поштова – 03110,
м. Київ, вул.
Солом'янська, 13; тел.
(044) 281-92-10, (044)
281-96-83, факс (044)
281-94-83;

електронна –
info@dsszzi.gov.ua.

Державна регуляторна служба України:

поштова – 01011,
м. Київ, вул.
Арсенальна, 9/11; тел.
(044) 254-56-73, факс
(044) 254-43-93;

електронна: inform@dkrp.gov.ua.

2. Обраний спосіб оприлюднення проекту акта

Проект акта оприлюднюється в мережі Інтернет за адресою:
www.dsszzi.gov.ua

Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України «Про внесення змін до

Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»

Звіт про повторне відстеження результативності

Порівняльна таблиця

Пояснювальна записка

3. Строк, протягом якого приймаються зауваження та пропозиції

Зауваження та пропозиції до проекту акта приймаються у період – «24» листопада 2017 року – «24» грудня 2017 року.

Зауваження та пропозиції до проекту акта необхідно надавати письмово на адреси, зазначені у пункті 2.

[Про цей сайт](#) | [Заявки](#) | [Адміністратор](#) | [Написати листа](#)

Розробник:
Корпорація
Софтлайн
(Україна)

bigmir.net хиты 2490 хосты
588



© Державна служба спеціального зв'язку та захисту інформації України