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

29.05.2019 № 04/02/03-1945

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

Щодо погодження проекту постанови Кабінету Міністрів України

Адміністрація Державної служби спеціального зв'язку та захисту інформації України відповідно до Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 18.07.2007 № 950, надсилає на повторне погодження проект постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації» (далі – проект постанови), розроблений відповідно до вимог статей 5 та 10 Закону України «Про технічні регламенти та оцінку відповідності», з урахуванням зауважень та пропозицій заінтересованих суб'єктів до його попередньої редакції.

Попередня редакція проекту постанови була погоджена рішенням ДРС від 24.05.2018 № 234.

Додатки: 1. Проект постанови на 31 арк.;
2. Пояснювальна записка до проекту постанови на 7 арк.
3. Порівняльна таблиця на 2 арк.
4. Аналіз регуляторного впливу на 12 арк.
5. Повідомлення про оприлюднення на 1 арк.
6. Висновок про проведення гендерно-правової експертизи на 2 арк.
7. Висновок про проведення антидискримінаційної експертизи, вх. № 2814 від 16.05.2019, прим. № __ на 1 арк.

Заступник Голови Служби П.І. Опаленик

Вик. Гавриков А.В.
тел. 281-96-99

0.31

ПРОЕКТ

КАБІНЕТ МІНІСТРІВ УКРАЇНИ
ПОСТАНОВА

від 20__ р. №

Київ

Про затвердження Технічного регламенту засобів криптографічного захисту інформації

Відповідно до статті 5 Закону України «Про технічні регламенти та оцінку відповідності» Кабінет Міністрів України **постановляє**:

1. Затвердити Технічний регламент засобів криптографічного захисту інформації, що додається.

2. Адміністрації Державної служби спеціального зв'язку та захисту інформації забезпечити впровадження Технічного регламенту, затвердженого цією постановою.

3. Установити, що:

з дня набрання чинності цієї постанови до 01 січня 2025 року оцінка відповідності засобів криптографічного захисту інформації Технічному регламенту, затвердженому цією постановою, здійснюється в рамках державної експертизи у сфері криптографічного захисту інформації або процедур оцінки відповідності, визначених Технічним регламентом, затвердженим цією постановою;

позитивні експертні висновки, виданні до дня набрання чинності цієї постанови за результатами державної експертизи у сфері криптографічного захисту інформації на засоби криптографічного захисту державних

інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, є чинними до завершення терміну їх дії.

4. Внести до постанов Кабінету Міністрів України зміни, що додаються.

5. Ця постанова набирає чинності через рік з дня її опублікування.

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

Л.О. Євдоченко

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 20__ р. № _____

ЗМІНИ,
що вносяться до постанов Кабінету Міністрів України

1. В абзаці першому пункту 22 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 лютого 2006 року № 373 (Офіційний вісник України, 2006 р., № 13, ст. 878, № 50, ст. 3324), слова «та сертифікації» виключити.

2. Перелік видів продукції, щодо яких органи державного ринкового нагляду здійснюють державний ринковий нагляд, затверджений постановою Кабінету Міністрів України від 28 грудня 2016 р. № 1069 (Офіційний вісник України, 2017, № 50, ст. 1550), доповнити пунктом 52 такого змісту:

52. Засоби криптографічного захисту інформації	постанова Кабінету Міністрів України від ___ _____ 20__ р. № _____ «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»	Адміністрація Держспецзв'язку

3. Пункт 4 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 р. № 411 (Офіційний вісник України, 2014 р., № 73, ст. 2066), доповнити підпунктом 7-1 такого змісту:

"7-1) здійснює державний ринковий нагляд у межах сфери своєї відповідальності;".

Л.О. Євдоченко

ПРОЕКТ

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів
України
від _____ № _____

ТЕХНІЧНИЙ РЕГЛАМЕНТ
засобів криптографічного захисту інформації

Загальна частина

1. Цей Технічний регламент установлює вимоги до розроблення, виготовлення, оцінки відповідності, експлуатації, відкликання, надання та вилучення з ринку, ринкового нагляду засобів криптографічного захисту інформації (продукція, криптографічний модуль), призначених для захисту відкритої та/або конфіденційної інформації.

Вимоги до засобів криптографічного захисту інформації, призначених для захисту службової інформації, таємної інформації або для організації спеціального зв'язку визначаються окремими нормативно-правовими актами.

2. Суб'єктами відносин у сфері криптографічного захисту інформації є:

розробник;

виробник;

розповсюджувач;

імпортер;

користувач;

орган з оцінки відповідності;

постачальник ключових документів;

Адміністрація Держспецзв'язку.

3. У цьому Технічному регламенті застосовуються такі скорочення та позначення:

апаратне забезпечення – АЗ;

вбудоване програмне забезпечення – ВПЗ;

криптографічний захист інформації – КЗІ;

критичні параметри безпеки – КПБ;

програмне забезпечення – ПЗ;

чутливі параметри безпеки – ЧПБ.

4. У цьому Технічному регламенті терміни вживаються в такому значенні:

введення в експлуатацію – будь-який захід, спрямований на початок використання користувачем засобів КЗІ;

введення в обіг – надання засобів КЗІ на ринку України в перший раз;

виведення з експлуатації – будь-який захід, спрямований на припинення використання користувачем засобів КЗІ;

використання засобу КЗІ – експлуатація засобу КЗІ відповідно до експлуатаційної документації на цей засіб;

вилучення з ринку засобів КЗІ – будь-який захід, спрямований на запобігання наданню на ринку засобів КЗІ;

випробування – визначення однієї чи кількох характеристик засобу КЗІ згідно з встановленою процедурою;

виробник – будь-яка фізична чи юридична особа (резидент чи нерезидент України), яка виготовляє засоби КЗІ або доручає їх виготовлення та реалізує під своїм найменуванням або торговельною маркою;

відкликання засобів КЗІ – будь-який захід, спрямований на забезпечення повернення користувачем засобу КЗІ розповсюджувачу;

захист від відмов, що можуть бути спричинені впливом навколишнього середовища – використання функцій захисту від компрометації безпеки засобу КЗІ від впливу навколишнього середовища (температура, зовнішні випромінювання, інші параметри) за умови його правильної експлуатації;

засіб КЗІ (криптографічний модуль) – набір АЗ та/або ПЗ та/або ВПЗ, що реалізують функцію (функції) безпеки та містяться в криптографічній межі;

інспектування – перевірка засобів КЗІ та процесів, пов'язаних з виготовленням засобів КЗІ, вимогам цього Технічного регламенту;

імпортер – будь-яка фізична чи юридична особа – резидент України, яка вводить в обіг на ринку України засоби КЗІ походженням з іншої країни;

код виявлення помилок – значення, обчислене з даних, що складається з надлишкових бітів інформації, призначених для виявлення непередбачених змін в даних;

криптографічна межа – чітко визначений периметр, який встановлює межу розташування всіх компонентів засобу КЗІ;

користувач – будь-яка фізична чи юридична особа, яка використовує засіб КЗІ;

критичний параметр безпеки – інформація, пов'язана з безпекою, розкриття або модифікація якої може спричинити загрозу безпеці засобу КЗІ;

модель кінцевих станів – математична модель послідовного механізму, яка складається з кінцевого набору вхідних подій (входів), кінцевого набору вихідних подій (виходів), кінцевого набору станів, функції, яка відображає зв'язок стану і входу з виходом, функції, яка відображає зв'язок стану та входу з станом (функція переходу станів), специфікації, яка описує початковий стан;

надання засобів КЗІ на ринку – будь-яке платне або безоплатне постачання засобів КЗІ для використання на ринку України;

орган з оцінки відповідності – підприємство, установа, організація чи їх структурний підрозділ, що здійснює оцінку відповідності засобів КЗІ, включаючи випробування, сертифікацію та інспектування;

оцінка відповідності засобів КЗІ – підтвердження органом з оцінки відповідності характеристик засобу КЗІ, за результатами чого видається документ про відповідність;

політика безпеки засобу КЗІ – точна специфікація правил безпеки, за якими працює засіб КЗІ, яка відповідає вимогам цього Технічного регламенту;

постачальник ключових документів – підприємство, установа, організація чи їх структурний підрозділ, що здійснює постачання ключових документів до засобів КЗІ;

постачання засобів КЗІ – будь-які операції, що передбачають надання права користувачу на законних підставах використовувати засоби КЗІ;

програмний інтерфейс – набір команд, які використовуються для запиту послуг засобу КЗІ, включаючи параметри, що входять або виходять за криптографічну межу;

публічні параметри безпеки – публічна інформація, пов'язана з безпекою, модифікація якої може скомпрометувати безпеку криптографічного модуля;

розробник – будь-яка фізична чи юридична особа, яка розробляє засіб КЗІ;

розроблення засобу КЗІ – розроблення технічної документації і технології виготовлення дослідних зразків засобів КЗІ;

розповсюджувач – виробник або імпортер або уповноважений представник, які надають засоби КЗІ на ринку України;

розповсюдження засобу КЗІ – надання засобів КЗІ на ринку України після введення їх в обіг;

тестування на відмови, що можуть бути спричинені впливом навколишнього середовища – використання конкретних методів для забезпечення обґрунтованої гарантії того, що безпека засобу КЗІ не буде

скомпрометована під впливом навколишнього середовища (температура, зовнішні випромінювання, інші параметри) за умови його правильної експлуатації;

уповноважений представник – будь-яка фізична чи юридична особа - резидент України, яка одержала від виробника або імпортера письмове доручення діяти від його імені стосовно визначених у цьому дорученні завдань;

функція безпеки – криптографічні алгоритми або методи захисту або механізми генерації та встановлення ЧПБ або механізми автентифікації або профілі захисту або показники для проведення тестування засобів КЗІ для пом'якшення наслідків неінвазивних атак, що визначені або погоджені Адміністрацією Держспецзв'язку для реалізації в засобах КЗІ відповідно до законодавства;

характеристика засобу КЗІ – тип засобу КЗІ, категорія засобу КЗІ, порядок доступу до інформації для захисту якої призначений засіб КЗІ, рівень безпеки засобу КЗІ та інша інформація, що дозволяє визначити об'єкт застосування засобу КЗІ;

чутливі параметри безпеки – критичні параметри безпеки та публічні параметри безпеки.

Інші терміни вживаються у значенні, наведеному в Законах України «Про технічні регламенти та оцінку відповідності», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні довірчі послуги», «Про державний ринковий нагляд і контроль нехарчової продукції», «Про загальну безпечність нехарчової продукції», «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання», чинних національних стандартах України ДСТУ ISO/IEC 19790 «Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів» (далі – ДСТУ ISO/IEC 19790), ДСТУ ISO/IEC 24759 «Інформаційні технології. Методи захисту. Вимоги до випробувань криптографічних модулів» (далі – ДСТУ ISO/IEC 24759).

5. Залежно від способу реалізації розрізняють такі типи продукції:

апаратний засіб КЗІ – засіб КЗІ, криптографічну межу якого задано периметром АЗ, та до складу якого може входити ПЗ;

програмний засіб КЗІ – засіб КЗІ, криптографічна межа якого обмежується компонентом (компонентами) ПЗ, які забезпечують виконання криптографічних перетворень у змінному операційному середовищі, що є зовнішнім по відношенню до його криптографічної межі;

вбудований програмний засіб КЗІ – засіб КЗІ, криптографічна межа якого обмежується компонентом (компонентами) ВПЗ, які забезпечують виконання криптографічних перетворень у обмеженому, незмінному, визначеному операційному середовищі;

гібридний програмний засіб КЗІ – засіб КЗІ, криптографічна межа якого обмежується компонентом (компонентами) ПЗ та частини АЗ;

гібридний вбудований програмний засіб КЗІ – засіб КЗІ, криптографічна межа якого обмежується компонентом (компонентами) вбудованого програмного забезпечення та частини апаратного забезпечення.

6. Залежно від призначення встановлюються такі категорії засобів КЗІ:

засоби КЗІ, призначені для шифрування інформації (далі – засіб КЗІ категорії «Ш»);

засоби КЗІ, призначені для виготовлення ключових даних або ключових документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ (далі – засіб КЗІ категорії «К»);

засоби КЗІ, призначені для надання електронних довірчих послуг та виконання функцій засобу кваліфікованого електронного підпису чи печатки (далі – засіб КЗІ категорії «Е»);

засоби КЗІ, призначена для забезпечення захисту (підтвердження) цілісності або неспростовності інформації, окрім продукції категорії «Е» (далі – засіб КЗІ категорії «П»);

засоби КЗІ, призначена для захисту інформації від несанкціонованого доступу, у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки (далі – засіб КЗІ категорії «Р»);

засоби КЗІ, спеціально призначені для розроблення, дослідження, виробництва та випробувань засобів КЗІ та криптографічних модулів (далі – засіб КЗІ категорії «З»).

7. Залежно від необхідного рівня забезпечення захисту інформації в інформаційно-телекомунікаційних системах, або відповідно до цінності інформації, що захищається з використанням засобів КЗІ, користувачем обирається засіб КЗІ відповідного рівня безпеки.

Рівень безпеки засобу КЗІ визначається у сукупності за 11 компонентами безпеки:

1) специфікація засобу КЗІ;

2) інтерфейси засобу КЗІ;

3) ролі, служби та автентифікація;

4) захист ПЗ/ВПЗ;

5) експлуатаційне середовище;

6) фізична безпека;

7) неінвазивна безпека;

8) управління ЧПБ;

9) самотестування;

10) гарантії життєвого циклу;

11) пом'якшення атак.

Цим Технічним регламентом визначаються чотири рівні безпеки засобів КЗІ відповідно до заходів безпеки, що визначаються Суттєвими вимогами, наведеними у додатку 1:

рівень безпеки 1 – базовий рівень безпеки, обов'язковий для всіх засобів КЗІ, що включає основні заходи безпеки, визначені у Суттєвих вимогах, за всіма компонентами безпеки;

рівень безпеки 2 – рівень з додатковими до рівня безпеки 1 заходами безпеки, визначеними у Суттєвих вимогах, що відносяться до компонентів безпеки 3, 4, 6 та 10 (в частині опису, доставки та експлуатації);

рівень безпеки 3 – рівень з додатковими до рівня безпеки 2 заходами безпеки, визначеними у Суттєвих вимогах, що відносяться до компонентів безпеки 2 - 4, 6 - 8 та 10 (в частині управління конфігурацією та тестування);

рівень безпеки 4 – найвищий рівень безпеки, з додатковими до рівня безпеки 3 заходами безпеки, визначеними у Суттєвих вимогах, що відносяться до компонентів безпеки 3, 6, 10 (в частині опису, доставки та експлуатації) та 11.

8. Діяльність суб'єктів відносин у сфері КЗІ підлягає ліцензуванню відповідно до законодавства у сфері ліцензування.

9. Суб'єкти відносин у сфері КЗІ визначають режим доступу до інформації про ці засоби, установлюють і підтримують відповідний режим безпеки такої інформації відповідно до законодавства.

Розроблення засобів КЗІ

10. Розроблення засобів КЗІ, що фінансується за рахунок коштів Державного бюджету України, здійснюється шляхом виконання відповідних науково-дослідних та дослідно-конструкторських робіт зі створення нових або модернізації існуючих зразків засобів КЗІ, відповідно до законодавства. Рішення про розроблення та технічні вимоги до таких засобів КЗІ погоджується з Адміністрацією Держспецзв'язку, крім засобів КЗІ, що створюється

Національним банком України для власних потреб та потреб банківської системи України.

11. Розроблення засобів КЗІ здійснюється з використанням тільки ліцензійного програмного забезпечення або за погодженням із замовником робіт комп'ютерних програм вільного використання, які повинні бути забезпечені документацією, що підтверджує правомірність їх використання згідно з ліцензією або належність до комп'ютерних програм вільного використання.

12. В засобах КЗІ реалізуються функції безпеки які визначаються або погоджуються Адміністрацією Держспецзв'язку.

Надання на ринку та експлуатація засобів КЗІ

13. Засоби КЗІ можуть бути надані на ринку та введені в експлуатацію тільки в разі, коли вони відповідають вимогам цього Технічного регламенту, а також забезпечено їх належний монтаж, інсталювання, обслуговування та використання за призначенням.

14. Підставою для початку експлуатації засобів КЗІ користувачем, що є юридичною особою, є відповідний акт розпорядчого характеру користувача.

15. Засоби КЗІ, які стали не придатними до експлуатації, виводяться з експлуатації відповідно до вимог експлуатаційної документації на засоби КЗІ.

Обов'язкові вимоги та презумпція відповідності засобів КЗІ

16. Засоби КЗІ повинні відповідати Суттєвим вимогам у обсязі встановленому для відповідного рівня безпеки. Політика безпеки засобу КЗІ повинна відповідати вимогам додатку В ДСТУ ISO/IEC 19790 або бути затвердженою органом з оцінки відповідності.

17. Презумпцією відповідності засобів КЗІ Суттєвим вимогам є реалізація норм національного стандарту ДСТУ ISO/IEC 19790 та оцінка відповідності засобів КЗІ відповідно до вимог національного стандарту ДСТУ ISO/IEC 24759 у спосіб визначений цим Технічним регламентом.

18. Уся документація на засоби КЗІ, що надаються на ринку або виготовляються в межах України, повинна бути викладена українською мовою. Додатково допускається застосування інших мов. В інших випадках можуть використовуватися іноземні мови.

Обмеження в наданні на ринку засобів КЗІ

19. Засоби КЗІ, що відносяться до товарів військового призначення, список яких затверджується Кабінетом Міністрів України, при здійсненні міжнародних передач підлягають державному контролю у встановленому законодавством порядку.

20. Надання на ринку криптографічних модулів, призначених для надання та/або отримання послуг електронного урядування, допускається після підтвердження їх сумісності із сервісами електронного урядування, у встановленому Державним агентством з питань електронного урядування порядку.

21. Засоби КЗІ, що відповідають Суттєвим вимогам, та не стосуються призначення, згідно з пунктами 19, 20 цього Технічного регламенту, не можуть бути обмежені в наданні на ринку, якщо інше не встановлено законом.

Обов'язки користувачів

22. Користувачі використовують продукцію, що відповідає вимогам цього Технічного регламенту, за наявності законних прав на її використання.

23. Користувачі отримують ключові документи та їх використовують у порядку встановленому Адміністрацією Держспецзв'язку.

24. Користувачі зобов'язані повернути продукцію розповсюджувачу у випадках встановлених Законом України «Про державний ринковий нагляд і контроль нехарчової продукції» та цим Технічним регламентом.

25. Користувач зобов'язаний експлуатувати засіб КЗІ відповідно до вимог політики безпеки. Користувачу забороняється несанкціоновано (без дозволу виробника) копіювати та розповсюджувати політику безпеки.

26. Для користувачів, що забезпечують використання засобів КЗІ для забезпечення захисту інформації в інформаційно-телекомунікаційних системах

відповідно до вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», вибір засобів КЗІ прийнятного рівня безпеки покладається на службу захисту інформації (при створенні та забезпеченні функціонування комплексної системи захисту інформації), а в інших випадках відповідно до законодавства.

Обов'язки виробників

27. Виробники під час введення в обіг засобів КЗІ повинні забезпечувати їх відповідність Суттєвим вимогам та дотримуватися процедур визначених у пунктах 19, 20 цього Технічного регламенту для окремих категорій засобів КЗІ.

28. Виробники повинні зберігати пов'язану з продукцією документацію доки не мине потреба але не менше ніж 10 років після введення в обіг останньої одиниці.

29. Виробники забезпечують дотримання процедур, необхідних для підтримання відповідності серійного виготовлення засобів КЗІ вимогам цього Технічного регламенту.

30. Виробники приймають та ведуть облік звернень користувачів щодо якості засобів КЗІ, досліджують продукцію щодо перевірки наданої користувачами інформації, надають відповіді користувачам.

31. Виробники у разі виявлення невідповідності засобів КЗІ встановленим вимогам здійснюють заходи щодо їх усунення, а у разі наявності при цьому ризиків у порушенні захисту інформації, що може завдати значних збитків користувачу, вживають заходів щодо відкликання засобів КЗІ. Про це виробники негайно повідомляють Адміністрацію Держспецзв'язку та подають детальну інформацію, що підтверджує це.

32. Виробники забезпечують, щоб на засоби КЗІ, які вони ввели в обіг, було нанесено візуально сприйнятну інформацію, яка дозволяє здійснити ідентифікацію засобів КЗІ, а в разі коли за об'єктивних обставин не має змоги

цього зробити, така інформація повинна бути зазначена на пакуванні засобів КЗІ або супроводжувальних до них документах.

33. Виробники зазначають на засобах КЗІ або супроводжувальних до них документах своє повне найменування, зареєстроване комерційне найменування чи зареєстровану торговельну марку (за наявності) та контактні дані, за якими можна зв'язатися з ними.

34. Виробники на обґрунтований запит Адміністрації Держспецзв'язку надають всю необхідну інформацію та документацію (в паперовій або електронній формі), необхідну для перевірки відповідності засобів КЗІ вимогам цього Технічного регламенту та співпрацюють з будь-яких питань спрямованих на усунення ризиків, що становить введена ними в обіг продукція.

35. Виробники забезпечують захист прав користувачів відповідно до вимог Закону України «Про захист прав споживачів».

Обов'язки уповноважених представників

36. Виробник на підставі письмового доручення може визначити уповноваженого представника. Обов'язки виробника, передбачені пунктами 28, 29, 31 цього Технічного регламенту не повинні включатися до предмету доручення.

Обов'язки імпортерів та розповсюджувачів

37. Розповсюджувачі вводять в обіг лише ті засоби КЗІ, які відповідають вимогам цього Технічного регламенту.

38. Якщо розповсюджувач вважає або має підстави вважати, що засоби КЗІ не відповідають Суттєвим вимогам він повідомляє про це виробника та Адміністрацію Держспецзв'язку.

39. До початку введення засобів КЗІ в обіг розповсюджувачі пересвідчуються в тому, що виробник виконав вимоги пунктів 27, 29 цього Технічного регламенту.

40. Імпортер також виконує вимоги пунктів 34, 35 цього Технічного регламенту, що застосовуються до виробників.

Процедури оцінки відповідності

41. Оцінка відповідності засобів КЗІ вимогам цього Технічного регламенту, здійснюється шляхом застосовування таких модулів оцінки відповідності:

для засобів КЗІ призначених для захисту конфіденційної інформації або відкритої інформації, що відноситься до державних інформаційних ресурсів застосовується модуль B (експертиза типу), встановлений в додатку 2, у поєднанні з модулем D (відповідність типу на основі забезпечення якості виробничого процесу), встановлений в додатку 3;

для засобів КЗІ, призначених для захисту відкритої інформації застосовується декларація про відповідність, встановлена в додатку 4.

Процедура оцінки відповідності у сфері КЗІ здійснюється на добровільних засадах та за рахунок замовника процедури оцінки відповідності. Вартість робіт з проведення процедури оцінки відповідності у сфері КЗІ визначається на договірних засадах.

42. Для проходження процедури оцінки відповідності у сфері КЗІ замовник процедури оцінки відповідності самостійно обирає орган з оцінки відповідності та укладає з ним відповідний договір.

43. Орган з оцінки відповідності при здійсненні процедур оцінки відповідності дотримується вимог Закону України «Про технічні регламенти та оцінку відповідності» та цього Технічного регламенту.

44. Строк прийняття рішення органом з оцінки відповідності про видачу документа про відповідність або відмову у видачі такого за результатами процедури оцінки відповідності у сфері КЗІ, не може бути більшим, ніж 6 місяців з дати надання органу з оцінки відповідності необхідних документів.

45. За результатами процедури оцінки відповідності у сфері КЗІ органом оцінки відповідності приймається одне з таких рішень:

1) продукція відповідає заявленому рівню безпеки;

2) продукція відповідає рівню безпеки, що нижче від заявленого;

3) продукція не відповідає жодному з рівнів безпеки.

46. У разі прийняття рішення про відповідність засобів КЗІ заявленому рівню безпеки, орган з оцінки відповідності видає замовнику процедури оцінки відповідності у сфері КЗІ документ про відповідність, невід'ємною частиною якого є звіт з результатами оцінки.

47. У разі, коли засіб КЗІ не відповідає заявленому рівню безпеки, він повертається на доопрацювання розробнику разом із звітом з результатами оцінки, в якому зазначено усі виявлені недоліки. У разі, коли продукція відповідає рівню безпеки, що нижче від заявленого, за згодою з розробником допускається видача документа про відповідність засобів КЗІ такому рівню.

48. У разі усунення недоліків до засобів КЗІ протягом 3 місяців, органом з оцінки відповідності за відповідним зверненням замовника може бути проведена додаткова процедура оцінки відповідності у сфері КЗІ у строк не більше 3 місяців.

49. Виробник, який складає декларацію про відповідність, бере на себе відповідальність за відповідність засобів КЗІ вимогам, установленим у цьому Технічному регламенті.

Загальні принципи маркування засобів КЗІ

50. Знак відповідності засобів КЗІ цьому Технічному регламенту наноситься на продукцію там де це можливо та має бути видимим, розбірливим і стійким до стирання. У інших випадках інформація про відповідність засобів КЗІ цьому Технічному регламенту вказується у супроводжувальній документації на продукцію.

51. Знак відповідності цьому Технічному регламенту наноситься до введення засобів КЗІ в обіг.

52. Ідентифікаційний номер наноситься органом з оцінки відповідності або за його вказівкою виробником або уповноваженим представником, а при складанні декларації виробником.

Призначення органів з оцінки відповідності, їх обов'язки

53. Призначення органів з оцінки відповідності здійснюється національним органом з акредитації за поданням Адміністрації Держспецзв'язку.

54. Призначені органи повинні відповідати вимогам Закону України «Про технічні регламенти та оцінку відповідності» та кваліфікаційним вимогам, встановленим Адміністрацією Держспецзв'язку.

55. Призначені органи здійснюють оцінку відповідності засобів КЗІ згідно з процедурами оцінки відповідності встановленими цим Технічним регламентом.

56. Оцінка відповідності повинна проводитися у пропорційний спосіб, без покладення зайвого навантаження на виробника. Призначені органи повинні провадити свою діяльність з належним урахуванням обсягів виробництва, ступеня складності технології виготовлення засобів КЗІ та характеру виробничого процесу.

57. У разі коли під час проведення моніторингу відповідності введених в обіг засобів КЗІ призначений орган виявить, що засоби КЗІ не відповідають вимогам він вимагає від виробника вжити заходів доопрацювання продукції або обмежує сферу дії, зупиняє дію або скасовує документ про відповідність, в залежності від наслідків, що можуть бути спричиненні.

58. Подання та розгляд апеляцій на рішення призначених органів здійснюються відповідно до Закону України «Про технічні регламенти та оцінку відповідності» у встановленому законодавством порядку.

59. Призначені органи інформують Адміністрацію Держспецзв'язку у встановленому нею порядку про:

відмову у видачі, обмеження сфери, зупинення або скасування документа про відповідність;

обставини, що впливають на сферу та умови призначення цих органів;

діяльність з оцінки відповідності, проведену в межах сфери їх призначення, та будь-яку іншу проведену діяльність, зокрема транскордонну діяльність, та роботи за договорами субпідряду.

Державний ринковий нагляд засобів КЗІ

60. Державний ринковий нагляд здійснюються відповідно до Закону України «Про державний ринковий нагляд і контроль нехарчової продукції» з урахуванням вимог цього Технічного регламенту.

61. У разі наявності достатніх підстав вважати, що засоби КЗІ становлять ризик для захисту інформації користувача Адміністрація Держспецзв'язку повинна провести перевірку відповідних характеристик засобів КЗІ або організувати проведення такої перевірки органом з оцінки відповідності. Якщо за результатами зазначеної перевірки встановлено, що продукція становить серйозний ризик, Адміністрація Держспецзв'язку невідкладно вживає заходів відповідно до законодавства щодо вилучення та/або відкликання цих засобів КЗІ.

62. Суб'єкти відносин у сфері КЗІ надають свої пояснення Адміністрації Держспецзв'язку відповідно до статті 33 Закону України «Про державний ринковий нагляд і контроль нехарчової продукції».

Л.О. Євдоченко

Додаток 1
до Технічного регламенту

СУТТЄВІ ВИМОГИ

Для відповідності засобу КЗІ певному рівню безпеки повинні бути виконанні організаційні, технічні та технологічні заходи у обсязі відповідного йому стовпця Таблиці № 1.

Заходи розділенні сполучником «або» є альтернативними.

Таблиця № 1.

№ з/п	Компонент	Рівень безпеки 1	Рівень безпеки 2	Рівень безпеки 3	Рівень безпеки 4
1.	Специфікація засобу КЗІ	Специфікація засобу КЗІ, криптографічна межа, функції безпеки (у необхідному обсязі), режими роботи засобу КЗІ. Опис засоби КЗІ, включаючи всі його складові. Усі сервіси засобу КЗІ надають інформацію про стан виконання функцій безпеки або визначених процесів.			
2.	Інтерфейси засобу КЗІ	Обов'язкові та необов'язкові інтерфейси. Специфікація всіх інтерфейсів та всіх входів і виходів даних		Довірений канал.	
3.	Ролі, служби та автентифікація	Логічне розділення обов'язкових та необов'язкових ролей та послуг.	Автентифікація оператора на основі ролі чи ідентичності.	Автентифікація оператора на основі ідентичності.	Багатофакторна автентифікація.

4.	Захист ПЗ/ВПЗ	Функція перевірки цілісності або код виявлення помилок. Програмний інтерфейс. Виконуваний код.	Функція перевірки цілісності на основі цифрового підпису або код автентифікації повідомлень	Функція перевірки цілісності на основі цифрового підпису або для засобів КЗІ категорій «К», «З» та «Р» код автентифікації повідомлень	
5.	Експлуатаційне середовище	Модифіковане, немодифіковане або обмежене. Контроль ЧПБ	Модифіковане. Контроль доступу на основі ролей або дій. Ведення аудиту подій.		
6.	Фізична безпека	Градація складових продукції	Докази втручання. Непрозоре покриття або корпус.	Фіксування фактів несанкціонованого втручання до корпусу криптографічного модуля (кришок, дверей тощо), та інформування про це. Сильний корпус або покриття. Захист від прямого зондування. Захист від відмов, що можуть бути спричинені впливом	Фіксування фактів будь-якого втручання до криптографічного модуля та інформування про це. Захист від відмов, що можуть бути спричинені впливом навколишнього середовища. Пом'якшення наслідків усунення несправностей.

				навколишнього середовища або тестування на відмови, що можуть бути спричинені впливом навколишнього середовища	
7.	Неінвазивна безпека	Модуль, призначений для пом'якшення наслідків від неінвазивних атак, згідно з вимогами додатку F ДСТУ ISO/IEC 19790			
		Ведення документації та застосування методів обмеження витоку інформації, згідно з вимогами додатку F ДСТУ ISO/IEC 19790		Тестування з метою пом'якшення наслідків.	
8.	Управління чутливими параметрами безпеки	Генератори випадкових бітів; генерація, створення, введення, виведення, зберігання та знищення ЧПБ			
		Транспортування або узгодження ЧПБ з використанням встановлених методів			
		ЧПБ, що встановлюються особою, можуть вводитися або виводитися у формі відкритого тексту		ЧПБ, що встановлюються особою, можуть вводитися або виводитися у зашифрованому вигляді з використанням надійного каналу або за допомогою процедур розділення знань	
9.	Самотестування	Перед початком експлуатації: перевіряється цілісність ПЗ/ВПЗ, правильність роботи обхідної функції та критичних функцій			
		Виконуються умови: реалізовані криптографічний алгоритм, подвійна логіка, завантаження ПЗ/ВПЗ, ручне введення даних, правильність роботи обхідної функції та критичних функцій			

10.	гарантії життєвого циклу	Управління конфігурацією	Система управління конфігурацією засобу КЗІ та його компонентів. Документація. Кожен засіб КЗІ та його компоненти повинні бути унікально ідентифікованими. Конфігурація засобу КЗІ та його компонентів повинна відслідковуватися протягом всього їх життєвого циклу	Автоматизована система управління конфігурацією	
		Дизайн	Модуль призначений для перевірки всіх наданих послуг, пов'язаних із безпекою		
		Модель кінцевих станів	Модель кінцевих станів		
		Опис	Анотовані вихідний код, схеми або мова опису апаратних засобів	Мова опису програмного забезпечення високого рівня. Мова опису обладнання високого рівня	Документація, що має анотації щодо доступу до компонентів засобу КЗІ, у тому числі тих, що заплановані до виконання
		Тестування	Функціональне тестування	Тестування на низькому рівні	
		Доставка та експлуатація	Ініціалізація процедур	Опис процедур доставки.	Автентифікація оператора здійснюється у спосіб визначений виробником
		Керівництво	Адміністративне та неадміністративне керівництво		
11.	Пом'якшення атак		Специфікація пом'якшення атак, для яких не існує вимог щодо тестування		Специфікація пом'якшення атак з вимогами до перевірки

Додаток 2
до Технічного регламенту

МОДУЛЬ В
Експертиза типу

1. Експертиза типу є частиною процедури оцінки відповідності, в якій призначений орган з оцінки відповідності (далі – призначений орган) досліджує технічний проект засобу КЗІ та перевіряє і засвідчує, що він відповідає вимогам Технічного регламенту засобів криптографічного захисту інформації (далі – Технічний регламент), які застосовуються до нього.

2. Експертиза типу виконується з проведенням обстеження зразка завершеного засобу КЗІ (експертиза типового зразка), що є репрезентативним для передбачуваного виробництва.

3. Виробник подає заявку на експертизу типу лише одному призначеному органу за своїм вибором, в якій зазначається найменування та адреса виробника, а в разі подання заявки уповноваженим представником - також його найменування і адреса та інформація про те, що така заявка не подана до жодного іншого призначеного органу, до якої додаються:

технічна документація, яка дає можливість оцінити відповідність продукції застосовним вимогам Технічного регламенту;

зразки засобів КЗІ, що є репрезентативними для передбаченого виробництва.

Призначений орган може затребувати додаткові зразки засобів КЗІ, якщо це необхідно для виконання програми випробувань.

4. Призначений орган:

проводить експертизу технічної документації і перевіряє її повноту та відповідність вимогам Технічного регламенту;

проводить відповідні дослідження і випробування або доручає їх проведення з метою перевірки того, що у разі обрання виробником для застосування рішення відповідних функцій безпеки вони були застосовані правильно;

погоджує з виробником місце проведення досліджень і випробувань.

Продовження додатка 2

5. Призначений орган складає звіт про оцінку, в якому наводяться дані про дії, виконані згідно з пунктом 4 цього додатка, та їх результати. Призначений орган може оприлюднити (повністю або частково) зміст зазначеного звіту лише за згодою виробника, за винятком випадків, коли призначений орган виконує свої зобов'язання перед Адміністрацією Держспецзв'язку.

Призначений орган оприлюднює (повністю або частково) звіт про оцінку за згодою виробника.

6. У разі коли типовий зразок продукції відповідає вимогам Технічного регламенту призначений орган повинен видати виробнику сертифікат експертизи типу. У цьому сертифікаті повинно зазначатися найменування і місцезнаходження виробника, висновки за результатами експертизи, умови чинності сертифіката (якщо такі є) та дані, необхідні для ідентифікації затвердженого типу. До сертифіката експертизи типу можуть додаватися один чи більше додатків.

У сертифікаті експертизи типу та додатках до нього повинна міститися вся необхідна інформація, яка дає змогу оцінювати відповідність виготовленої продукції дослідженому типовому зразку, що пройшов експертизу, та здійснювати контроль під час експлуатації.

У разі коли типовий зразок продукції не відповідає застосовним вимогам Технічного регламенту, призначений орган вживає заходів визначених у пункті 46 Технічного регламенту.

7. Призначений орган повинен постійно відслідковувати будь-які зміни загальновизнаного рівня сучасного розвитку науки і техніки, які можуть вказувати на те, що затверджений тип продукції вже не відповідає застосовним вимогам Технічного регламенту, та повинен визначити, чи такі зміни потребують подальшого вивчення. Якщо це так, призначений орган повинен повідомити про це виробнику.

Виробник повинен інформувати призначений орган, який зберігає технічну документацію стосовно сертифіката експертизи типу, про всі модифікації затвердженого типу, що можуть вплинути на відповідність продукції суттєвим вимогам Технічного регламенту або на умови чинності цього сертифіката. Такі модифікації потребують додаткового затвердження у формі доповнення до первинного сертифіката експертизи типу.

8. Призначений орган повинен інформувати Адміністрацію Держспецзв'язку та інші призначені органи (за наявності) про видані або скасовані ним сертифікати експертизи типу та/або будь-які доповнення до них, а

також періодично чи на запит Адміністрації Держспецзв'язку надавати список таких сертифікатів та будь-яких доповнень до них, у видачі яких він відмовив або дію яких зупинив чи встановив щодо них інші обмеження.

Адміністрація Держспецзв'язку, інші органи державного ринкового нагляду та призначені органи мають право за запитами одержувати копію сертифікатів експертизи типу та/або доповнень до них, копію технічної документації та результати досліджень, проведених призначеним органом. Призначений орган зберігає копію сертифіката експертизи типу, додатків і доповнень до нього, а також технічний файл, в якому міститься подана виробником документація, доки не мине потреба але не менше ніж 10 років після введення останнього зразка продукції в обіг.

9. Виробник повинен зберігати копію сертифіката експертизи типу, додатків і доповнень до нього разом з технічною документацією для надання на запити органів державного ринкового нагляду, доки не мине потреба але не менше ніж 10 років після введення останнього зразка продукції в обіг.

10. Уповноважений представник виробника може подати заявку згідно з пунктом 3 цього додатка та виконувати обов'язки, визначені в пунктах 7 та 9 цього додатка, за умови визначення цих обов'язків у дорученні.

Додаток 3
до Технічного регламенту

МОДУЛЬ D
Відповідність типу на основі забезпечення якості виробничого процесу

1. Відповідність типу на основі забезпечення якості виробничого процесу є частиною процедури оцінки відповідності, за допомогою якої виробник виконує обов'язки, встановлені в пунктах 2 і 5 цього додатка, та гарантує і декларує під свою виключну відповідальність, що певна продукція відповідає типу, описаному в сертифікаті експертизи типу, та відповідає вимогам Технічного регламенту засобів криптографічного захисту інформації (далі – Технічний регламент), які застосовуються до зазначеної продукції.

Виробництво

2. Виробник повинен застосовувати схвалену систему управління якістю для виробництва, контролю та випробувань готової продукції, яка конкретизована в пунктах 3-7 цього додатка та підлягає нагляду, визначеному в пунктах 8-11 цього додатка.

Система управління якістю

3. Виробник подає призначеному органу з оцінки відповідності (далі - призначений орган) за вибором заявку на оцінку системи управління якістю стосовно певної продукції, в якій зазначається найменування та адреса виробника, а в разі подання заявки уповноваженим представником також його найменування і адреса та інформація про те, що така заявка не подана до жодного іншого призначеного органу, до якої додаються:

уся відповідна інформація стосовно характеристик засобу КЗІ, що розглядається;

документація стосовно системи управління якістю;

технічна документація щодо затвердженого типу продукції та копія сертифіката експертизи типу.

4. Система управління якістю повинна гарантувати відповідність продукції типу, описаному в сертифікаті експертизи типу, та застосовним вимогам Технічного регламенту.

Усі прийняті виробником елементи, вимоги та положення системи управління якістю повинні бути систематично і упорядковано задокументовані у вигляді політик, цілей та керівництв, викладених у письмовій формі.

Документація системи управління якістю має забезпечувати однозначне тлумачення програм, планів, настанов і записів щодо якості.

Зазначена документація повинна містити, зокрема, належний опис:

організаційної структури, обов'язків та повноважень керівництва стосовно контролю якості продукції;

відповідних методів виробництва, контролю якості та забезпечення якості, процесів і системних заходів, які будуть застосовуватися;

досліджень і випробувань, які будуть проводитися до, під час та після виробництва, а також періодичності їх проведення;

записів щодо якості виробничого процесу та/або продукції (протоколи контролю та результати випробувань, дані калібрувань, звітів про кваліфікацію відповідного персоналу та інше);

засобів моніторингу, за допомогою яких досягається необхідний рівень якості продукції та ефективного функціонування системи управління якістю.

5. Призначений орган повинен оцінити систему управління якістю з метою визначення рівня її відповідності вимогам, зазначеним у пункті 4 цього додатка.

Група з проведення аудиту, крім членів з досвідом стосовно систем управління якістю, повинна мати у своєму складі принаймні одного члена з досвідом оцінювання відповідної продукції та технології її виробництва, а також знаннями застосовних вимог Технічного регламенту. Проведення аудиту повинно включати відвідування підприємств виробника з метою їх оцінки. Група з проведення аудиту повинна оцінити технічну документацію, зазначену в абзаці сьомому пункту 4 цього додатка, з метою перевірки здатності виробника визначати відповідні вимоги Технічного регламенту та проводити дослідження, необхідні для забезпечення відповідності продукції таким вимогам.

Призначений орган повинен повідомити виробнику про своє рішення. Зазначене повідомлення повинно містити висновки аудиту та обґрунтоване рішення за результатами оцінки.

6. Виробник повинен виконувати зобов'язання, що виникають в результаті схвалення системи управління якістю, та підтримувати її в адекватному та ефективному стані.

7. Виробник зобов'язаний повідомляти призначеному органу, який схвалив систему управління якістю, про будь-які заплановані зміни у системі управління якістю.

Призначений орган повинен оцінити будь-які запропоновані зміни та прийняти рішення щодо того, чи буде змінена система управління якістю надалі відповідати вимогам, зазначеним у пункті 4 цього додатка, чи необхідно провести повторну оцінку.

Призначений орган повинен повідомити виробнику про своє рішення. Зазначене повідомлення повинно містити висновки дослідження та обґрунтоване рішення за результатами оцінки.

Нагляд під відповідальністю призначеного органу

8. Призначений орган здійснює нагляд з метою пересвідчитися в належному виконанні виробником обов'язків, що виникають в результаті схвалення системи управління якістю.

9. Для цілей оцінки виробник зобов'язаний надавати призначеному органу доступ до місць виробництва, контролю, випробувань і зберігання продукції, а також усю необхідну інформацію, зокрема:

документацію щодо системи управління якістю;

записи щодо якості (протоколи контролю та результати випробувань, дані калібрувань, звіти стосовно кваліфікації відповідного персоналу тощо).

10. Призначений орган повинен проводити періодичні аудити, щоб пересвідчитися в тому, що виробник підтримує в належному стані та застосовує систему управління якістю, та надавати виробнику звіт про аудит. Періодичність проведення аудиту становить не менше ніж один раз на рік.

11. Крім періодичних аудитів, призначений орган може здійснювати відвідування виробника без попередження. Під час таких відвідувань призначений орган може у разі потреби проводити випробування засобів КЗІ або доручати їх проведення з метою перевірки правильності функціонування системи управління якістю. Призначений орган повинен надавати виробнику звіт про відвідування, а у разі проведення випробувань - протокол випробувань.

Маркування знаком відповідності технічним регламентам, декларація про відповідність та заява про відповідність

12. Виробник наносить знак відповідності технічним регламентам та під відповідальність призначеного органу, зазначеного в пункті 3 цього додатка, його ідентифікаційний номер на кожну одиницю продукції (крім компонентів),

що відповідає типу, описаному в сертифікаті експертизи типу, та застосовним вимогам Технічного регламенту, які поширюються на цю продукцію.

13. Виробник складає письмову декларацію про відповідність для кожної моделі засобу КЗІ (крім компонентів). У декларації про відповідність повинна бути ідентифікована модель продукції, для якої її було складено. Кожен виріб (крім компонентів) повинен супроводжуватися копією декларації про відповідність.

14. Виробник повинен зберігати доки не мине потреба але не менше ніж 10 років після введення в обіг останньої одиниці засобу КЗІ:

документацію, зазначену в пунктах 3, 13 цього додатка;

інформацію щодо схвалених змін, зазначених у пункті 7 цього додатка;

рішення та звіти призначеного органу, зазначені в пунктах 7, 10 та 11 цього додатка.

15. Призначений орган повинен інформувати Адміністрацію Держспецзв'язку та інші призначені органи про системи управління якістю, які були схвалені або скасовані, а також періодично чи на їх запит, надавати список систем управління якістю, у схваленні яких відмовлено або дію яких зупинено чи іншим чином обмежено.

Уповноважений представник

16. Уповноважений представник виробника може подати заявку згідно з пунктом 3 цього додатка та виконувати обов'язки, визначені в пунктах 7 та 12-14 цього додатка, за умови визначення цих обов'язків у дорученні.

Додаток 4
до Технічного регламенту

ДЕКЛАРАЦІЯ
про відповідність вимогам Технічного регламенту засобів криптографічного захисту інформації

_____
(повне найменування виробника або його уповноважено представника чи постачальника,

_____
місцезнаходження, код ЄДРПОУ)

в особі _____
(посада, прізвище, ім'я та по батькові)

підтверджує, що _____
(повна назва засобу криптографічного захисту інформації, тип, марка, модель)

яка виготовляється за _____
(назва та позначення документа)

Відповідає технічному регламенту засобів криптографічного захисту інформації згідно з _____
(позначення та назва нормативного документа)

Комплект документації (експлуатаційної, технічної та з питань безпеки) до засобу криптографічного захисту інформації згідно вимог Технічного регламенту засобів криптографічного захисту інформації в наявності.

Протокол випробувань засобу криптографічного захисту інформації, що проведені (за наявності): _____
(місцезнаходження та назва призначеного органу

_____
з оцінки відповідності, протокол випробувань: дата оформлення, номер)

Декларацію складено під повну відповідальність: _____
(повне найменування

_____
виробника або його уповноваженого представника чи постачальника)

_____ _____ _____
(посада особи, яка склала декларацію про відповідність) (підпис) (прізвище та ініціали)

М.П.

«____» _____20___р. Місце для відмітки про реєстрацію декларації про відповідність

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проекту постанови Кабінету Міністрів України
«Про затвердження Технічного регламенту засобів криптографічного захисту інформації»

Мета: удосконалення процедур технічного регулювання у сфері криптографічного захисту інформації

1. Підстава розроблення проекту акта

Проект постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформацією» (далі – проект постанови) розроблено відповідно до статті 5 Закону України «Про технічні регламенти та оцінку відповідності», пункту 43 Плану розроблення технічних регламентів на 2018-2019 роки, затвердженого наказом Мінекономрозвитку від 15.02.2018 № 196.

2. Обґрунтування необхідності прийняття акту

Відповідно до пункту 2 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» функціонування національної системи кібербезпеки забезпечується шляхом створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО.

Відповідно до статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації (далі – КЗІ). Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

На цей час розроблення та оцінка відповідності засобів КЗІ здійснюється відповідно до таких нормативно-правових актів України:

Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22 травня 1998 року № 505/98;

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141, зареєстрованого в Мін'юсті 30.07.2007 за № 862/14129 (у редакції наказу Адміністрації Держспецзв'язку від 14.12.2015 № 767);

Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100, зареєстроване в Мін'юсті 16.07.2008 № 651/15342.

Зазначеними вище нормативно-правовими актами у сфері КЗІ не передбачено застосування процедури оцінки відповідності засобів КЗІ

відповідно до вимог Закону України «Про технічні регламенти та процедури оцінки відповідності».

Технічний регламент засобів криптографічного захисту інформації (далі – Технічний регламент) розроблено на основі таких міжнародних стандартів:

ISO/IEC 19790 Інформаційні технології. Методи захисту. Вимоги щодо захисту криптографічних модулів (видання друге від 15.08.2012 із змінами від 01.12.2015),

ISO/IEC 24759 Інформаційні технології. Методи захисту. Вимоги щодо перевірки криптографічних модулів (видання третє від березня 2017 року),

Також, відповідно до положень статті 394 та додатку XVII–3 Угоди про асоціацію між Україною з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі – Угода про асоціацію) Україна має імплементувати положення Регламенту (ЄС) 910/2014 Європейського Парламенту та Ради від 23 липня 2014 р. щодо електронної ідентифікації та довірчих послуг для цілей електронних трансакцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС Європейського Парламенту та Ради (далі - Регламент ЄС 910).

Згідно з підпунктом 7 пункту 1912 Плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі – Угода про асоціацію), затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106, необхідно привести у відповідність з міжнародними та європейськими стандартами національні акти технічного регулювання у сфері електронних довірчих послуг (інфраструктури відкритих ключів).

Імплементаційне Рішення Комісії (ЄС) 2016/650 від 25 квітня 2016 року щодо стандартів оцінки безпеки засобів для створення кваліфікованих підпису та печатки відповідно до статей 30(3) та 39(2) Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку, передбачає сертифікацію засобів кваліфікованого електронного підпису чи печатки (далі – засіб КЕП) відповідно до міжнародних та європейських стандартів з питань безпеки та захисту інформації:

1) ISO/IEC 15408 — Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій, частини 1–3, як зазначено нижче:

ISO/IEC 15408-1:2009 Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 1. ISO, 2009;

ISO/IEC 15408-2:2008 Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 2. ISO, 2008;

ISO/IEC 15408-3:2008 Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 3. ISO, 2008.

2) ISO/IEC 18045:2008: Інформаційні технології — Методи забезпечення безпеки — Методика оцінки безпеки інформаційних технологій;

3) EN 419 211 Профілі захисту для засобу для створення захищеного підпису, частини 1–6 — у відповідних випадках — як зазначено нижче:

EN 419211-1:2014 Профілі захисту для засобу для створення захищеного підпису — Частина 1: Огляд;

EN 419211-2:2013 Профілі захисту для засобу для створення захищеного підпису — Частина 2: Засіб з генерацією ключів;

EN 419211-3:2013 Профілі захисту для засобу для створення захищеного підпису — Частина 3: Засіб з імпортуванням ключів;

EN 419211-4:2013 Профілі захисту для засобу для створення захищеного підпису — Частина 4: Розширення для засобу з генерацією ключів і надійним каналом зв'язку з програмою генерації сертифікатів;

EN 419211-5:2013 Профілі захисту для засобу для створення захищеного підпису — Частина 5: Розширення для засобу з генерацією ключів і надійним каналом зв'язку з програмою створення підписів;

EN 419211-6:2014 Профілі захисту для засобу для створення захищеного підпису — Частина 6: Розширення для засобу з імпортуванням ключів і надійним каналом зв'язку з програмою створення підписі.

Технічний регламент передбачає механізми забезпечення виготовлення та оцінки відповідності засобів КЗІ, що є засобами КЕП (засоби КЗІ категорії «Е»), вимогам міжнародних та європейських стандартів EN 419211, ISO/IEC 15408, ISO/IEC 18045.

Отже, на сьогодні важливим є гармонізація норм Технічного регламенту з відповідними нормами міжнародних стандартів ISO/IEC 19790, ISO/IEC 24759 та тих, що необхідні для виконання вимог Регламенту (ЄС) 910, що у свою чергу повинно забезпечити: підвищення рівня безпечності продукції до загальноєвропейського; посилення відповідальності виробників і постачальників за безпечність продукції, сприяння транскордонній електронній торгівлі.

3. Суть проекту акта

Проектом постанови пропонується затвердити Технічний регламент, який встановить вимоги до розроблення, виготовлення, оцінки відповідності, експлуатації, відкликання, надання та вилучення з ринку, ринкового нагляду засобів криптографічного захисту інформації (продукція, криптографічний модуль), призначених для захисту відкритої та/або конфіденційної інформації.

Проектом постанови передбачено внесення змін до:

Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 лютого 2006 року № 373;

Переліку видів продукції, щодо яких органи державного ринкового нагляду здійснюють державний ринковий нагляд, затверджений постановою Кабінету Міністрів України від 28 грудня 2016 р. № 1069;

Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 р. № 411.

4. Правові аспекти

У даній сфері суспільних відносин діють Закони України «Про технічні регламенти та оцінку відповідності», «Про державний ринковий нагляд і контроль нехарчової продукції», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах».

Технічний регламент є рамковим документом, який охоплює сферу регулювання чинних на сьогодні Указу Президента України від 30.06.2011 № 717/2011 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» та наказу Адміністрації Держспецзв'язку від 20.07.2007 № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації», які з набранням його чинності потребуватимуть внесення змін.

4-1. Відповідність засадам реалізації органами виконавчої влади принципів державної політики цифрового розвитку

Проект постанови стосується засад реалізації органами виконавчої влади принципів державної політики цифрового розвитку та потребує проведення цифрової експертизи Державним агентством з питань електронного урядування України.

5. Фінансово-економічне обґрунтування

Упровадження положень проекту постанови не потребує додаткових фінансових витрат з державного бюджету.

6. Прогноз впливу

Проект постанови є регуляторним актом, за предметом правового регулювання має вплив на інтереси суб'єктів господарювання та держави шляхом запровадження обов'язковості проведення оцінки відповідності засобів КЗІ.

Проект постанови за предметом правового регулювання не має впливу на:
розвиток регіонів;
ринок праці;
громадське здоров'я;
екологію та навколишнє природнє середовище;
інші сфери суспільних відносин.

6-1. Стратегічна екологічна оцінка

Проект постанови не передбачає заходів для проведення моніторингу наслідків виконання документа державного планування для довкілля у тому числі для здоров'я населення, та не стосується вимог Закону України «Про стратегічну екологічну оцінку».

7. Позиція заінтересованих сторін

За результатами проведених консультацій із суб'єктами господарювання до проекту постанови, розміщеного на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України, висловлено пропозиції та

зауваження ІССЗЗІ НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» та ТОВ «ІННОВЕЙШН ДЕВЕЛОПМЕНТ ХАБ», які враховано частково.

Проект постанови матиме вплив на ключові інтереси заінтересованих сторін, про що зазначено в прогнозі впливу, що додається.

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 доведено до відома суб'єктів господарювання шляхом оприлюднення на офіційному веб-сайті Держспецзв'язку (http://www.dsszzi.gov.ua) у розділі «Регуляторна діяльність», підрозділ «Повідомлення про оприлюднення та проекти. До нього було висловлено пропозиції та зауваження ІССЗЗІ НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» та ТОВ «ІННОВЕЙШН ДЕВЕЛОПМЕНТ ХАБ», які враховано частково.

9. Позиція заінтересованих органів

Проект постанови потребує погодження з Мінекономрозвитку, ДРС, Мінфіном, Національним банком України, Державним агентством України з питань електронного урядування, Науковим комітетом Національної ради України з питань розвитку науки і технологій.

10.Правова експертиза

Проект постанови потребує проведення правової експертизи Міністерством юстиції України.

11. Запобігання дискримінації

У проекті постанови відсутні положення, які містять ознаки дискримінації.

Громадська антидискримінаційна експертиза проекту постанови не проводилася.

11-1. Відповідність принципу забезпечення рівних прав та можливостей жінок і чоловіків

У проекті постанови відсутні положення, які порушують принцип забезпечення рівних прав та можливостей жінок і чоловіків.

12. Запобігання корупції

У проекті постанови відсутні правила і процедури, які можуть містити ризики вчинення корупційних правопорушень.

Громадська антикорупційна експертиза проекту постанови не проводилася.

13. Прогноз результатів

Прийняття проекту постанови забезпечить:

відповідність засобів КЗІ вимогам з безпеки, визначених міжнародними та європейськими національними стандартами України;

запровадження незалежної оцінки відповідності засобів КЗІ відповідно до вимог Закону України «Про технічні регламенти та процедури оцінки відповідності»;

імплементацію вимог Регламенту ЄС 910 в частині безпеки засобів КЕП (засоби КЗІ категорії «Е»), що є зобов'язанням України в рамках виконання Угоди про асоціацію;

сприяння сумісності засобів КЗІ України та НАТО;

підвищення рівня доступності послуг електронного урядування з використанням засобів КЗІ;

підвищення рівня кіберзахисту.

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

«17» 05 2019 року

ПРОГНОЗ ВПЛИВУ
реалізації акта на ключові інтереси заінтересованих сторін

до проекту постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»

1. **Короткий опис суті проекту**
Запровадження процедур технічного регулювання у сфері криптографічного захисту інформації (далі – КЗІ) на засадах Закону України «Про технічні регламенти та оцінку відповідності» (далі – Закон) та встановлення суттєвих вимог до засобів КЗІ, що базуються на нормах національного стандарту України ISO/IEC 19790 «Інформаційні технології. Методи захисту. Вимоги щодо захисту криптографічних модулів».

2. **Вплив на ключові інтереси усіх заінтересованих сторін**

Заінтересована сторона	Ключовий інтерес	Очікуваний вплив на ключовий інтерес із зазначенням передбачуваної динаміки змін основних показників		Пояснення
		Короткостроковий вплив (до року)	Середньостроковий вплив (більше року)	
Громадяни	Підвищення рівня безпеки засобів КЗІ	позитивний	позитивний	Відповідність безпеки засобів КЗІ міжнародним стандартам
Держава	Підвищення рівня безпеки засобів КЗІ	позитивний	позитивний	Відповідність безпеки засобів КЗІ міжнародним стандартам
Суб'єкти господарювання (розробники засобів КЗІ)	Можливість створення конкурентноспроможньої продукції з підтвердженою відповідністю	позитивний (перехідний період – застосування старої та нової процедури оцінки відповідності)	позитивний (перехідний період – застосування старої та нової процедури оцінки відповідності)	Міжнародне визнання документів про відповідність, виданих відповідно до вимог Закону

Голова Державної служби спеціального зв'язку та захисту інформації України
«17» 05 2019 року

Леонід Євдоченко

Порівняльна таблиця
до проекту постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»

<table>
<tr><th>Зміст положення (норми) чинного законодавства</th><th>Зміст відповідного положення (норми) проекту акта</th></tr>
<tr><td colspan="2">Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 лютого 2006 року № 373</td></tr>
<tr><td>22. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією.</td><td>22. Порядок проведення державної експертизи системи захисту, державної експертизи засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією.</td></tr>
<tr><td colspan="2">Перелік видів продукції, щодо яких органи державного ринкового нагляду здійснюють державний ринковий нагляд, затверджений постановою Кабінету Міністрів України від 28 грудня 2016 р. № 1069</td></tr>
<tr><td>…
Норма відсутня
…</td><td><table>
<tr><td>…</td><td>…</td><td>…</td></tr>
<tr><td>52. Засоби криптографічного захисту інформації</td><td>постанова Кабінету Міністрів України від _____ 20__ р. № _____ «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»</td><td>Адміністрація Держспецзв’язку</td></tr>
</table></td></tr>
</table>

Зміст положення (норми) чинного законодавства	Зміст відповідного положення (норми) проекту акта
Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 р. № 411	
4. Адміністрація Держспецзв'язку відповідно до покладених на неї завдань: … **Норма відсутня** …	4. Адміністрація Держспецзв'язку відповідно до покладених на неї завдань: … **7^1) здійснює державний ринковий нагляд у межах сфери своєї відповідальності;** …

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

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
до проекту постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформацією»

І. Визначення проблеми

Проект постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформацією» (далі – проект постанови) розроблено Адміністрацією Держспецзв'язку на виконання пункту 43 Плану розроблення технічних регламентів на 2018-2019 роки, затвердженого наказом Мінекономрозвитку від 15.02.2018 № 196.

Відповідно до пункту 2 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» функціонування національної системи кібербезпеки забезпечується шляхом створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО.

Відповідно до статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації (далі – КЗІ). Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

На цей час розроблення та оцінка відповідності засобів КЗІ здійснюється відповідно до таких нормативно-правових актів України:

Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22 травня 1998 року № 505/98;

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141, зареєстрованого в Мін'юсті 30.07.2007 за № 862/14129 (у редакції наказу Адміністрації Держспецзв'язку від 14.12.2015 № 767);

Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100, зареєстроване в Мін'юсті 16.07.2008 № 651/15342.

Зазначеними вище нормативно-правовими актами у сфері КЗІ не передбачено застосування процедури оцінки відповідності засобів КЗІ

відповідно до вимог Закону України «Про технічні регламенти та процедури оцінки відповідності».

Технічний регламент засобів криптографічного захисту інформації (далі – Технічний регламент) розроблено на основі таких міжнародних стандартів:

ISO/IEC 19790 Інформаційні технології. Методи захисту. Вимоги щодо захисту криптографічних модулів (видання друге від 15.08.2012 із змінами від 01.12.2015),

ISO/IEC 24759 Інформаційні технології. Методи захисту. Вимоги щодо перевірки криптографічних модулів (видання третє від березня 2017 року),

Також, відповідно до положень статті 394 та додатку XVII–3 Угоди про асоціацію між Україною з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі – Угода про асоціацію) Україна має імплементувати положення Регламенту (ЄС) 910/2014 Європейського Парламенту та Ради від 23 липня 2014 р. щодо електронної ідентифікації та довірчих послуг для цілей електронних трансакцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС Європейського Парламенту та Ради (далі - Регламент ЄС 910).

Згідно з підпунктом 7 пункту 1912 Плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі – Угода про асоціацію), затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106, необхідно привести у відповідність з міжнародними та європейськими стандартами національні акти технічного регулювання у сфері електронних довірчих послуг (інфраструктури відкритих ключів).

Імплементаційне Рішення Комісії (ЄС) 2016/650 від 25 квітня 2016 року щодо стандартів оцінки безпеки засобів для створення кваліфікованих підпису та печатки відповідно до статей 30(3) та 39(2) Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку, передбачає сертифікацію засобів кваліфікованого електронного підпису чи печатки (далі – засіб КЕП) відповідно до міжнародних та європейських стандартів з питань безпеки та захисту інформації:

1) ISO/IEC 15408 — Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій, частини 1–3, як зазначено нижче:

ISO/IEC 15408-1:2009 Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 1. ISO, 2009;

ISO/IEC 15408-2:2008 Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 2. ISO, 2008;

ISO/IEC 15408-3:2008 Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 3. ISO, 2008.

2) ISO/IEC 18045:2008: Інформаційні технології — Методи забезпечення безпеки — Методика оцінки безпеки інформаційних технологій;

3) EN 419 211 Профілі захисту для засобу для створення захищеного підпису, частини 1–6 — у відповідних випадках — як зазначено нижче:

EN 419211-1:2014 Профілі захисту для засобу для створення захищеного підпису — Частина 1: Огляд;

EN 419211-2:2013 Профілі захисту для засобу для створення захищеного підпису — Частина 2: Засіб з генерацією ключів;

EN 419211-3:2013 Профілі захисту для засобу для створення захищеного підпису — Частина 3: Засіб з імпортуванням ключів;

EN 419211-4:2013 Профілі захисту для засобу для створення захищеного підпису — Частина 4: Розширення для засобу з генерацією ключів і надійним каналом зв'язку з програмою генерації сертифікатів;

EN 419211-5:2013 Профілі захисту для засобу для створення захищеного підпису — Частина 5: Розширення для засобу з генерацією ключів і надійним каналом зв'язку з програмою створення підписів;

EN 419211-6:2014 Профілі захисту для засобу для створення захищеного підпису — Частина 6: Розширення для засобу з імпортуванням ключів і надійним каналом зв'язку з програмою створення підписі.

Технічний регламент передбачає механізми забезпечення виготовлення та оцінки відповідності засобів КЗІ, що є засобами КЕП (засоби КЗІ категорії «Е»), вимогам міжнародних та європейських стандартів EN 419211, ISO/IEC 15408, ISO/IEC 18045.

Отже, на сьогодні важливим є гармонізація норм Технічного регламенту з відповідними нормами міжнародних стандартів ISO/IEC 19790, ISO/IEC 24759 та тих, що необхідні для виконання вимог Регламенту (ЄС) 910, що у свою чергу повинно забезпечити: підвищення рівня безпечності продукції до загальноєвропейського; посилення відповідальності виробників і постачальників за безпечність продукції, сприяння транскордонній електронній торгівлі.

Основні групи, на які проблема справляє вплив:

Групи	Так	Ні
Громадяни	Так	
Держава	Так	
Суб'єкти господарювання	Так	

Проблема не може бути розв'язана за допомогою ринкових механізмів, оскільки це не буде відповідати вимогам чинного законодавства України.

II. Цілі державного регулювання

Основними цілями розроблення проекту постанови є:

забезпечення відповідності засобів КЗІ вимогам з безпеки, визначених міжнародними та європейськими національними стандартами України;

запровадження незалежної оцінки відповідності засобів КЗІ відповідно до вимог Закону України «Про технічні регламенти та процедури оцінки відповідності»;

імплементація вимог Регламенту ЄС 910 з безпеки засобів КЕП (засоби КЗІ категорії «Е»), що є зобов'язанням України в рамках виконання Угоди про асоціацію;

сприяння сумісності засобів КЗІ України та НАТО;

підвищення рівня доступності послуг електронного урядування з використанням засобів КЗІ;

підвищення рівня кіберзахисту.

Цей проект регуляторного акта має сприяти в цілому розв'язанню проблеми, зазначеної в попередньому розділі аналізу регуляторного впливу.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	*Прийняття проекту постанови*
Альтернатива 2	*Збереження чинного регулювання*

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. *Прийняття проекту постанови*	Високі, передбачає створення нормативно-правової бази у сфері КЗІ, необхідної для належного функціонування національної системи кібербезпеки; створення умов для міжнародного співробітництва у сфері електронних довірчих послуг та електронної ідентифікації	Впровадження вимог регуляторного акта державними органами не потребує додаткових витрат з бюджету, оскільки здійснюватиметься в межах повноважень відповідних органів та діючого законодавства
Альтернатива 2. *Збереження чинного регулювання*	Відсутні, оскільки дана ситуація призведе до відставання технологій з розроблення та оцінки засобів КЗІ від кращих міжнародних практик	Вразливості системи кіберзахисту через недосконалість засобів КЗІ Не виконання зобов'язань в рамках Угоди про асоціацію

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. *Прийняття проекту постанови*	Високі, отримання безпечної, сумісної з сервісами електронного урядування продукції з відповідним рівнем гарантій	Додаткових витрат не потребує
Альтернатива 2. *Збереження чинного регулювання*	Відсутні	Ризики компрометації засобів КЗІ через їх невідповідність сучасним вимогам з безпеки, що може призвести до моральних та економічних витрат.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Оцінка впливу на сферу інтересів суб'єктів господарювання

Під час визначення впливу на сферу інтересів суб'єктів господарювання доцільно розглянути такі фактори, зокрема:

вплив на продуктивність та конкурентоспроможність суб'єктів господарювання;

вплив на інновації та розвиток.

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	14	15	-	-	29
Питома вага групи у загальній кількості, відсотків	45%	55%	-	-	100%

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. *Прийняття проекту постанови*	Високі Створення більш якісної (безпечної) продукції, застосування якої передбачено законодавством у сферах кіберзахисту та електронних довірчих послуг, сприятиме попиту на неї та надасть можливість суб'єктам господарювання, що є розробниками, виробниками та	Додаткових витрат не потребує

	розповсюджувачами засобів КЗІ, а також органами з оцінки відповідності, отримати додаткові прибутки	
Альтернатива 2. *Збереження чинного регулювання*	Відсутні	Додаткових витрат не потребує

Сумарні витрати за альтернативами	**Сума витрат, гривень**
Альтернатива 1. *Прийняття проекту постанови*	Додаткових витрат не потребує
Альтернатива 2. *Збереження чинного регулювання*	Додаткових витрат не потребує

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Вибір оптимального альтернативного способу здійснюється з урахуванням системи бальної оцінки ступеня досягнення визначених цілей.

Вартість балів визначається за чотирибальною системою оцінки ступеня досягнення визначених цілей, де:

4 - цілі прийняття регуляторного акта, які можуть бути досягнуті повною мірою (проблема більше існувати не буде);

3 - цілі прийняття регуляторного акта, які можуть бути досягнуті майже повною мірою (усі важливі аспекти проблеми існувати не будуть);

2 - цілі прийняття регуляторного акта, які можуть бути досягнуті частково (проблема значно зменшиться, деякі важливі та критичні аспекти проблеми залишаться невирішеними);

1 - цілі прийняття регуляторного акта, які не можуть бути досягнуті (проблема продовжує існувати).

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	**Бал результативності (за чотирибальною системою оцінки)**	**Коментарі щодо присвоєння відповідного бала**
1. Прийняття проекту постанови	4	Цілі прийняття регуляторного акта можуть бути досягнуті повною мірою (проблема більше існувати не буде)
2. Залишення існуючої ситуації без змін	1	Цілі прийняття регуляторного акта не можуть бути досягнуті (проблема продовжить існувати)

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
1. Прийняття проекту постанови	Підвищення рівня безпеки засобів КЗІ	Додаткових витрат не потребує	проблема більше існувати не буде
2. Залишення існуючої ситуації без змін	немає	Збільшення витрат на ліквідацію наслідків кібератак, компрометації даних тощо	проблема продовжує існувати

V. 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 Технічний регламент.

Технічний регламент визначає:

суб’єктів відносин у сфері КЗІ, їх функції та обов’язки;

вимоги до розроблення, виготовлення, оцінки відповідності, експлуатації, відкликання, надання та вилучення з ринку, ринкового нагляду засобів КЗІ;

суттєві вимоги до засобів КЗІ;

Для досягнення цієї цілі проектом постанови передбачається:

затвердити Технічний регламент;

внести зміни до постанови Кабінету Міністрів України від 28.12.2016 № 1069 «Про затвердження переліку видів продукції, щодо яких органи державного ринкового нагляду здійснюють державний ринковий нагляд»;

внести зміни до постанови Кабінету Міністрів України від 29.02.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

перехідний період, що включає поетапне застосування норм Технічного регламенту.

Заходи, що пропонуються для розв’язання проблеми:

погодити проект постанови із заінтересованими державними органами;

направити проект постанови на правову експертизу до Мін’юсту;

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

забезпечити інформування суб’єктів господарювання, на сферу дії яких поширюватиметься регуляторний акт, про вимоги регуляторного акта.

Реалізація положень проекту постанови забезпечить:

відповідність засобів КЗІ вимогам з безпеки, визначених міжнародними та європейськими національними стандартами України;

запровадження незалежної оцінки відповідності засобів КЗІ відповідно до вимог Закону України «Про технічні регламенти та процедури оцінки відповідності»;

імплементацію вимог Регламенту ЄС 910 з безпеки засобів КЕП (засоби КЗІ категорії «Е»), що є зобов'язанням України в рамках виконання Угоди про асоціацію;

сприяння сумісності засобів КЗІ України та НАТО;

підвищення рівня доступності послуг електронного урядування з використанням засобів КЗІ;

підвищення рівня кіберзахисту.

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

Адміністрація Держспецзв'язку повинна забезпечити:

впровадження затвердженого Технічного регламенту;

розробку та приведення власних нормативно-правових актів у відповідність із цією постановою до дня набрання її чинності.

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

Розрахунок витрат на виконання вимог регуляторного акта для органів виконавчої влади, органів місцевого самоврядування не здійснюється.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності проекту постанови, як регуляторного акта є:

1) розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта – не прогнозується;

2) кількість суб'єктів господарювання та/або фізичних осіб, на яких поширюватиметься дія акта;

3) розмір коштів і час, що витрачатимуться суб'єктами господарювання, пов'язаними з виконанням вимог акта – не прогнозується;

4) кількість звернень від суб'єктів господарювання та/або фізичних осіб, на яких поширюватиметься дія акта;

5) рівень поінформованості суб'єктів господарювання та/або фізичних осіб стосовно основних положень регуляторного акта – достатньо високий.

З цією метою проект регуляторного акту оприлюднений на офіційному веб-сайті Держспецзв'язку для громадського обговорення, а після прийняття акта він буде опублікований у засобах масової інформації та розміщений на сайтах Кабінету Міністрів України, Верховної Ради України та в інформаційно-аналітичній системі "Ліга".

IX. 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 акту з метою внесення до нього змін.

Базове відстеження результативності регуляторного акта буде здійснюватися через один рік, після набрання чинності цього регуляторного акта 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

«17» 05 2019 року

Додаток 1

ВИТРАТИ
на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1	2	3	4
1	Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо, гривень	0 грн.	0 грн.
2	Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів), гривень	0 грн.	0 грн.
3	Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень	0 грн.	0 грн.
4	Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо), гривень	0 грн.	0 грн.
5	Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень	0 грн.	0 грн.
6	Витрати на оборотні активи (матеріали, канцелярські товари тощо), гривень	0 грн.	0 грн.
7	Витрати, пов'язані із наймом додаткового персоналу, гривень	0 грн.	0 грн.
8	Інше (уточнити), гривень	0 грн.	0 грн.
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень	0 грн.	0 грн.
10	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць*	29	
11	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень	0 грн.	0 грн.
* статистика стосовно розподілу на суб'єктів господарювання малого, середнього чи великого підприємництва не ведеться та не вимагається			

Розрахунок відповідних витрат на одного суб'єкта господарювання

Вид витрат	У перший рік	Періодичні (за рік)	Витрати за п'ять років
Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо	0 грн.	0 грн.	0 грн.

Вид витрат	Витрати на сплату податків та зборів (змінених/нововведених) (за рік)	Витрати за п'ять років
Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів)	0 грн.	0 грн.

Вид витрат	Витрати* на ведення обліку, підготовку та подання звітності (за рік)	Витрати на оплату штрафних санкцій за рік	Разом за рік	Витрати за п'ять років
Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам (витрати часу персоналу)	0 грн.	0 грн.	0 грн.	0 грн.

* Вартість витрат, пов`язаних із підготовкою та поданням звітності державним органам, визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації).

Вид витрат	Витрати* на адміністрування заходів державного нагляду (контролю) (за рік)	Витрати на оплату штрафних санкцій та усунення виявлених порушень (за рік)	Разом за рік	Витрати за п'ять років
Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо)	0 грн.	0 грн.	0 грн.	0 грн.

* Вартість витрат, пов`язаних з адмініструванням заходів державного нагляду (контролю), визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації.

Вид витрат	Витрати на проходження відповідних процедур (витрати часу, витрати на експертизи, тощо)	Витрати безпосередньо на дозволи, ліцензії, сертифікати, страхові поліси (за рік - стартовий)	Разом за рік (стартовий)	Витрати за п'ять років
Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо)	0 грн.	0 грн.	0 грн.	0 грн.

Вид витрат	За рік (стартовий)	Періодичні (за наступний рік)	Витрати за п'ять років
Витрати на оборотні активи (матеріали, канцелярські товари тощо)	0 грн.	0 грн.	0 грн.

Вид витрат	Витрати на оплату праці додатково найманого персоналу (за рік)	Витрати за п'ять років
Витрати, пов'язані із наймом додаткового персоналу	0 грн.	0 грн.

Повідомлення про оприлюднення
проекту постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»

1. Стислий виклад змісту проекту акта

Проект постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформацією» (далі – проект постанови) розроблено відповідно до статті 5 Закону України «Про технічні регламенти та оцінку відповідності» (далі – Закон), пункту 43 Плану розроблення технічних регламентів на 2018-2019 роки, затвердженого наказом Мінекономрозвитку від 15.02.2018 № 196.

Технічним регламентом запроваджуються процедури оцінки відповідності засобів криптографічного захисту інформації (далі – КЗІ) відповідно до вимог Закону.

Технічний регламент визначає:

суб'єктів відносин у сфері КЗІ, їх функції та обов'язки;

вимоги до розроблення, виготовлення, оцінки відповідності, експлуатації, відкликання, надання та вилучення з ринку, ринкового нагляду засобів КЗІ;

суттєві вимоги до засобів КЗІ.

2. Адреси для зауважень та пропозицій до проекту акта:

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

поштова: вул. Солом'янська, 13, м. Київ, 03680;

електронна: info@dsszzi.gov.ua;

Державної регуляторної служби України:

поштова: вул. Арсенальна, 9/11, м. Київ, 01011;

електронна: inform@dkrp.gov.ua

3. Обраний спосіб оприлюднення проекту акта

Проект постанови та аналіз регуляторного впливу розміщено на веб-сайті Держспецзв'язку.

4. Строк, протягом якого приймаються зауваження та пропозиції

Пропозиції та зауваження до проекту постанови просимо надсилати протягом місяця з дати його оприлюднення.

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

«17» 05 2019 р.

вх. № 04/02/03-1445

Прим. № ____

ВИСНОВОК
про проведення гендерно-правової експертизи проекту постанови Кабінету Міністрів України

"Про затвердження Технічного регламенту засобів криптографічного захисту інформації"

Проект нормативно-правового акта розроблено Адміністрацією Державної служби спеціального зв'язку та захисту інформації України

1. **Перелік міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, та резолюцій міжнародних конференцій, міжнародних організацій, їх органів, використаних під час проведення експертизи.**

Під час проведення гендерно-правової експертизи проекту нормативно-правового акта застосовувалися: Міжнародний пакт про громадянські і політичні права, 1966 рік; Конвенція про боротьбу з торгівлею людьми і з експлуатацією проституції третіми особами, 1949 рік; Конвенція про ліквідацію всіх форм дискримінації щодо жінок, 1979 рік; Конвенція про захист прав людини і основоположних свобод, 1950 рік та протоколи до неї; Європейська соціальна хартія (переглянута), 1996 рік; Конвенція Ради Європи про заходи щодо протидії торгівлі людьми, 2005 рік; Конвенція про права осіб з інвалідністю, 2006 рік; Конвенція Міжнародної організації праці № 156 про рівне ставлення і рівні можливості для трудящих чоловіків і жінок: трудящі із сімейними обов'язками, 1981 рік; Конвенція Міжнародної організації праці № 100 про рівне винагородження чоловіків і жінок за працю рівної цінності, 1951 рік; Міжнародна конвенція про ліквідацію всіх форм расової дискримінації, 1965 рік; Міжнародний пакт про економічні, соціальні і культурні права, 1966 рік; Рамкова конвенція про захист національних меншин, 1995 рік; Загальна декларація прав людини, 1948 рік; Пекінська декларація, 1995 рік; Резолюція 47/135 Генеральної Асамблеї ООН "Декларація про права осіб, що належать до національних або етнічних, релігійних та мовних меншин", 1992 рік.

2. Перелік актів законодавства, використаних під час експертизи.

Під час проведення гендерно-правової експертизи проекту нормативно-правового застосовувалися: Конституція України, Закони України "Про забезпечення рівних прав та можливостей жінок і чоловіків", "Про засади запобігання та протидії дискримінації в Україні", "Про запобігання та протидію домашньому насильству", "Про протидію торгівлі людьми".

дод. 04/02/03 - 11445

3. Наявність або відсутність положень проекту нормативно-правового акта, які не відповідають принципу забезпечення рівних прав та можливостей жінок і чоловіків.

У проекті нормативно-правового акта немає положень, які не відповідають принципу забезпечення рівних прав та можливостей жінок і чоловіків.

4. Проведення аналізу положень проекту нормативно-правового акта, які можуть порушувати принцип забезпечення рівних прав та можливостей жінок і чоловіків.

У проекті нормативно-правового акта немає положень, які не відповідають принципу забезпечення рівних прав та можливостей жінок і чоловіків.

Директор Департаменту правової роботи
Адміністрації Державної служби спеціального
зв'язку та захисту інформації України Сергій Федорів

Заступник Голови Державної
служби спеціального зв'язку та
захисту інформації України Петро Опаленик

16 травня 2019 р.

Власюк А.М. 281 92 97

КОПІЯ

Прим. № 1

ВИСНОВОК

про проведення антидискримінаційної експертизи
проекту постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»

Проект постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації» (далі – проект акта) розроблено Адміністрацією Держспецзв'язку.

1. Положення проекту акта, які містять ознаки дискримінації

Положень, які містять ознаки дискримінації, у проекті акта немає

(зазначається про наявність(наводиться відповідне положення) або відсутність у проекті акта положень, які містять ознаки дискримінації)

2. Обґрунтування дискримінаційного характеру положень проекту акта

Немає

(у разі наявності у проекті акта положень, які містять ознаки дискримінації, зазначається їх дискримінаційний характер, а також наслідки, до яких може призвести їх застосування)

3. Пропозиції щодо усунення у проекті акта положень, які містять ознаки дискримінації

Відсутні

(зазначаються пропозиції щодо усунення положень, які містять ознаки дискримінації)

Директор Департаменту правової роботи
Адміністрації Державної служби спеціального
зв'язку та захисту інформації України
полковник юстиції С.М. Федорів

(підпис)

14 травня 2019 року

18/01-752
14.05.2019

Власюк А.М. 281 92 97

Служба діловодства
Адміністрації Держспецзв'язку
1 №1
Вх. № 2814
(кількість) від 16 05 2019