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

30.03.2018 № 04/03/03-1362

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 Ільїчов 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 13 арк., прим. № 1.
5. Копія оприлюдненого повідомлення про оприлюднення проекту постанови на 1 арк., прим. № 1.

Додатки тільки на адресу.

Голова Служби Л.О. Євдоченко

Державна регуляторна служба України
№ 5232/0/19-18 від 03.04.2018

0.31

ПРОЕКТ

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

П О С Т А Н О В А

від _____ 2018 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**

gov 04/03/03 7362

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 2018 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, де такий засіб захисту інформації використовується.».

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, організовують 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.

Прим. №__

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
Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджені постановою Кабінету Міністрів України від 29 березня 2006 року № 373	
3. У правилах наведені нижче терміни вживаються у такому значенні: …	3. У правилах наведені нижче терміни вживаються у такому значенні: **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;**
11. У системі здійснюється обов'язкова реєстрація: … ~~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~~	**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.**

07 № 24/1/03/03-7362

Зміст положення (норми) чинного акта законодавства	Зміст положення (норми) проекту акта
~~безпеки.~~	
20. Вимоги та порядок створення системи захисту встановлюються Адміністрацією Держспецзв'язку (далі - Адміністрація). Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту.	20. Вимоги та порядок створення системи захисту встановлюються Адміністрацією Держспецзв'язку (далі - Адміністрація). **Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту, та підлягають погодженню з Адміністрацією.**
21. У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю. У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент	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

Зміст положення (норми) чинного акта законодавства	Зміст положення (норми) проекту акта
проектування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.	державної експертизи системи захисту, **де такий засіб захисту інформації використовується.**
22. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією. ~~Органи виконавчої влади, які мають дозвіл на провадження діяльності з технічного захисту інформації для власних потреб, вправі за згодою департаменту організовувати 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~~.	22. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією. **Державні органи, військові формування, органи місцевого самоврядування, які мають дозвіл на проведення робіт з технічного захисту інформації для власних потреб, організовують 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.**
~~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.~~	**виключили**

Зміст положення (норми) чинного акта законодавства	Зміст положення (норми) проекту акта
~~Для проведення інших видів робіт з технічного захисту інформації, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії.~~ ~~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.~~	

Директор Департаменту захисту інформації
Адміністрації Державної служби
спеціального зв'язку та захисту інформації України
«___» _____ 2018 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»;

вх. № 04/03/03-13662

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, 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.

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 основні засади забезпечення кібербезпеки України», 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.

6[1]. 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.

10[1]. 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 Леонід Євдоченко
«___» _____ 2018 року

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ

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

І. 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) та у відповідності до Закону України «Про основні засади забезпечення кібербезпеки України».

На даний час у сфері забезпечення кібербезпеки спостерігаються наступні проблеми:

збільшення кількості комп'ютерних вірусів;

збільшення чисельності та потужності кібератак, які завдають збитків інформаційним ресурсам держави та приватного сектору економіки.

За підрахунками спеціалістів збитки України в результаті кібератаки вірусу Petya у 2017 році склали 0,4 % ВВП України, що є більше за 300 млн. доларів. Більш детально про масштаби збитків на прикладі енергетичної сфери економіки держави наведено в третьому розділі аналізу регуляторного впливу.

Оскільки нормативні вимоги до захисту державних інформаційних ресурсів не відповідають сучасним загрозам у сфері кібербезпек, дана проблема може бути розв'язана шляхом внесення відповідних змін в законодавство, зокрема в «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджені постановою Кабінету Міністрів України від 29 березня 2006 року № 373.

Слід підкреслити, що ці зміни спрямовані на захист державних інформаційних ресурсів. Приватний сектор економіки самостійно визначає ступінь захисту та належні заходи кібербезпеки власних інформаційних ресурсів.

до н 04/03/03-1362

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

- введенно новий термін – «не документовані функції»;
- введенно норми щодо обов'язкового погодження технічних завдань на створення комплексної системи захисту інформації (далі – КСЗІ), призначених для захисту державних інформаційних ресурсів Адміністрацією Держспецзв'язку;
- введенно норми щодо додаткової процедури перевірки засобів захисту інформації 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, щодо організації 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 постановою 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.

Планується, що результатом державного регулювання буде зменшення кількості збитків, які завдаються державним інформаційним ресурсам внаслідок кібератак та проникнення шкідливих вірусів. У разі невжиття відповідних заходів, передбачених проектом постанови вразливість інформаційних ресурсів держави залишається на рівні 100%, а при вжитті відповідних заходів: створення КСЗІ, призначених для захисту державних інформаційних ресурсів; перевірка засобів захисту інформації на наявність не документованих функцій вразливість державних інформаційних ресурсів зменшиться до 10%, що автоматично призведе до зменшення розміру збитків, заподіяних державі приблизно в такому ж пропорційному співвідношенні.

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. **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.** Згідно пункту 4 вищезгаданої постанови такою інформацією є: відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі – відкрита інформація); конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації» (далі - конфіденційна інформація); службова інформація; інформація, яка становить державну або іншу передбачену законом таємницю (далі - таємна інформація); інформація, вимога щодо захисту якої встановлена законом.

	Як найбільш ефективний приймається другий варіант.

Оцінка впливу на сферу інтересів держави

Слід зазначити, що в цьому розділі (дивись вище) зазначено на кого розповсюджується зміни до постанови. Щодо центральних органів виконавчої влади, міністерств, відомств, служб, фондів – це приблизно 83 суб'єкти, щодо військових формувань – ця інформація є інформацією з обмеженим доступом. Вплив розраховано.

Вид альтернативи	Вигоди	Витрати
Альтернатива 1: залишення законодавства без змін	відсутні	0,4 % ВВП України – сума збитків, заподіяних вірусом Petya в червні 2017 року
Альтернатива 2: прийняття акта про внесення змін	За підрахунками спеціалістів збитки України в результаті кібер атаки вірусу Petya у 2017 році склали 0,4 % ВВП України (дані взяті з мережі Internet), що є більше за 300 млн. доларів. Кібератаки у 2017 році було здійснено не тільки на державні підприємства, установи, організації, а й ряд підприємств, які є об'єктами критичної інфраструктури держави. Зокрема, збитки енергокомпаній України були надзвичайно великими.*	30133,92 грн. Витрати, пов'язані з перевіркою засобів захисту інформації на наявність не документованих функцій в рамках проведення державної експертизи в галузі технічного захисту інформації та погодження технічних завдань

*Кібератаки на енергетичні компанії України почались ще у 2015 році. Перша зареєстрована успішна кібератака на енергетичну систему з

виведенням її із ладу сталась 23 грудня 2015 року. Російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній України. Наступна, і набагато менш масштабна за наслідками, кібератака сталась вночі з 17 на 18 грудня 2016 року. Також кібератаку було повторно здійснено влітку 2017 року.

Наслідки кібератаки на енергетичну систему

Назва підприємства енергетики	Збитки нанесені підприємствам
«Прикарпаттяобленерго»	вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин
«Київобленерго»	З 15:31 хв. до 16:30 хв. було повністю або частково відключено близько п'ятдесяти населених пунктів у Білоцерківському, Кагарлицькому, Миронівському, Фастівському, Сквирському, Макарівському, Рокитнянському, Іванківському та Яготинському адміністративних районах, без електричної енергії були понад 80 378 споживачів. Електропостачання було відключено 30 вузлових підстанцій від яких живиться низка стратегічних об'єктів, понад 80 тисяч споживачів були без електрики протягом однієї-трьох годин
«Чернівціобленерго»	захоплення управління АСДУ з виконанням операцій вимикань на підстанціях; виведення з ладу елементів IT інфраструктури (джерела безперебійного живлення, модеми, RTU, комутатори); знищення інформації на серверах та робочих станціях (утилітою KillDisk); атака на телефонні номери кол-центрів, з метою відмови в обслуговуванні знеструмлених абонентів. Перерва в електропостачанні склала від 1 до 3,5 годин. Загальний недовідпуск — 73 МВт·год (0.015 % від добового обсягу споживання України).
«Прикарпаттяобленерго»	Приблизно о 3:30 по обіді 23 грудня 2015 року хакери зайшли в мережі SCADA через вкрадені облікові записи і віддали команди на вимкнення систем безперебійного живлення, які вони вже переконфігурували раніше. Після цього вони почали вимикати запобіжні системи, які переривали живлення. Але перед цим вони запустили атаку за методикою «відмова від обслуговування» на кол-центри обленерго, аби користувачі не могли повідомити про аварію.

В цій таблиці наведено дані щодо збитків енергетичних компаній. Також кібератаки щороку завдають збитків державним установам, підприємствам, організаціям. На жаль ці установи не надають офіційної інформації щодо розмірів цих збитків. Але ми маємо дані щодо збитків країни в цілому, щодо збитків іноземних компаній; крім того, в Internet джерелах наявна інформація, що внаслідок вірусу «Petya» тільки авто бізнес України зазнав 20 млн. євро збитків. А згідно підрахунків консалтингової компанії PricewaterhouseCoopers хакери й автори комп'ютерних вірусів у 2002 році нанесли світовій економіці збитки у розмірі $1,5 трлн. На сьогоднішній день розмір збитків ще більший.

Ці суми є дуже великими і дозволяють зробити висновки, що забезпечення належного кіберзахисту шляхом внесення змін у відповідні нормативні акти щодо посилення вимог з кібербезпеки дозволить зекономити значні суми державних коштів.

Оскільки неможливо точно спрогнозувати кількість органів державної влади, які будуть здійснювати дії щодо перевірки засобів захисту інформації на наявність не документованих функцій, кількість процедур за рік та кількість засобів захисту інформації, які підлягатимуть перевірці на наявність не документованих функцій витрати на виконання вимог регулювання, надаються виходячи із розрахунку на одного суб'єкта – органа державної влади та на одну КСЗІ.

Оцінка вартості адміністративних процедур органа державної влади щодо виконання регулювання, а саме – погодження технічних завдань на створення КСЗІ, призначених для захисту державних інформаційних ресурсів здійснюється з урахуванням тільки часових затрат, оскільки саме погодження технічних завдань є безкоштовним.

Вартість часу співробітника органу державної влади розрахована за показником місячної заробітної плати головного спеціаліста бюджетної сфери 7500 грн. (7500:21:8 = 44,64)

Процедура регулювання органу державної влади (розрахунок на один орган державної влади)	Планові витрати часу на процедуру	Вартість часу співробітника органу державної влади – головного спеціаліста (заробітна плата)	Оцінка кількості процедур за рік, що припадають на одного суб'єкта	Оцінка кількості суб'єктів, що підпадають під дію процедури регулювання*	Витрати на адміністрування регулювання, гривень
1. Підготовка інформації для відправки технічного завдання на погодження	2 год.	44,64 грн.			89,28 грн.

2.Підготовка листа на зауваження до технічного завдання у разі їх наявності	1 год.	44,64 грн.			44,64 грн.
Загалом:					133,92 грн.

* Як зазначено вище – це біля 83 суб'єктів, щодо військових формувань – ця інформація є інформацією з обмеженим доступом. Тому витрати визначено на одного суб'єкта.

Середня вартість проведення експертних досліджень засобів захисту інформації, у тому числі на наявність не документованих функцій дорівнює – 30000 грн. Вартість розрахована згідно проведеного цінового опитування серед суб'єктів господарювання, які є організаторами експертних досліджень у галузі технічного захисту інформації, і є приблизною, оскільки послуги перевірки засобів захисту інформації на наявність не документованих функцій на сьогоднішній день ще не надаються суб'єктами господарювання в Україні. Ця ж сума була застосована при здійсненні аналізу регуляторного впливу до проекту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про внесення змін до Положення про державну експертизу в сфері технічного захисту інформації», після погодження якого Державною регуляторною службою України, було внесено зміни в установленому порядку.

Оцінка впливу на сферу інтересів громадян.

Вплив відсутній, оскільки проект постанови не стосується громадян.

Оцінка впливу на сферу інтересів суб'єктів господарювання.

Дія регуляторного акта поширюється тільки 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 (тобто працюють з державними інформаційними ресурсами).

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів	*відсоткова кількість				

господарювання, що підпадають під дію регулювання, одиниць	суб'єктів не може бути визначена, оскільки дія регуляторного акта поширюється тільки на органи державної влади, військові формування, органи місцевого самоврядування, підприємства, установи та організації, які працюють з державними інформаційними ресурсами. На сьогодні це переважно є тільки державні органи, військові формування	—	—	—	—
Питома вага групи у загальній кількості, відсотків	**відсоткова кількість суб'єктів не може бути визначена з вищезазначених причин	—	—	—	—

Вид альтернативи	Вигоди	Витрати
Альтернатива 1: залишення законодавства без змін	—	—
Альтернатива 2: прийняття акта про	Якщо суб'єкт господарювання буде	Від 30133,92 грн. та вище, в залежності від

внесення змін	працювати з державними інформаційними ресурсами, то економія державних коштів (яка виникне внаслідок не завдання збитків від комп'ютерних вірусів) буде – до 0,4 % ВВП країни. Точну суму вигод неможливо спрогнозувати.	вартості експертизи в сфері технічного захисту інформації засобів захисту інформації

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 будуємо 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	Вигоди проявляються в уникненні збитків, яких може бути	30133,92 грн.	Забезпечення кібернетичної безпеки в системі органів державної влади України є одним із пріоритетних завдань в сфері

	завдано в результаті кібератак		забезпечення оборони країни в цілому. Тому виконання рішення РНБО України та, в подальшому побудова необхідної та належної системи захисту є обов'язковим.
Альтернатива 1: залишення законодавства без змін	вигода відсутня	до 0,4 % ВВП країни	У разі залишення законодавства без змін не буде виконано відповідне рішення РНБО України. Оскільки кібер атаки та проникнення комп'ютерних вірусів набирає все більших обертів в Україні і світі, то невжиття заходів до попередження таких атак призведе до значних збитків з боку держави

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 та втілення засад кібербезпеки в Україні	Зовнішні ризики відсутні
Альтернатива 1: залишення законодавства без змін		Зовнішні ризики відсутні

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

Основним механізмом для розв'язання визначеної проблеми є прийняття проекту постанови та фактична реалізація її положень.

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 засобів захисту інформації на наявність не документованих функцій в рамках проведення державної експертизи в галузі технічного захисту інформації.

Відповідно до пункту 2 проекту постанови 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. Отже буде час для приведення засобів захисту інформації та систем захисту у відповідність до нових вимог та пройти державну експертизу, порядок якої визначено «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.

Разом з тим, прийняття постанови призведе до необхідності заміни існуючих засобів обробки інформації, які не відповідають сучасним вимогам. Це потребуватиме матеріальних витрат, оскільки любий сучасний захист інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем потребує коштів.

Організаційні заходи, які необхідно здійснити для впровадження проекту постанови:

а) дії органів виконавчої влади – надання допомоги та консультацій органам державної влади, військовим формуванням, органам місцевого самоврядування, підприємствам, установам та організаціям, які працюють з державними інформаційними ресурсами; та контроль за його виконанням всіма суб'єктами на яких поширюється проект постанови.

б) дії суб'єктів господарювання – дія регуляторного акта поширюється тільки на органи державної влади, військові формування, органи місцевого самоврядування, підприємства, установи та організації, які працюють з державними інформаційними ресурсами. Тому суб'єктам господарювання, які працюють з державними інформаційними ресурсами необхідно буде пройти державну експертизу у сфері технічного захисту інформації на комплексну систему захисту інформації відповідно до встановлених законодавством єдиних для всіх суб'єктів вимог. Ці вимоги є рівними для всіх суб'єктів господарювання.

Таким чином, проектом передбачається забезпечення впровадження сучасних вимог щодо кіберзахисту державних інформаційних ресурсів, вирішення проблем у сфері забезпечення кібербезпеки, пов'язаних із наслідками здійснення кібератак на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури.

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

Проект наказу стосується інтересів держави.

Тест малого підприємництва не проводиться, оскільки неможливо підрахувати витрати на сектор регулювання.

Погодження технічного завдання на створення системи або системи захисту є безкоштовним і проводиться в рамках державної експертизи, наявні лише часові витрати.

Послуга щодо перевірки засобів захисту інформації на наявність не документованих функцій є новою і витрати пораховані в розділі ІІІ.

Негативних наслідків у зв'язку з прийняттям регуляторного акту не очікується.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Термін дії регуляторного акта не обмежений у часі, оскільки заходи щодо перевірки засобів захисту інформації в рамках проведення державної експертизи в галузі технічного захисту інформації вживаються постійно.

Зміна терміну дії акта можлива у разі зміни законодавчих актів України, на вимогах яких розроблено та базується проект регуляторного акта.

Термін набрання чинності регуляторним актом – відповідно до вимог законодавства після його офіційного оприлюднення.

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

Прогнозними значеннями показників результативності регуляторного акта є:

1. Розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних із дією акта – прямих надходжень до державного бюджету не зпередбачається.

2. Кількість суб'єктів господарювання та/або фізичних осіб, на яких поширюється дія акта – необмежена. Дія проекту регуляторного акта поширюватиметься на органи державної влади, військові формування, органи

місцевого самоврядування, підприємства, установи та організації, які працюють з державними інформаційними ресурсами

3. Рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень регуляторного акта – високий, оскільки повідомлення про оприлюднення, проект наказу та аналізу регуляторного впливу акта розміщено на офіційному веб-сайті Міністерства освіти і науки України (www.dsszzi.gov.ua, розділ "Регуляторна діяльність").

4. Час, що необхідно буде витратити суб'єктам господарювання та/або фізичним особам, для виконання вимог акта – фактично не змінюватиметься.

IX. 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 технічного захисту інформації.

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.

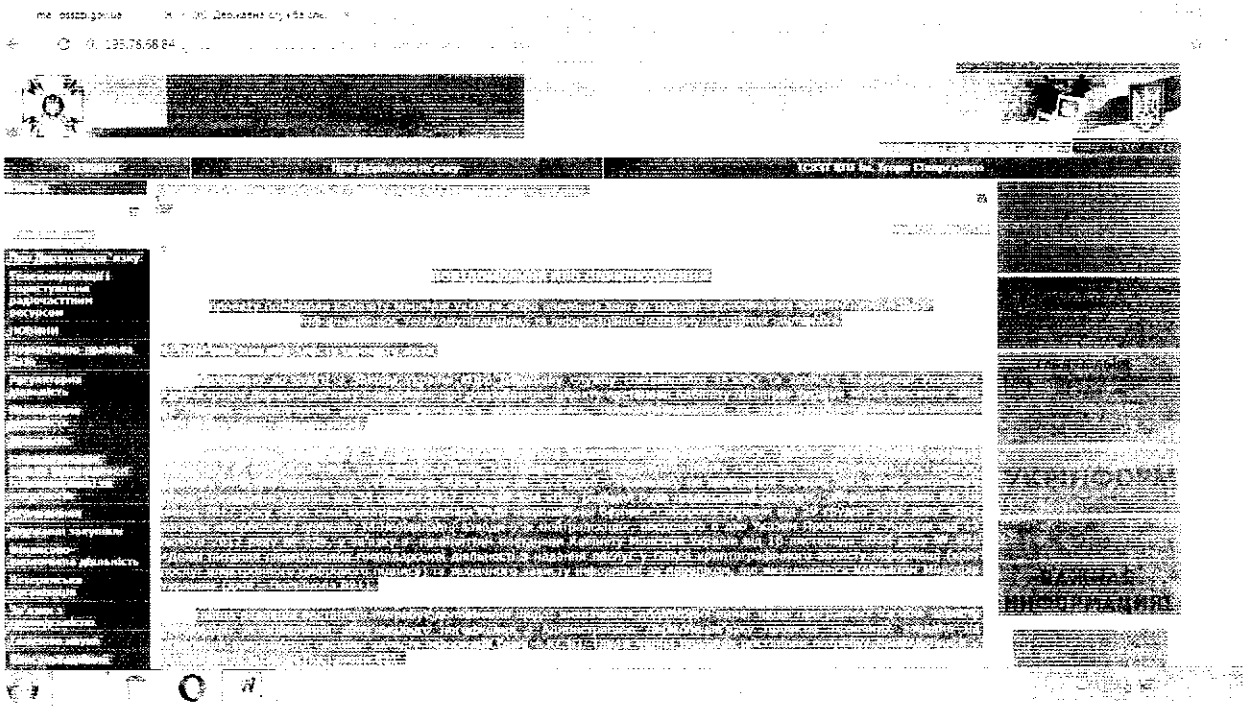
Періодичне відстеження результативності здійснюватиметься кожних три роки після проведення повторного відстеження.

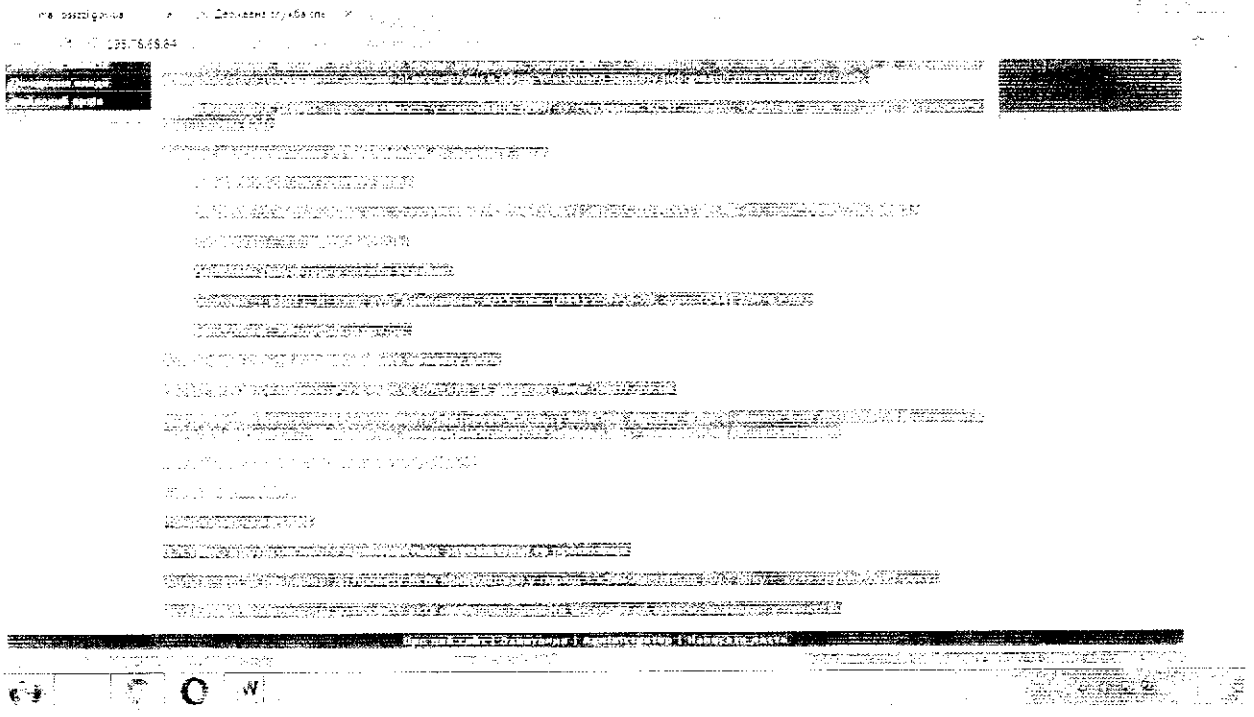
Метод проведення відстеження результативності – статистичний.

Вид даних, за допомогою яких здійснюватиметься відстеження результативності, – статистичні.

Відстеження результативності вищезазначеного регуляторного акта проводитиметься шляхом розгляду пропозицій та зауважень від суб'єктів на яких поширюється регуляторний акт, які надійшли до Адміністрації Держспецзв'язку протягом усього терміну його дії.

Директор Департаменту захисту інформації
Адміністрації Держспецзв'язку А.І. Пушкарьов
«___» _____2018 року





AV ~ 04/03/03 - 7362