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

27.09.2018 № 04/02-1719

Державна регуляторна служба України
вул. Арсенальна, 9/11, м. Київ, 01011

Щодо повторного погодження
проекту постанови

Адміністрацією Держспецзв'язку доопрацьовано 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).

Просимо у найкоротший термін опрацювати зазначений проект та погодити його в установленому порядку.

Додатки: 1. Проект Постанови на 8 аркушах.
2. Пояснювальна записка до проекту Постанови на 4 аркушах.
3. Аналіз регуляторного впливу проекту Постанови на 8 аркушах.
4. Повідомлення про оприлюднення проекту нормативно-правового акта (скріншот) на 1 аркуші.

Голова Служби Л.О. Євдоченко

Шикер 281-88-37

0.31

Проект

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

П О С Т А Н О В А

від _____ 2018 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

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2018 р. №

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

1. Ці Вимоги встановлюють основи проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури держави, крім банківської системи України.

2. Терміни, що вживаються у цих Вимогах, мають таке значення:

аудитор інформаційної безпеки (далі – аудитор ІБ) – фізична особа, яка підтвердила кваліфікаційну придатність для провадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

аудиторська фірма у сфері інформаційної безпеки (далі – фірма ІБ) – юридична особа, яка провадить діяльність аудиту інформаційної безпеки на підставах та в порядку, що передбачені цими Вимогами, Порядком проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, національними та міжнародними стандартами аудиту інформаційної безпеки;

відомості аудиту інформаційної безпеки (далі – відомості аудиту ІБ) – записи та інша інформація, отримана під час здійснення аудиту інформаційної безпеки на об'єктах критичної інфраструктури та може бути перевірена;

уразливість – нездатність інформаційної системи протистояти реалізації певної загрози або сукупності загроз;

звіт аудиту інформаційної безпеки на об'єктах критичної інфраструктури (далі – звіт аудиту ІБ) – якісна та/або кількісна оцінка ступеня відповідності стану інформаційної безпеки на об'єктах критичної інфраструктури встановленим вимогам національних стандартів та рекомендаціям міжнародних стандартів аудиту інформаційної безпеки. Звіт аудиту ІБ може містити інформацію з обмеженим доступом;

незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури (далі – аудит ІБ) – систематизований, незалежний і документований процес отримання об'єктивної оцінки стану інформаційної безпеки на об'єктах критичної інфраструктури та відповідності її встановленим вимогам національних стандартів та рекомендаціям міжнародних стандартів захисту об'єктів критичної інформаційної інфраструктури;

ризик – функція імовірності реалізації певної загрози, виду і величини завданих збитків;

тестування на проникнення – метод оцінювання захищеності інформаційної системи чи мережі шляхом часткового моделювання дій

зовнішніх зловмисників з проникнення у неї і внутрішніх зловмисників з отримання несанкціонованого доступу до інформації; таке тестування виконується з позиції потенційного порушника і може містити активне використання вразливостей.

Інші терміни вживаються у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах".

3. Аудит ІБ проводиться згідно з нормами чинного законодавства України, національних стандартів та з урахуванням рекомендацій міжнародних стандартів аудиту ІБ, та специфіки об'єкта критичної інфраструктури.

4. Фірма ІБ набуває права на провадження аудиту ІБ за умови відповідності цим Вимогам та Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

5. Загальний розмір частки засновників (учасників) фірми ІБ, які не є аудиторами ІБ не може перевищувати 30 відсотків.

6. Проведення аудиту ІБ є обов'язковим для об'єктів критичної інфраструктури.

7. Організація проведення аудиту ІБ покладається на власників та/або керівників об'єктів критичної інфраструктури.

8. Проводити аудит ІБ мають право виключно аудитори ІБ (фірми ІБ).

9. Під час аудиту ІБ обов'язково проводиться тестування на проникнення з використанням апаратно-програмних засобів пошуку та аналізу уразливостей, які мають бути погоджені власником (розпорядником) та/або керівником об'єкта критичної інфраструктури.

10. 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.

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

12. 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.

13. 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.

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

1) цілі, межі та методи проведення аудиту ІБ;

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

3) дати та місця проведення аудита ІБ;

4) план та графік аудиту ІБ;

5) відомості аудиту ІБ;

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

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

Л.О. Євдоченко

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2018 р. №

ПОРЯДОК
проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури

1. Цей Порядок визначає процедуру організації та здійснення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, крім банківської системи України.

2. У цьому Порядку під терміном "критичні бізнес/операційні процеси" слід розуміти процеси організації функціонування об'єктів критичної інфраструктури, реалізація загроз щодо яких призводить до найбільших втрат самого об'єкта критичної інфраструктури, навколишнього середовища, суспільства, держави.

Інші терміни вживаються у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах" та Вимогах щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

3. Метою проведення незалежного аудиту інформаційної безпеки (далі – ІБ) на об'єктах критичної інфраструктури є отримання об'єктивної оцінки стану інформаційної безпеки (або кібербезпеки) на об'єктах критичної інфраструктури (стан захищеності) та її відповідності встановленим вимогам національних стандартів та рекомендаціям міжнародних стандартів інформаційної безпеки (або кіберзахисту) об'єктів критичної інфраструктури і надання рекомендацій щодо уникнення (зменшення, перекладання чи прийняття) ризиків.

4. Проведення незалежного аудиту ІБ (далі – аудит ІБ) базується на таких принципах:

1) незалежність аудиторів ІБ. Аудитори ІБ (фірми ІБ) незалежні в своїй діяльності та не мають конфлікту інтересів. Незалежність є основою для неупередженості при проведенні аудиту ІБ та об'єктивності при формуванні висновків аудиту ІБ;

2) повнота аудиту ІБ. Обсяг аудиту ІБ повинен бути достатнім для формування об'єктивних висновків щодо стану інформаційної безпеки на об'єктах критичної інфраструктури (стан захищеності) та її відповідності встановленим вимогам національних стандартів та рекомендаціям міжнародних стандартів інформаційної безпеки;

3) однозначність висновків. Висновки аудиту ІБ повинні однозначно кваліфікувати ступені ризику;

4) етичність поведінки. Етичність поведінки аудитора ІБ (представників фірми ІБ) базується на відповідальності, непідкупності, неупередженості;

5) конфіденційність. Аудитор ІБ (фірма ІБ) несе відповідальність за розголошення інформації, отриманої під час аудиту ІБ, відповідно до чинного законодавства.

5. Основні етапи проведення аудиту ІБ на об'єктах критичної інфраструктури:

1) організація проведення аудиту ІБ;

2) попередній аналіз документів;

3) підготовка плану аудиту ІБ;

4) збір відомостей аудиту ІБ;

5) аналіз зібраних даних;

6) підготовка звіту за результатами аудиту ІБ;

7) розробка та затвердження плану уникнення (зменшення, перекладання чи прийняття) ризиків.

6. На першому етапі власником (розпорядником) та/або керівником об'єкта критичної інфраструктури ініціюється зустріч з аудиторами ІБ, на якій укладається договір з проведення аудиту ІБ (далі – Договір) та узгоджуються питання щодо:

1) цілей, меж та методів проведення аудиту ІБ;

2) отримання доступу до документів, необхідних для планування аудиту ІБ;

3) порядку доступу до інформації з обмеженим доступом, встановленого власником (розпорядником) та/або керівником об'єкта критичної інфраструктури;

4) підготовки до проведення аудиту ІБ, встановлення його строків;

5) необхідності у супроводженні уповноваженими представниками власника та/або керівника об'єкта критичної інфраструктури аудитора ІБ під час проведення аудиту ІБ.

7. Аудитор ІБ (фірма ІБ) складає план проведення аудиту ІБ (далі – План) на основі аналізу отриманих документів та результатів попередніх аудитів ІБ (за наявності).

8. При складанні Плану аудитор ІБ (фірма ІБ):

1) визначає нормативні вимоги (політики, стандарти, керівні принципи та процедури), за якими побудовано захист об'єкта критичної інформаційної інфраструктури;

2) деталізує межі та цілі аудиту ІБ;

3) виконує аналіз ризиків;

4) розробляє покрокову процедуру проведення аудиту ІБ;

5) визначає необхідні ресурси для аудиту ІБ.

9. План погоджується з власником (розпорядником) та/або керівником об'єкта критичної інфраструктури.

10. Для отримання відомостей аудиту ІБ аудитор ІБ (фірма ІБ):

1) проводить інтерв'ю (анкетування) та спостереження за діями персоналу;

2) використовує загальне чи спеціалізоване аудиторське програмне забезпечення для аналізу вмісту файлів та файлів налаштувань програмного і програмно-апаратного забезпечення;

3) переглядає та аналізує параметри автоматизованих систем безпосередньо під час зустрічей із відповідальними співробітниками;

4) використовує попередні аудиторські звіти та аналізує системні журнали, журнали реєстрації подій та логи програмного і програмно-апаратного забезпечення;

5) аналізує технічну документацію та документацію користувача, рекомендації постачальника компонентів автоматизованих систем;

6) аналізує налаштування компонентів автоматизованих систем;

7) аналізує організаційну структуру автоматизованих систем;

8) узагальнює отримані фактичні дані про стан кіберзахисту на об'єкті критичної інфраструктури та перевіряє їх відповідність вимогам національних стандартів та рекомендаціям міжнародних стандартів інформаційної безпеки.

11. Відповідно до встановлених Договором строків аудитор ІБ (фірма ІБ) надає власнику (розпоряднику) та/або керівнику об'єкта критичної інфраструктури звіт аудиту ІБ та рекомендації для уникнення (зменшення, перекладання чи прийняття) ризиків.

12. Аудитори ІБ (фірми ІБ) під час проведення аудиту ІБ зобов'язані:

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;

6) відповідати за незаконне розголошення інформації, отриманої при проведенні аудиту ІБ.

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;

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 несе відповідальність за невиконання плану уникнення (зменшення, перекладання чи прийняття) ризиків.

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до 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"

Мета: визначення основних вимог та механізму впровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

1. Підстава розроблення проекту акта

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) розроблено на виконання частини третьої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" щодо впровадження системи незалежного аудиту інформаційної безпеки та абзацу четвертого пункту 1 Плану організації підготовки проектів актів, необхідних для забезпечення реалізації Закону України "Про основні засади забезпечення кібербезпеки України", схваленого на засіданні Кабінету Міністрів України 22 листопада 2017 року (протокол № 66).

2. Обґрунтування необхідності прийняття акта

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії їм та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для вчинення терористичних актів.

Аналіз кіберзагроз свідчить, що кібератаки на комунікаційні системи та системи управління технологічними процесами об'єктів критичної інфраструктури держави таких галузей, як енергетика, хімічна промисловість та інші можуть призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Водночас набуття чинності Законом України "Про основні засади забезпечення кібербезпеки України" визначає, що до Переліку об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту,

інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами потенційно небезпечних технологій і виробництв.

На сьогодні результатом кібератак є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування об'єктів критичної інфраструктури, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку з цим з урахуванням потреб національної безпеки і необхідності системного підходу до розв'язання проблеми на загальнодержавному рівні отримання відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Необхідність прийняття постанови зумовлена відсутністю відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури та, як наслідок, унеможливлює системний підхід до розв'язання проблеми захисту критичної інфраструктури на загальнодержавному рівні.

Проблеми забезпечення належного рівня інформаційної безпеки на об'єктах критичної інфраструктури не можуть бути розв'язані без існування систематизованого підходу до аналізу стану захисту інформації, який базувався би на реальних показниках, отриманих під час проведення незалежного аудиту інформаційної безпеки.

3. Суть проекту акта

Проектом постанови пропонується 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.

4. Правові аспекти

У цій сфері правового регулювання діють такі основні нормативно-правові акти:

Закон України "Про основні засади забезпечення кібербезпеки України";

Закон України "Про Державну службу спеціального зв'язку та захисту інформації України";

Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27.01.2016 "Про Стратегію кібербезпеки України";

Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затверджене постановою КМУ від 03.09.2014 № 411.

5. Фінансово-економічне обґрунтування

Оцінити витрати з державного бюджету на реалізацію проекту постанови буде можна після визначення переліку об'єктів критичної інфраструктури.

6. Прогноз впливу

Оцінити вплив проекту постанови за предметом правового регулювання на забезпечення прав та інтересів суб'єктів господарювання і держави буде можна після визначення переліку об'єктів критичної інфраструктури.

Проект постанови за предметом правового регулювання не впливає на ринкове середовище, розвиток регіонів, забезпечення прав громадян, ринок праці, громадське здоров'я, екологію та навколишнє природне середовище та інші сфери суспільних відносин.

7. Позиція заінтересованих сторін

Реалізація постанови не матиме впливу на інтереси окремих верств (груп) населення, об'єднаних спільними інтересами.

Проект постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку.

Проект постанови не стосується соціально-трудової сфери.

Проект постанови не стосується сфери наукової та науково-технічної діяльності.

8. Громадське обговорення

Проект постанови розміщено на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.

9. Позиція заінтересованих органів

Проект постанови потребує погодження з Міністерством оборони України, Міністерством економічного розвитку і торгівлі України, Міністерством фінансів України, Міністерством внутрішніх справ України, Міністерством енергетики та вугільної промисловості України, Міністерством інфраструктури України, Генеральним штабом Збройних Сил України, Службою безпеки України, Службою зовнішньої розвідки України, Державною регуляторною службою України, Національною поліцією України, Державним агентством з питань електронного урядування, Національним банком України.

10. Правова експертиза

Проект постанови потребує проведення правової експертизи Мін'юстом.

11. Запобігання дискримінації

У проекті постанови немає положень, які містять ознаки дискримінації. Громадська антидискримінаційна експертиза не проводилася.

12. Запобігання корупції

У проекті постанови немає правил і процедур, які можуть містити ризики вчинення корупційних правопорушень. Громадська антикорупційна експертиза не проводилася.

13. Прогноз результатів

Прийняття постанови дозволить налагодити моніторинг стану захищеності інформаційних ресурсів об'єктів критичної інфраструктури, що дасть можливість отримати відомості про реальний стан ІБ як на окремих об'єктах критичної інфраструктури, регіонах, так і в державі в цілому в реальному часі. Зазначене дасть можливість централізованого аналізу та надання рекомендацій щодо усунення вразливостей в системах ІБ та застосування гармонізованих із міжнародними та європейськими стандартами вимог щодо захисту інформації на території України.

Оцінити вплив постанови на ключові інтереси заінтересованих сторін, окремих верств (груп) населення, об'єднаних спільними інтересами та суб'єктів господарювання буде можна після затвердження переліку об'єктів критичної інфраструктури держави.

Голова Державної служби спеціального
зв'язку та захисту інформації України Леонід Євдоченко
«___» _____ 2018 року

Аналіз регуляторного впливу

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"

1. Визначення проблеми

Відповідно до частини третьої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" Адміністрацією Держспецзв'язку розроблено 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).

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії їм та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для вчинення терористичних актів.

Аналіз кіберзагроз свідчить, що кібератаки на комунікаційні системи тасистеми управління технологічними процесами об'єктів критичної інфраструктури держави таких галузей, як енергетика, хімічна промисловість та інші можуть призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави.

Так, протягом останніх трьох років на інформаційно-телекомунікаційні системи деяких об'єктів, які за своїм значенням і роллю для життєдіяльності суспільства є об'єктами критичної інфраструктури, здійснено низку масштабних кібератак, зокрема:

1) 21 - 25 травня 2014 відбулися DDoS-атаки і злом сайту ЦВК під час президентських виборів, внаслідок яких на сайті з'явилися помилкові результати. Незважаючи на повідомлення про злом, саме ці дані були озвучені в новинах на російському Першому каналі як реальні результати виборів в Україні;

2) у червні 2014 року на серверах приватних компаній України і країн НАТО були виявлені шкідливі програми, які займалися кібершпіонажем. Серед них такі, як Turla/Uroburos/Snake, RedOctober, MiniDuke і NetTraveler;

3) 23 грудня 2015 року за допомогою троянської програми BlackEnergy3, у використанні якої були раніше помічені російські хакери, було відключено близько 30 підстанцій Прикарпаттяобленерго, в зв'язку з чим більше ніж 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго;

4) 6 грудня 2016 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, що вивела з ладу ряд комп'ютерів, а також знищила критично важливі бази даних, що призвело до затримки бюджетних виплат на сотні мільйонів гривень;

5) 15 грудня 2016 року українські хакери на замовлення невстановленої особи із Санкт-Петербурга здійснили DDOS-атаку на сайт Укрзалізниці, внаслідок чого протягом дня була повністю заблокована його робота. Атака була націлена на крадіжку даних про пассажироперевезення;

6) 17 грудня 2016 року кібератака на підстанцію "Північна" компанії "Укренерго" призвела до збою в автоматиці управління, через що більше години знеструмленими залишалися райони у північній частині правобережного Києва і прилеглі райони області;

7) у першій половині дня 27 червня 2017 року розпочалася масова кібератака на український державний та комерційний сектор із застосування шкідливого програмного забезпечення – вірусу-шифрувальника файлів Petya Ransomware. Її жертвами стали інформаційно-телекомунікаційні системи "Укрпошти", аеропорту "Бориспіль", "Укренерго", ДТЕК, багатьох банків, ЗМІ, телеканалів, АЗС та інших компаній.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Водночас Закон України "Про основні засади забезпечення кібербезпеки України" визначає, що до Переліку об'єктів критичної інфраструктури (далі – Перелік) можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами потенційно небезпечних технологій і виробництв.

На сьогодні результатом кібератак є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування об'єктів критичної інфраструктури, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку з цим з урахуванням потреб національної безпеки і необхідності системного підходу до розв'язання проблеми на загальнодержавному рівні отримання відомостей щодо реального стану інформаційної безпеки на об'єктах

критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Необхідність прийняття постанови зумовлена відсутністю відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури та, як наслідок, унеможливлює системний підхід до розв'язання проблеми захисту критичної інфраструктури на загальнодержавному рівні.

Проблеми забезпечення належного рівня інформаційної безпеки на об'єктах критичної інфраструктури не можуть бути розв'язані без існування систематизованого підходу до аналізу стану захисту інформації, який базувався би на реальних показниках, отриманих під час проведення незалежного аудиту інформаційної безпеки.

Метою проекту постанови є визначення основних вимог та механізму впровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Основні групи (підгрупи), на які проблема впливає:

Групи (підгрупи)	Так	Ні
Громадяни		+
Держава	+	
Суб'єкти господарювання,	+	
У тому числі суб'єкти малого підприємництва		+

Проблема не може бути розв'язана за допомогою ринкових механізмів, оскільки на сьогодні відсутні вимоги щодо передачі інформації стосовно стану інформаційної безпеки об'єктами критичної інфраструктури державі.

Проблема не може бути розв'язана за допомогою діючих регуляторних актів, оскільки на сьогодні таких нормативно-правових актів немає.

2. Цілі державного регулювання

Основною ціллю проекту постанови є створення правових засад отримання об'єктивної інформації щодо стану інформаційної безпеки об'єктів критичної інфраструктури шляхом проведення незалежного аудиту інформаційної безпеки.

Проведення періодичного незалежного аудиту інформаційної безпеки стане обов'язковим до виконання підприємствами, установами та організаціями, які згідно до законодавства віднесені до об'єктів критичної інфраструктури.

3. Визначення та оцінка альтернативних способів досягнення цілей

3.1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Збереження чинного законодавства, що призведе до відсутності об'єктивної інформації щодо стану інформаційної безпеки на об'єктах критичної інфраструктури та до відсутності (неадекватності) вимог з кіберзахисту, що поставить під загрозу населення, стале функціонування цих об'єктів та існування держави як інституту в цілому. Такий спосіб є неприйнятним та не відповідає вимогам Закону. Це не забезпечить досягнення поставленої цілі регулювання.

Альтернатива 2	Прийняття проекту постанови Кабінету Міністрів України

3.2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	**Відсутні** (такий підхід призведе до відсутності об'єктивної інформації щодо стану інформаційної безпеки на об'єктах критичної інфраструктури держави та, як наслідок, унеможливлює системний підхід до розв'язання проблеми захисту критичної інфраструктури на загальнодержавному рівні)	Додаткових витрат не потребує
Альтернатива 2	**Висока** (надасть можливість отримувати актуальну інформацію щодо стану інформаційної безпеки на об'єктах критичної інфраструктури держави шляхом проведення заходів аудиту інформаційної безпеки, дотримуватися принципів плановості й системності аудиту інформаційної безпеки та гарантувати державні інтереси в зазначених галузях; у межах повноважень виявляти та запобігати виникненню порушень вимог законодавства у зазначеній сфері об'єктами критичної інфраструктури та забезпечувати інтереси суспільства, зокрема належної якості кіберзахисту та кібероборони)	Оцінити витрати з державного бюджету на реалізацію регуляторного акта буде можливо після визначення об'єктів критичної інфраструктури.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	Відповідно до Зеленої книги з питань захисту критичної інфраструктури в Україні, підготовленої Національним інститутом стратегічних досліджень із залученням українських та зарубіжних експертів, і за підтримки Офісу зв'язку НАТО в Україні на сьогодні в Україні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних		Дія регуляторного акта не буде розповсюджуватися на малі та мікросуб'єкти господарювання		0 %
Питома вага групи у загальній кількості, відсотків	Питома вага великих та середніх суб'єктів господарювання у загальній кількості може бути визначена тільки після віднесення об'єктів до об'єктів критичної інфраструктури, 100		0		100 %

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає (процедура проведення планових заходів аудиту ІБ не зможе застосуватися у зв'язку з невідповідністю вимог її проведення чинному законодавству, призведе до відсутності (висування неадекватних) вимог із кіберзахисту, що може призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави у випадку здійснення терористичних актів по відношенню до таких об'єктів)	Додаткових витрат не потребує

Альтернатива 2	Високі (узгодження інтересів бізнесу та держави, чіткий порядок та плановість проведення заходів аудиту ІБ Адміністрації Держспецзв'язку)	Оцінити витрати на реалізацію регуляторного акта неможливо через відсутність переліку об'єктів критичної інфраструктури держави. Орієнтовна вартість — 168 000 тис. грн. *

* вартість є орієнтовною. Оцінити витрати на реалізацію регуляторного акта буде можна після визначення об'єктів критичної інфраструктури. Відповідно до Зеленої книги з питань захисту критичної інфраструктури в Україні, підготовленої Національним інститутом стратегічних досліджень із залученням українських та зарубіжних експертів, і за підтримки Офісу зв'язку НАТО в Україні на сьогодні в Україні існує понад 24 тис. об'єктів, віднесених до категорії потенційно небезпечних. Через відсутність даних щодо вартості послуг незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури України за мінімальну вартість проведення незалежного аудиту інформаційної безпеки взята мінімальна вартість проведення фінансового аудиту в Україні — 7000 грн.

3.3. Сумарні витрати за альтернативами

Вид альтернативи	Сума витрат, гривень
Альтернатива 1	Додаткових витрат не потребує
Альтернатива 2	Оцінити витрати з державного бюджету на реалізацію регуляторного акта буде можна після визначення об'єктів критичної інфраструктури. Орієнтовні сумарні витрати становлять 168 500 тис. грн.

4. Вибір найбільш оптимального альтернативного способу досягнення цілей

Враховуючи вищенаведені позитивні та негативні сторони альтернативних способів досягнення мети, доцільно прийняти розроблений проект постанови. Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1	1	Цілі прийняття регуляторного акта не можуть бути досягнуті (проблема продовжує існувати)
Альтернатива 2	4	Зазначений спосіб повністю відповідає вимогам сучасності, є найбільш доцільним та дасть змогу врегулювати проведення заходів аудиту інформаційної безпеки на об'єктах критичної інфраструктури держави

Вид альтернативи	Вигоди (підсумок)	Витрати (Підсумок)	Обґрунтування альтернативи
Альтернатива 1	Немає	Додаткових витрат не потребує	Проблема продовжує існувати
Альтернатива 2	Надасть можливість отримувати актуальну інформацію щодо стану інформаційної безпеки на об'єктах критичної інфраструктури держави шляхом вжиття заходів аудиту інформаційної	Оцінити витрати з державного бюджету та витрати суб'єктів господарювання на реалізацію регуляторного акта буде можна після визначення переліку об'єктів критичної	Проблема більше існувати не буде

	безпеки, дотримуватися принципів плановості й системності аудиту інформаційної безпеки та гарантувати державні інтереси в зазначених галузях; у межах повноважень виявляти та запобігати виникненню порушень вимог законодавства у зазначеній сфері об'єктами критичної інфраструктури та забезпечувати інтереси суспільства, зокрема належної якості кіберзахисту та кібероборони	інфраструктури. Орієнтовна сума 168 500 тис. грн.	

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

Механізмом, який забезпечить розв'язання визначеної проблеми, є прийняття регуляторного акта.

Адміністрацією Держспецзв'язку підготовлено проект постанови, яким пропонується 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, що визначає:

обов'язковість проведення періодичного незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

вимоги до організаційних заходів та порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

відповідальність відповідних сторін при проведенні незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Для досягнення цієї цілі проектом постанови передбачається:

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

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

Заходи, що пропонуються для розв'язання проблеми:

погодити проект постанови з Міністерством фінансів України, Міністерством економічного розвитку і торгівлі України, Міністерством внутрішніх справ України, Міністерством оборони України, Службою безпеки України, Державним агентством з питань електронного урядування України, Міністерством енергетики та вугільної промисловості України, Міністерством інфраструктури України, Міністерством освіти і науки України, Національним банком України, Генеральним штабом Збройних сил України та Службою зовнішньої розвідки України;

надіслати проект постанови на правову експертизу до Міністерства юстиції України;

забезпечити інформування громадськості про вимоги регуляторного акта шляхом його оприлюднення на офіційному веб-сайті Держспецзв'язку.

Реалізація положень проекту постанови:

Дозволить отримувати актуальну інформацію щодо стану інформаційної безпеки на об'єктах критичної інфраструктури, визначити об'єкти критичної інформаційної інфраструктури, які мають першочергово (пріоритетно) захищатися від кібератак відповідно до законодавства у сфері захисту інформації та кібербезпеки.

Дії суб'єктів господарювання – ознайомитися з регуляторним актом та дотримуватися його вимог.

6. 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

Оцінити витрати з державного бюджету на реалізацію регуляторного акта буде можна після визначення об'єктів критичної інфраструктури.

Питома вага суб'єктів малого підприємництва (малих та мікропідприємств разом) у загальній кількості суб'єктів господарювання, на яких поширюється регулювання, становить 0 відсотків, тому розрахунок витрат на запровадження державного регулювання для суб'єктів малого підприємництва (Тест малого підприємництва) не проводився.

7. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується.

Строк набрання чинності регуляторним актом настає з дня затвердження переліку об'єктів критичної інфраструктури.

8. Визначення показників результативності дії регуляторного акта

Прогнозні значення показників результативності регуляторного акта будуть встановлюватися після набрання ним чинності.

Прогнозними значеннями показників результативності регуляторного акта є:

розмір надходжень до державного та місцевого бюджетів і державних цільових фондів, пов'язаних з дією акта – надходжень не передбачається;

розмір коштів і час, що витрачатимуться суб'єктами господарювання та/або фізичними особами, пов'язаними з виконанням вимог акта, оцінити неможливо до затвердження переліку об'єктів критичної інфраструктури. Додаткові витрати від суб'єктів господарювання, пов'язані з виконанням вимог акта, – орієнтовно 168 000 тис. грн;

рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта – проект акта розміщено на веб-сайті Держспецзв'язку (електронна адреса: www.dsszzi.gov.ua) у підрозділі «Повідомлення про оприлюднення та проекти» розділу «Регуляторна діяльність»;

кількість порушень, виявлених підчас проведення аудиту інформаційної безпеки на об'єктах критичної інфраструктури;

кількість наданих рекомендацій щодо підвищення рівня захищеності;

оцінка рівня кіберзахисту (кіберзагрози) за результатами проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

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

Адміністрація Держспецзв'язку буде здійснювати базове, повторне та періодичні відстеження результативності регуляторного акта у строки, встановлені статтею 10 Закону України "Про засади державної регуляторної політики у сфері господарської діяльності".

Проведення відстеження результативності регуляторного акта буде здійснюватися шляхом збирання статистичних даних відповідно до вищезазначених показників та аналізу звернень заінтересованих осіб щодо необхідності перегляду нормативно-правового акта з метою внесення до нього змін.

Базове відстеження результативності регуляторного акта буде здійснюватися через один рік після набрання чинності цим регуляторним актом шляхом збирання статистичних даних, одержання пропозицій до нього, їх аналізу.

Повторне відстеження результативності регуляторного акта буде здійснюватись не пізніше двох років з дня набрання чинності цим актом шляхом аналізу статистичних даних.

Періодичні відстеження результативності регуляторного акта будуть здійснюватись шляхом аналізу статистичних даних раз на кожні три роки, починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Голова Державної служби спеціального
зв'язку та захисту інформації України Леонід Євдоченко
«___» _____ 2018 року

20 липня 2018

Повідомлення про оприлюднення

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»

1. Стислий виклад змісту проекту акта

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" розроблено на виконання частини третьої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" щодо впровадження системи незалежного аудиту інформаційної безпеки та абзацу четвертого пункту 1 Плану організації підготовки проектів актів, необхідних для забезпечення реалізації Закону України "Про основні засади забезпечення кібербезпеки України", схваленого на засіданні Кабінету Міністрів України 22 листопада 2017 року (протокол № 66).

Документ визначає основні вимоги та механізм впровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

2. Адреси для зауважень та пропозицій до проекту акта

Пропозиції та зауваження до проекту постанови просимо надсилати протягом місяця з дати його оприлюднення на адреси:

- Адміністрації Державної служби спеціального зв'язку та захисту інформації України:

поштова: вул. Солом'янська, 13, м. Київ, 03110; тел. (044) 281-88-51;

електронна: ddkc@dsszzi.gov.ua;

- Державної регуляторної служби України:

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

факс (044) 254-43-93;

електронна: inform@dkrp.gov.ua

3. Обраний спосіб оприлюднення проекту акта

Проект акта та аналіз його регуляторного впливу розміщено на веб-сайті Держспецзв'язку (електронна адреса: www.dsszzi.gov.ua) у підрозділі «Повідомлення про оприлюднення та проекти» розділу «Регуляторна діяльність».

4. Строк, протягом якого приймаються зауваження та пропозиції

Зауваження та пропозиції до проекту акта приймаються протягом місяця з дати його оприлюднення.

Голова Державної служби спеціального
зв'язку та захисту інформації України Леонід Євдоченко

«___» _____ 2018 р.