ТЕХНІЧНИЙ РЕГЛАМЕНТ
засобів криптографічного захисту інформації

Загальна частина

1. Цей Технічний регламент встановлює вимоги з безпеки до засобів криптографічного захисту інформації, що використовуються на об'єктах критичної інформаційної інфраструктури або відповідно до вимог законодавства.

Вимоги цього Технічного регламенту не розповсюджуються на засоби криптографічного захисту інформації, які використовуються фізичною особою або групою фізичних осіб для власних потреб.

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:
АЗ – апаратне забезпечення;
ВПЗ – вбудоване програмне забезпечення;
ГВБ – генератор випадкових бітів;
КЗІ – криптографічний захист інформації;
КПБ – критичні параметри безпеки;
ПЗ – програмне забезпечення;
ППБ – публічні параметри безпеки;
ЧПБ – чутливі параметри безпеки.

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

1) введення в експлуатацію – використання засобів КЗІ за його призначенням споживачем (користувачем) в Україні вперше;

2) введення в обіг – надання засобів КЗІ на ринку України вперше;

3) вилучення з обігу – будь-який захід, спрямований на запобігання наданню на ринку засобів КЗІ, що перебувають в ланцюгу постачання засобів КЗІ;

4) виробник – будь-яка фізична чи юридична особа (резидент чи нерезидент України), яка виготовляє засіб КЗІ або доручає його розроблення чи виготовлення та реалізує засоби КЗІ під своїм найменуванням або торговельною маркою (знаком для товарів);

5) відкликання – будь-який захід, спрямований на забезпечення повернення засобів КЗІ, які вже було надано споживачу (користувачу);

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

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

8) знак відповідності технічним регламентам – маркування, за допомогою якого виробник вказує, що засіб КЗІ відповідає вимогам, визначеним у технічних регламентах, якими передбачено нанесення цього маркування;

9) електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис;

10) імпортер – будь-яка фізична чи юридична особа, яка є суб'єктом господарювання – резидентом України і яка вводить в обіг на території України засоби КЗІ походженням з іншої країни;

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

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

13) модель кінцевих станів – математична модель послідовного механізму, яка складається з кінцевого набору вхідних подій (входів), кінцевого набору вихідних подій (виходів), кінцевого набору станів, функцій, які відображають зв'язок стану і входу з виходом, функцій, які відображають зв'язок стану та входу зі станом (функція переходу станів), специфікацій, які описують початковий стан;

14) надання на ринку – будь-яке платне або безоплатне постачання засобів КЗІ для розповсюдження, споживання чи використання на ринку України у процесі провадження господарської діяльності;

15) неінвазивна атака – атака, яка може бути здійснена на засіб КЗІ без фізичного контакту з ним або його компонентами, які знаходяться в криптографічній межі;

16) неінвазивна безпека – захищеність засобу КЗІ від неінвазивних атак;

17) ключовий документ – носій ключової інформації встановленого зразка із значеннями КПБ;

18) орган з оцінки відповідності – орган (підприємство, установа, організація чи їх структурний підрозділ), що здійснює діяльність з оцінки

відповідності, у тому числі калібрування, випробування, сертифікацію та інспектування;

19) оцінка відповідності – процес доведення того, що задані вимоги, які стосуються продукції, процесу, послуги, системи, особи чи органу, були виконані;

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

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

22) профіль захисту – нормативний документ, що визначає сукупність завдань захисту та набір функцій безпеки для певної категорії засобів КЗІ;

23) публічні параметри безпеки – публічна інформація, пов'язана з безпекою, модифікація якої може скомпрометувати безпеку засобу КЗІ;

24) ризик компрометації інформації – будь-яка подія, що призвела або з високою ймовірністю може призвести до порушення властивостей інформації (конфіденційність, цілісність, доступність, неспростовність), для захисту яких призначено засіб КЗІ;

25) розповсюджувач – будь-яка інша (не виробник або імпортер) фізична чи юридична особа в ланцюгу постачання продукції, яка надає продукцію на ринку;

26) суб'єкти господарювання – виробники, уповноважені представники, імпортери та розповсюджувачі;

27) схвалена функція безпеки – криптографічні алгоритми та протоколи, методи захисту (генерації та встановлення ЧПБ, автентифікації сутностей тощо), профілі захисту, технічні специфікації, показники для проведення тестування засобів КЗІ для пом`якшення наслідків неінвазивних атак, що визначені або погоджені Адміністрацією Держспецзв'язку, у випадках, передбачених законом, затверджені Кабінетом Міністрів України, для реалізації в засобах КЗІ відповідно до законодавства;

28) 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;

29) технічна специфікація – документ, що встановлює технічні вимоги, яким повинна задовольняти продукція, процес або послуга у сфері КЗІ;

30) уповноважений представник – будь-яка фізична чи юридична особа – резидент України, яка одержала від виробника письмове доручення діяти від його імені стосовно визначених завдань;

31) характеристика засобу КЗІ – тип засобу КЗІ, категорія засобу КЗІ, порядок доступу до інформації, для захисту якої призначено засіб КЗІ, рівень безпеки засобу КЗІ та інша інформація, що дозволяє визначити можливість

застосування засобу КЗІ в певній інформаційно-телекомунікаційній системі або відповідно до вимог законодавства;

32) цифровий підпис – електронний підпис, створений за результатом криптографічного перетворення блоку даних, з якими пов'язаний цей електронний підпис, що дає можливість одержувачеві блоку даних довести його походження і цілісність, а також захистити від підробки. Цифровий підпис при виконанні умов Закону України «Про електронні довірчі послуги» може застосовуватися як удосконалений електронний підпис чи печатка або кваліфікований електронний підпис чи печатка;

33) 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 тестування криптографічних модулів» (далі – ДСТУ ISO/IEC 24759).

5. Залежно від способу реалізації розрізняють такі типи засобів КЗІ:

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

засоби КЗІ, призначені 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»).

Суттєві вимоги

7. Засоби КЗІ повинні бути розроблені таким чином, щоб забезпечити їх безпечну конструкцію та встановлення для досягнення таких цілей безпеки:

використання і коректної реалізації схвалених функцій безпеки;

захисту засобу КЗІ від несанкціонованого використання або експлуатації;

запобігання несанкціонованому розкриттю змісту засобу КЗІ, у тому числі критичних параметрів безпеки;

запобігання несанкціонованій та непоміченій модифікації засобу КЗІ і криптографічних алгоритмів, у тому числі несанкціонованій модифікації, заміні, вставці і видаленню загальних послуг;

інформування про робочий стан засобу КЗІ;

переконання, що засіб КЗІ коректно функціонує у схваленому режимі;

виявлення помилок у роботі засобу КЗІ і запобігання компрометації ЧПБ через помилки;

забезпечення належного проєктування, доставки й встановлення засобу КЗІ.

8. Засоби КЗІ повинні відповідати Загальним вимогам до рівнів безпеки засобів КЗІ, наведеним у додатку 1, в обсязі, встановленому для відповідного рівня безпеки.

Засоби КЗІ повинні відповідати одному з чотирьох рівнів безпеки:

рівень безпеки 1 – базовий рівень безпеки, обов'язковий для всіх засобів КЗІ, що містить основні заходи безпеки, визначені у Загальних вимогах до рівнів безпеки, за всіма компонентами безпеки;

рівень безпеки 2 – рівень з додатковими до рівня безпеки 1 заходами безпеки, визначеними у Загальних вимогах до рівнів безпеки засобів КЗІ, що належать 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 Загальних вимогах до рівнів безпеки засобів КЗІ, що

належать 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 Загальних вимогах до рівнів безпеки засобів КЗІ, що належать до компонентів безпеки 3, 6, 10 (в частині опису, доставки та експлуатації) та 11.

9. Рівень безпеки засобу КЗІ повинен визначається у сукупності за такими компонентами безпеки:

1) специфікація засобу КЗІ;
2) інтерфейси засобу КЗІ;
3) ролі, послуги та автентифікація;
4) безпека ПЗ/ВПЗ;
5) операційне середовище;
6) фізична безпека;
7) неінвазивна безпека;
8) управління ЧПБ;
9) самотестування;
10) гарантії життєвого циклу;
11) пом'якшення атак.

10. У засобах КЗІ опціонально повинні бути реалізовані схвалені функції безпеки, якщо законодавством не встановлено обов'язковість реалізації певного набору функцій безпеки:

1) блокові шифри;
2) потокові шифри;
3) асиметричні алгоритми й методи;
4) коди автентифікації повідомлень;
5) геш-функції;
6) автентифікація сутностей;
7) управління ключами;
8) генерація випадкових бітів;
9) генерація ЧПБ;
10) методи управління ключами;
11) методи автентифікації;
12) метрики тестування послаблення наслідків неінвазивних атак;
13) профілі захисту.

Схвалені функції безпеки 1) - 11) цього пункту визначаються переліками національних стандартів України та технічних специфікацій, затверджених Адміністрацією Держспецзв'язку.

11. Засоби КЗІ категорії «Е» повинні відповідати профілям захисту інформації, встановленим Кабінетом Міністрів України.

Презумпція відповідності суттєвим вимогам

12. Презумпцією відповідності засобів КЗІ суттєвим вимогам є реалізація норм ДСТУ ISO/IEC 19790 та оцінка відповідності засобів КЗІ відповідно до вимог ДСТУ ISO/IEC 24759 у спосіб, визначений пунктом 50 цього Технічного регламенту.

Додатково для засобів КЗІ, які відповідно до законодавства повинні відповідати профілю захисту інформації, розробленому згідно ДСТУ ISO/IEC 15408 «Інформаційні технології. Методи захисту. Критерії оцінки», оцінка відповідності засобів КЗІ такому профілю здійснюватися з дотриманням вимог ДСТУ ISO/IEC 18045 «Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ».

Надання засобів КЗІ на ринку

13. Засоби КЗІ надаються на ринку у разі, коли вони відповідають вимогам цього Технічного регламенту.

14. Засоби КЗІ категорії «Е» надаються на ринку з дотриманням вимог Закону України «Про електронні довірчі послуги».

15. Надання на ринку засобів КЗІ, призначених для надання та/або отримання послуг електронного урядування, допускається після підтвердження їх сумісності із сервісами електронного урядування в установленому Міністерством цифрової трансформації України порядком.

Введення в експлуатацію засобів КЗІ

16. Засоби КЗІ вводяться в експлуатацію у разі, коли вони відповідають вимогам цього Технічного регламенту, та за умови належного встановлення, обслуговування та використання за своїм призначенням.

Вільне переміщення засобів КЗІ

17. Забороняється перешкоджати наданню на ринку України засобів КЗІ, які відповідають вимогам цього Технічного регламенту, якщо інше не встановлено законом та цим Технічним регламентом.

Обов'язки виробників

18. Виробники під час введення в обіг засобів КЗІ повинні забезпечувати, щоб ці засоби КЗІ були розроблені і виготовлені відповідно до суттєвих вимог.

19. Виробники повинні скласти технічну документацію відповідно до пунктів 62 – 65 цього Технічного регламенту і провести оцінку відповідності засобів КЗІ за однією із процедур, передбачених пунктом 50 цього Технічного регламенту, або мати результати такої оцінки.

20. Якщо за результатами оцінки відповідності засобів КЗІ буде доведено їх повну відповідність вимогам цього Технічного регламенту, виробники повинні скласти декларацію про відповідність згідно з додатком 6 до цього

Технічного регламенту та нанести маркування знаком відповідності технічним регламентам.

21. Виробники повинні зберігати технічну документацію та декларацію про відповідність доки не мине потреба але не менше ніж 10 років після введення в обіг останньої одиниці засобів КЗІ.

22. Виробники для серійного виробництва засобів КЗІ повинні застосовувати процедури згідно з вимогами цього Технічного регламенту. Повинні враховуватися зміни в конструкції чи характеристиках засобів КЗІ та зміни в стандартах із переліку національних стандартів, зазначених у пункті 12 цього Технічного регламенту, або в інших технічних специфікаціях, шляхом посилання на які декларується відповідність засобів КЗІ вимогам цього Технічного регламенту.

23. Якщо зазначені засоби КЗІ становлять ризик, виробники з метою захисту інтересів споживачів (користувачів) повинні проводити випробування зразків засобів КЗІ, що надаються на ринку, досліджувати їх і за потреби вести реєстр скарг, невідповідних вимогам засобів КЗІ, відкликаних засобів КЗІ, а також інформувати розповсюджувачів про будь-який моніторинг.

24. Виробники повинні гарантувати, що засоби КЗІ, які вони надають на ринку, мають позначення характеристики засобу КЗІ, партії або серійного номера тощо, що дасть змогу його ідентифікувати, або у разі неможливості або невиправданості через характер засобів КЗІ зазначити це на пакуванні або супровідних документах.

25. Виробники повинні зазначити на засобах КЗІ назву своєї компанії, зареєстровану торгову назву або зареєстровану торгову марку та поштову адресу, за якою з ними можна зв'язатися. Якщо розмір або характер засобів КЗІ не дає змоги це зробити, вказати цю інформацію на упаковці засобів КЗІ або в супровідному документі. Зазначається лише одна адреса, за якою можна зв'язатися з виробником. Контактні дані наводяться відповідно до Закону України «Про забезпечення функціонування української мови як державної».

26. Виробники повинні забезпечити супроводження засобів КЗІ документами, визначеними додатком 5 до цього Технічного регламенту та оформленими відповідно до Закону України «Про забезпечення функціонування української мови як державної».

27. Виробники повинні забезпечити супроводження кожної одиниці засобів КЗІ копією декларації про відповідність або спрощеної декларації про відповідність. Спрощена декларація про відповідність, форма якої наведена в додатку 6 до цього Технічного регламенту, повинна містити точну інтернет-адресу, за якою можна отримати повний текст декларації про відповідність.

28. У разі наявності вимог щодо підтвердження сумісності засобів КЗІ із сервісами електронного урядування виробник зобов'язаний надавати у

товаросупровідній документації інформацію про сумісність засобів КЗІ відповідно до встановлених законодавством вимог.

Центральний орган виконавчої влади, що реалізує державну політику у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства встановлює вимоги до сумісності засобів КЗІ із сервісами електронного урядування.

29. Виробники, які вважають чи мають підстави вважати, що засоби КЗІ, які вони надали на ринку, не відповідають цьому Технічному регламенту, повинні негайно вжити коригувальних заходів, необхідних для приведення таких засобів КЗІ у відповідність з цим Технічним регламентом, а в разі потреби відкликати його або вилучити. Крім того, якщо засоби КЗІ становлять певний ризик, виробники повинні негайно поінформувати про це органи державного ринкового нагляду, надавши детальну інформацію, зокрема про невідповідність таких засобів КЗІ Технічному регламенту, про вжиті коригувальні заходи та про їх результати.

30. На обґрунтований запит органу державного ринкового нагляду виробники повинні надати йому всю інформацію та документацію (у паперовій або електронній формі), необхідну для демонстрації відповідності засобів КЗІ вимогам цього Технічного регламенту. На вимогу цього органу державного ринкового нагляду виробники повинні співпрацювати з ним щодо будь-яких заходів, які вживаються для усунення ризиків, що становить введений ними в обіг засіб КЗІ.

Уповноважені представники

31. Виробник у разі потреби на підставі письмового доручення (договір, довіреність тощо) визначає уповноваженого представника.

Обов'язки виробника, встановлені в пункті 18 цього Технічного регламенту, та обов'язки виробника щодо складення технічної документації, встановлені пункті 19 цього Технічного регламенту, не можуть бути предметом доручення для уповноваженого представника.

32. Уповноважений представник виконує завдання на підставі наданого доручення, яке повинно давати йому можливість щонайменше вчиняти такі дії:

зберігати декларацію про відповідність та технічну документацію і надавати їх на вимогу органів ринкового нагляду доки не мине потреба, але не менше ніж 10 років після введення в обіг останньої одиниці засобів КЗІ;

на обґрунтований запит органу державного ринкового нагляду надавати йому інформацію і документацію, необхідні для демонстрації відповідності засобів КЗІ вимогам цього Технічного регламенту;

на обґрунтований запит органу державного ринкового нагляду співпрацювати з ним та проводити будь-які заходи для усунення ризиків, які може створювати засіб КЗІ, на який поширюються повноваження уповноваженого представника.

Обов'язки імпортерів

33. Імпортери повинні вводити в обіг тільки такі засоби КЗІ, які відповідають вимогам цього Технічного регламенту.

34. Перед введенням засобів КЗІ в обіг імпортери повинні пересвідчитися, що:

виробник провів відповідну процедуру оцінки відповідності, визначену у пункті 50 цього Технічного регламенту;

виробник склав технічну документацію;

засоби КЗІ мають маркування знаком відповідності технічним регламентам і супроводжуються інформацією та документацією, зазначеними у пунктах 26 – 28 цього Технічного регламенту;

виробник виконав усі вимоги, наведені у пунктах 24 і 26 цього Технічного регламенту.

Якщо імпортер вважає або має підстави вважати, що засоби КЗІ не відповідають суттєвим вимогам, він не вводить засоби КЗІ в обіг, доки вони не будуть приведені у відповідність з такими вимогами. Крім того, якщо засоби КЗІ становлять ризик, імпортер повинен поінформувати про це виробника та органи державного ринкового нагляду.

35. Імпортери повинні зазначати на засобах КЗІ своє найменування, зареєстроване комерційне найменування чи зареєстровану торговельну марку (знак для товарів і послуг) та контактну поштову адресу, а у разі, коли нанесення відповідної інформації неможливе, то вона наноситься на пакуванні чи в документі, що супроводжує такі засоби КЗІ.

Контактні дані наводяться відповідно до закону про порядок застосування мов.

36. Імпортери повинні забезпечити, щоб засоби КЗІ супроводжувалися експлуатаційною документацією, викладеною згідно з вимогами Закону України «Про забезпечення функціонування української мови як державної».

37. Імпортери повинні забезпечити, щоб умови зберігання чи транспортування засобів КЗІ, доки вони перебувають під їх відповідальністю, не ставили під загрозу відповідність таких засобів КЗІ суттєвим вимогам.

38. Якщо зазначені засоби КЗІ становлять ризик, імпортери з метою захисту здоров'я і безпеки споживачів (користувачів) повинні проводити випробування зразків засобів КЗІ, що надаються на ринку, досліджувати їх і за потреби вести реєстр скарг, невідповідних вимогам засобів КЗІ, відкликаних засобів КЗІ, а також інформувати розповсюджувачів про будь-який такий моніторинг.

39. Імпортери, які вважають або мають підстави вважати, що засоби КЗІ, які вони ввели в обіг, не відповідають цьому Технічному регламенту, повинні негайно вжити коригувальних заходів для приведення засобів КЗІ у відповідність із зазначеними вимогами, а у разі потреби відкликати їх або вилучити. Крім того, якщо засоби КЗІ становлять ризик, імпортери повинні

негайно інформувати про це органи державного ринкового нагляду, надаючи пояснення стосовно невідповідності та будь-яких прийнятих коригувальних заходів.

40. Імпортери повинні доки не мине потреба, але не менше ніж 10 років після введення в обіг останньої одиниці засобів КЗІ зберігати копію декларації про відповідність для надання її на запит органів державного ринкового нагляду та забезпечити можливість надання таким органам за їх запитами доступу до технічної документації.

41. На обґрунтований запит органу державного ринкового нагляду імпортери повинні надати йому всю інформацію та документацію (у паперовій або електронній формі), необхідні для демонстрації відповідності засобів КЗІ вимогам цього Технічного регламенту. На вимогу цього органу державного ринкового нагляду імпортери повинні співпрацювати з ним щодо будь-яких заходів, які вживаються для усунення ризиків, що становить введений ними в обіг засіб КЗІ.

Обов'язки розповсюджувачів

42. Розповсюджувачі під час надання засобів КЗІ на ринку повинні діяти згідно з вимогами цього Технічного регламенту.

43. Перед наданням засобів КЗІ на ринку розповсюджувачі повинні перевірити, що засоби КЗІ мають маркування знаком відповідності технічним регламентам, супроводжуються документами, передбаченими цим Технічним регламентом, експлуатаційною документацією, які складені згідно з вимогами законодавства про порядок застосування мов, і що виробник та імпортер виконали вимоги, зазначені у пунктах 24 – 28 і 35 цього Технічного регламенту.

Якщо розповсюджувач вважає або має підстави вважати, що засоби КЗІ не відповідають суттєвим вимогам, він не повинен надавати засоби КЗІ на ринку до їх приведення у відповідність з такими вимогами.

Якщо зазначені засоби КЗІ становлять будь-який ризик, розповсюджувач повинен повідомити про це виробнику або імпортеру, а також органам державного ринкового нагляду.

44. Розповсюджувачі повинні забезпечити, щоб умови зберігання чи транспортування засобів КЗІ, доки вони перебувають під їх відповідальністю, не ставили під загрозу відповідність таких засобів КЗІ суттєвим вимогам.

45. Розповсюджувачі, які вважають або мають підстави вважати, що засоби КЗІ, які вони надали на ринку, не відповідають цьому Технічному регламенту, повинні переконатися, що вжиті коригувальні заходи, необхідні для приведення засобів КЗІ у відповідність із зазначеними вимогами, є достатніми, а у разі потреби – відкликати їх або вилучити. Крім того, якщо засоби КЗІ становлять ризик, розповсюджувачі повинні негайно інформувати про це органи ринкового нагляду та надати пояснення, зокрема інформацію про невідповідність і виконані коригувальні заходи.

46. На обґрунтований запит органу державного ринкового нагляду розповсюджувачі повинні надати йому інформацію та документацію (у паперовій або електронній формі), необхідні для демонстрації відповідності засобів КЗІ вимогам цього Технічного регламенту. На вимогу такого органу державного ринкового нагляду розповсюджувачі повинні співпрацювати з ним щодо будь-яких заходів, які вживаються для усунення ризиків, що становить засіб КЗІ, який вони надали на ринку.

Випадки, коли обов'язки виробників покладаються на імпортерів та розповсюджувачів

47. Імпортер або розповсюджувач повинен вважатися виробником для цілей цього Технічного регламенту і виконувати обов'язки виробника відповідно до вимог пунктів 18 – 30 цього Технічного регламенту у разі, коли може бути порушена відповідність засобів КЗІ вимогам цього Технічного регламенту, а саме, коли вони:

вводять в обіг засоби КЗІ під своїм найменуванням або торговою маркою (знаком для товарів і послуг);

вносять зміни до засобів КЗІ, які вже введено в обіг.

Ідентифікація суб'єктів господарювання

48. Суб'єкти господарювання повинні надавати органам державного ринкового нагляду за їх запитами інформацію, що дає змогу ідентифікувати:

будь-якого суб'єкта господарювання, який поставив їм засоби КЗІ;

будь-якого суб'єкта господарювання, якому вони поставили засоби КЗІ.

Суб'єкти господарювання повинні надавати зазначену в абзацах першому – третьому цього пункту інформацію протягом 10 років після того, як їм було поставлено засоби КЗІ, і протягом 10 років після того, як вони поставили засоби КЗІ.

Процедури оцінки відповідності

49. Виробник повинен провести оцінку відповідності засобів КЗІ з метою підтвердження відповідності суттєвим вимогам. Оцінка відповідності повинна враховувати усі передбачені умови експлуатації.

50. Виробник повинен продемонструвати відповідність засобів КЗІ суттєвим вимогам, визначеним у пунктах 7 – 12 цього Технічного регламенту, застосовуючи такі процедури оцінки відповідності:

1) для одиничного виробу – внутрішній контроль виробництва згідно з додатком 2;

2) для партії продукції – експертиза типу засобу КЗІ в поєднанні з відповідністю типові на основі внутрішнього контролю виробництва згідно з додатком 3 до цього Технічного регламенту;

3) для продукції, що виготовляється серійно, – відповідність на основі цілковитого забезпечення якості згідно з додатком 4 до цього Технічного регламенту.

Декларація про відповідність

51. У декларації про відповідність зазначається про те, що виконання суттєвих вимог було доведено.

52. Декларація про відповідність складається за структурою згідно з додатком 6 до цього Технічного регламенту.

Декларація про відповідність повинна містити елементи даних, наведені в додатку 6 до цього Технічного регламенту, і постійно оновлюватися.

Декларація про відповідність складається державною мовою, а у разі, коли вона була складена іншою мовою, – перекладається на державну мову.

Спрощена декларація про відповідність, зазначена у пункті 27 цього Технічного регламенту, повинна містити дані, наведені у додатку 7, і постійно оновлюватися. Повний текст декларації про відповідність державною мовою повинен бути доступний на вебсайті за адресою, зазначеною в спрощеній декларації про відповідність.

53. Якщо на засоби КЗІ поширюється дія кількох технічних регламентів, що вимагають складення декларації про відповідність, складається єдина декларація про відповідність щодо всіх таких технічних регламентів. У такій декларації про відповідність зазначаються відповідні технічні регламенти, у тому числі відомості про їх офіційне опублікування.

54. Єдина декларація про відповідність може мати форму досьє, яке складається з відповідних окремих декларацій про відповідність.

55. Виробник шляхом складання декларації бере на себе відповідальність за відповідність засобів КЗІ вимогам цього Технічного регламенту.

Загальні принципи маркування знаком відповідності технічним регламентам

56. Загальні принципи маркування знаком відповідності технічним регламентам наведені у статті 30 Закону України “Про технічні регламенти та оцінку відповідності”.

57. Ураховуючи конструкцію засобів КЗІ, висота знака відповідності технічним регламентам може бути менше як 5 міліметрів за умови, що він залишається видимим та розбірливим.

Правила та умови нанесення знака відповідності технічним регламентам та ідентифікаційного номера призначеного органу

58. Знак відповідності технічним регламентам повинен наноситися на засоби КЗІ таким чином, щоб він був видимий, розбірливий і незмивний, або, якщо це неможливо, на його інформаційну табличку з технічними даними. Знак відповідності також наноситься на упаковку і повинен бути помітним та розбірливим.

59. Знак відповідності технічним регламентам повинен наноситися перед введенням засобів КЗІ в обіг.

60. Маркування знаком відповідності технічним регламентам повинно супроводжуватися ідентифікаційним номером призначеного органу з оцінки відповідності (далі – призначений орган), якщо застосовувалася процедура оцінки відповідності, наведена у додатку 4 до цього Технічного регламенту.

Ідентифікаційний номер призначеного органу повинен мати таку саму висоту, що і знак відповідності. Ідентифікаційний номер призначеного органу повинен проставлятися самим призначеним органом або за його вказівкою виробником чи його уповноваженим представником.

61. Обмежувальні (коригувальні) заходи в разі неналежного застосування знака відповідності технічним регламентам вживаються відповідно до законодавства.

Технічна документація

62. Технічна документація повинна містити всі відповідні дані або відомості про засоби, що застосовуються виробником для забезпечення відповідності засобів КЗІ суттєвим вимогам. Зміст технічної документації наведено у додатку 5 до цього Технічного регламенту.

63. Технічна документація повинна складатися до введення засобів КЗІ в обіг і постійно оновлюватися.

64. Якщо технічна документація та кореспонденція, що стосуються будь-якої процедури експертизи типу, складені іншою мовою, ніж державна мова, на обґрунтований запит призначених органів суб'єкти господарювання зобов'язані за власний рахунок і у погоджений з такими органами строк забезпечити їх переклад на державну мову в необхідному обсязі. За згодою сторін технічна документація може надаватися мовою складення технічної документації.

65. Якщо технічна документація не відповідає пунктам 62 – 64 цього Технічного регламенту та не містить достатніх відповідних даних або засобів, які використовувалися для забезпечення відповідності засобів КЗІ суттєвим вимогам, орган державного ринкового нагляду у разі потреби звертається до виробника або імпортера з вимогою надати органу державного ринкового нагляду протягом певного періоду відповідні пояснення та матеріали з метою перевірки відповідності засобів КЗІ суттєвим вимогам.

Призначення органів з оцінки відповідності

66. Органи з оцінки відповідності для виконання ними як третіми сторонами завдань з оцінки відповідності згідно з цим Технічним регламентом призначається відповідно до Закону України «Про технічні регламенти та оцінку відповідності».

Вимоги до призначених органів

67. З метою призначення орган з оцінки відповідності повинен відповідати загальним вимогам до призначених органів відповідно до

статті 32 Закону України «Про технічні регламенти та оцінку відповідності» та спеціальним вимогам до призначених органів, установленим у пунктах 68 – 75 цього Технічного регламенту.

68. Орган з оцінки відповідності повинен бути третьою стороною, незалежною від організації або засобів КЗІ, які він оцінює.

Орган з оцінки відповідності, власником корпоративних прав якого є об'єднання підприємців, що представляє юридичних осіб та/або фізичних осіб - підприємців, які беруть участь у проєктуванні, виготовленні, постачанні, складанні, використанні чи обслуговуванні засобів КЗІ, які такий орган оцінює, може вважатися третьою стороною за умови доведення незалежності такого органу та відсутності будь-якого конфлікту інтересів.

69. Орган з оцінки відповідності, його керівництво і персонал, відповідальний за виконання завдань з оцінки відповідності:

не повинні бути проєктувальниками, виробниками, постачальниками, інсталяторами, покупцями, власниками, користувачами або наладниками засобу КЗІ, який вони оцінюють, а також не повинні бути представниками будь-якої із цих сторін. Це не виключає можливості використання засобу КЗІ, який пройшов оцінку відповідності і є необхідним для діяльності органу з оцінки відповідності, або використання такого засобу КЗІ в особистих цілях;

не повинні безпосередньо брати участь у проєктуванні, виробництві або створенні, маркетингу, налагоджуванні, експлуатації, або технічному обслуговуванні засобів КЗІ, або представляти сторони, залучені для такої діяльності. Вони не повинні брати участь у будь-якій діяльності, яка може вплинути на незалежність їх суджень або професійну чесність стосовно діяльності з оцінки відповідності, для виконання якої вони призначені. Особливо це стосується консультаційних послуг.

Органи з оцінки відповідності повинні забезпечувати дотримання дочірніми підприємствами або субпідрядниками, які ними залучаються до виконання робіт з оцінки відповідності, вимог щодо конфіденційності інформації, об'єктивності чи неупередженості під час діяльності з оцінки відповідності таких органів.

70. Органи з оцінки відповідності та їх персонал повинні провадити діяльність з оцінки відповідності з високим ступенем професіоналізму та необхідною технічною компетентністю в конкретній сфері, а також повинні бути вільні від будь-якого тиску і спонукань, зокрема фінансових, які можуть вплинути на їх рішення або результати їх діяльності з оцінки відповідності, особливо стосовно осіб або груп осіб, заінтересованих у результатах такої діяльності.

71. Орган з оцінки відповідності повинен бути здатний виконувати всі завдання з оцінки відповідності, зазначені у додатках 3 і 4 до цього Технічного регламенту, щодо яких він був призначений, незалежно від того, чи виконуються такі завдання самим органом з оцінки відповідності або від його імені і під його відповідальність.

Орган з оцінки відповідності в будь-який час і для кожної процедури оцінки відповідності та кожного виду засобів КЗІ, щодо яких він був призначений, повинен мати в своєму розпорядженні:

кваліфікований та досвідчений персонал для виконання завдань з оцінки відповідності;

описи процедур для кожного виду засобів КЗІ, відповідно до яких проводиться оцінка відповідності, із забезпеченням прозорості та здатності відтворення таких процедур. Орган з оцінки відповідності повинен мати відповідний порядок дій і процедур, які виконуються ним як призначеним органом, або під час інших видів діяльності;

процедури для провадження діяльності, які належним чином враховують розмір підприємства і сектору діяльності, а також структуру, ступінь технологічної складності засобів КЗІ, масовість або серійність процесу виробництва.

Орган з оцінки відповідності повинен мати кошти, необхідні для своєчасного та належного виконання технічних та адміністративних завдань, пов'язаних з діяльністю з оцінки відповідності.

72. Персонал, відповідальний за виконання завдань з оцінки відповідності, повинен мати:

технічну та професійну підготовку для провадження діяльності з оцінки відповідності, щодо якої орган з оцінки відповідності призначається чи був призначений;

знання вимог, що стосуються оцінок відповідності, які вони проводять, та відповідні повноваження для їх проведення;

знання та розуміння суттєвих вимог, визначених у пунктах 7 – 12 цього Технічного регламенту, порядок і сферу застосування стандартів із переліку національних стандартів, а також відповідних положень законодавства України щодо умов застосування, надання на ринку та введення в експлуатацію засобів КЗІ, які він оцінює;

здатність оформляти сертифікати експертизи типу засобу КЗІ та/або сертифікати на систему якості, записи та звіти, які підтверджують проведення оцінки відповідності.

73. Повинна бути забезпечена неупередженість органу з оцінки відповідності, його керівника, заступників керівника і персоналу, відповідального за виконання завдань з оцінки відповідності.

Оплата праці керівника, заступників керівника органу з оцінки відповідності та його персоналу, відповідального за виконання завдань з оцінки відповідності, не повинна залежати від кількості проведених оцінок відповідності чи їх результатів.

74. Персонал органу з оцінки відповідності повинен зберігати комерційну таємницю стосовно всієї інформації, одержаної під час виконання завдань згідно з додатками 3 і 4 до цього Технічного регламенту, за винятком її надання у визначених законодавством випадках відповідним уповноваженим органам, а

також захищати права власності суб'єктів господарювання на їх власну інформацію.

75. Органи з оцінки відповідності повинні брати участь у відповідній діяльності із стандартизації або забезпечувати поінформованість свого персоналу, відповідального за виконання завдань з оцінки відповідності, про таку діяльність.

Залучення призначеними органами субпідрядників та дочірніх підприємств

76. Якщо призначений орган залучає до виконання конкретних робіт, пов'язаних з оцінкою відповідності, субпідрядника або дочірнє підприємство, він повинен пересвідчитися у відповідності зазначеного субпідрядника чи дочірнього підприємства вимогам, визначеним у пунктах 67 – 75 цього Технічного регламенту, та повідомити про це орган, що призначає.

77. Призначені органи несуть повну відповідальність за роботи, що виконуються субпідрядниками або дочірніми підприємствами, незалежно від їх місцезнаходження.

78. Субпідрядник або дочірнє підприємство можуть бути залучені до виконання робіт з оцінки відповідності лише за згодою замовника.

79. Призначені органи повинні зберігати для надання на запити органу, що призначає, відповідні документи стосовно оцінювання кваліфікації залучених субпідрядників чи дочірніх підприємств і робіт, які вони виконали згідно з додатками 3 і 4 до цього Технічного регламенту.

Функціональні обов'язки призначених органів

80. Призначені органи повинні проводити оцінку відповідності згідно з процедурами оцінки відповідності, наведеними у додатках 3 і 4 до цього Технічного регламенту.

81. Оцінка відповідності проводиться без покладення зайвого навантаження на суб'єкта господарювання з урахуванням галузі, в якій діє такий суб'єкт господарювання, що замовляє роботи з оцінки відповідності, його характеристик, а саме структури, ступеня складності технології виробництва відповідного засобу КЗІ та масового чи серійного характеру виробничого процесу.

При цьому призначені органи дотримуються ступеня вимогливості та рівня захисту, що є необхідними для оцінювання відповідності засобів КЗІ вимогам цього Технічного регламенту.

82. Якщо призначений орган вважає, що суттєві вимоги або вимоги, наведені у відповідних стандартах з переліку національних стандартів чи технічних специфікаціях, не були дотримані виробником, зазначений орган повинен вимагати від виробника вжити відповідних коригувальних заходів і не видавати сертифікат експертизи типу засобу КЗІ або документ на оцінену систему якості.

83. Якщо під час проведення моніторингу виданих сертифікатів експертизи типу засобу КЗІ або оціненої системи якості призначений орган виявить, що засіб КЗІ більше не відповідає суттєвим вимогам, зазначений орган повинен вимагати від виробника вжити відповідних коригувальних заходів та у разі потреби призупинити дію або скасувати сертифікат експертизи типу засобу КЗІ або документ стосовно оціненої системи якості.

84. Якщо коригувальних заходів не було вжито або вони не призвели до необхідних результатів, призначений орган залежно від обставин повинен обмежити сферу, призупинити дію або скасувати сертифікат експертизи типу засобу КЗІ або документів стосовно оціненої системи якості.

Апеляції на рішення призначених органів

85. Подання та розгляд апеляцій на рішення призначених органів здійснюються відповідно до вимог статті 43 Закону України «Про технічні регламенти та оцінку відповідності».

Координація діяльності призначених органів

86. Відповідна координація та співпраця між органами з оцінки відповідності, призначеними згідно з цим Технічним регламентом, впроваджуються та належним чином функціонують у формі секторальної групи призначених органів.

Призначені органи беруть участь у роботі секторальної групи безпосередньо або через визначених представників.

Державний ринковий нагляд і державний контроль засобів КЗІ

87. Державний ринковий нагляд і державний контроль засобів КЗІ здійснюються відповідно до Закону України «Про державний ринковий нагляд і контроль нехарчової продукції» з урахуванням спеціальних вимог, визначених у пунктах 88 – 92 цього Технічного регламенту.

88. У разі виявлення невідповідності засобів КЗІ встановленим вимогам, орган ринкового нагляду невідкладно вимагає від відповідного суб'єкта господарювання вжити протягом визначеного строку заходів до приведення таких засобів КЗІ у відповідність із встановленими цим Технічним регламентом вимогами (крім випадків, формальної невідповідності) та у разі, якщо такі невідповідності можуть призвести до компрометації інформації, проводить перевірку характеристик засобу КЗІ з метою оцінки такого ризику. Відповідні суб'єкти господарювання повинні для цього співпрацювати з органами державного ринкового нагляду.

Якщо органом ринкового нагляду за результатами проведення перевірки характеристик засобу КЗІ встановлено, що засіб КЗІ становить серйозний ризик, орган державного ринкового нагляду відповідно до Методики вжиття обмежувальних (коригувальних) заходів, затвердженої постановою Кабінету Міністрів України від 26 грудня 2011 року № 1407, невідкладно вимагає від відповідного суб'єкта господарювання вилучити такий засіб КЗІ з обігу та/або

відкликати його чи заборонити надання такого засобу КЗІ на ринку. Суб'єкт господарювання має право надати органу державного ринкового нагляду свої пояснення відповідно до статті 33 Закону України «Про державний ринковий нагляд і контроль нехарчової продукції».

89. Суб'єкт господарювання повинен забезпечити проведення коригувальних заходів стосовно усіх засобів КЗІ, зазначених у пункті 88 цього Технічного регламенту, які надано ним на ринку.

90. У разі невідповідності засобів КЗІ встановленим вимогам органи державного ринкового нагляду повинні зазначити, чим обумовлена невідповідність:

невідповідністю засобів КЗІ суттєвим вимогам;

недоліками стандартів з переліку національних стандартів, зазначених у пункті 12 цього Технічного регламенту.

Формальна невідповідність засобів КЗІ

91. Додатково до застережень, зазначених у пунктах 88 – 90 цього Технічного регламенту, органи державного ринкового нагляду повинні вимагати від суб'єкта господарювання усунути такі формальні невідповідності:

1) знак відповідності технічним регламентам було нанесено з порушенням вимог, наведених у пунктах 56 – 61 цього Технічного регламенту;

2) знак відповідності технічним регламентам не було нанесено;

3) якщо застосовується процедура оцінки відповідності на основі цілковитого забезпечення якості згідно з додатком 4 до цього Технічного регламенту, ідентифікаційний номер призначеного органу застосовано з порушенням вимог, наведених у пункті 60 цього Технічного регламенту, або його не нанесено взагалі;

4) декларацію про відповідність не складено;

5) декларацію про відповідність складено невірно;

6) технічна документація недоступна або неукомплектована;

7) інформації, зазначеної у пунктах 24, 25 і 35 цього Технічного регламенту, немає, вона недостовірна або неповна;

8) інформація про можливе використання засобів КЗІ, декларація про відповідність або обмеження щодо використання, зазначені у пунктах 26 – 28 цього Технічного регламенту, не наведені у супровідних документах до засобів КЗІ;

9) вимоги до ідентифікації суб'єктів господарювання, наведені у пункті 48 цього Технічного регламенту, не виконано.

92. Якщо зберігається формальна невідповідність засобу КЗІ, зазначена у пункті 91 цього Технічного регламенту, органи державного ринкового нагляду повинні вжити усіх необхідних заходів до обмеження чи заборони надання відповідного засобу КЗІ на ринку або переконатися, що він вилучений або відкликаний з ринку.

Додаток 1
до Технічного регламенту засобів криптографічного захисту інформації
(пункт 8)

Загальні вимоги до рівнів безпеки засобів криптографічного захисту інформації

Для відповідності засобу КЗІ певному рівню безпеки повинні бути виконані організаційні, технічні та технологічні заходи в обсязі, вказаному у відповідній колонці таблиці № 1.

Заходи, розділені 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, схвалені функції безпеки, нормальні і погіршені режими роботи. Опис засобу КЗІ, у тому числі всіх компонентів АЗ, ПЗ і ВПЗ. Усі послуги надають інформацію про стан для зазначення, коли послуга використовує затверджений алгоритм шифрування, функції безпеки або процес відповідно до схваленої процедури			
2.	Інтерфейси засобу КЗІ	Обов'язкові й опційні інтерфейси. Специфікація всіх інтерфейсів і всіх шляхів передачі даних введення і виведення		Надійний канал	
3.	Ролі, послуги й автентифікація	Логічний поділ обов'язкових та необов'язкових функцій та послуг	Автентифікація оператора на основі ролей або особистості	Автентифікація оператора на основі особистості	Багатофакторна автентифікація
4.	Безпека ПЗ/ВПЗ	Схвалені методи забезпечення цілісності, визначені інтерфейсом засобу КЗІ. Код, придатний до виконання	Функція перевірки цілісності на основі цифрового підпису або коду автентифікації повідомлень	Тест на цілісність на основі схвалених цифрових підписів або для засобів КЗІ категорій «К», «З» та «Р» на основі автентифікації повідомлення	

№ з/п	Компонент	Рівень безпеки 1	Рівень безпеки 2	Рівень безпеки 3	Рівень безпеки 4
5.	Операційне середовище	Не модифікується, обмежене або придатне до модифікації. Контроль ЧПБ	Модифікується. Керування доступом на основі ролей або розподілу. Ведення аудиту подій		
6.	Фізична безпека	Промислові компоненти	Докази спроб злому. Непрозорий корпус засобу КЗІ або покриття	Виявлення та реагування на спроби злому корпусу засобу КЗІ (кришок, дверей тощо) та інформування про це. Сильний корпус або покриття. Захист від прямого зондування. Захист від відмов, що можуть бути спричинені впливом навколишнього середовища, або тестування на відмови, що можуть бути спричинені впливом навколишнього середовища	Всеохоплююче виявлення та реагування на спроби злому, спричинені впливом навколишнього середовища. Пом'якшення навмисної несправності
7.	Неінвазивна безпека	Модуль, призначений для пом'якшення наслідків від неінвазивних атак згідно з вимогами додатка F до ДСТУ ISO/IEC 19790			

№ з/п	Компонент		Рівень безпеки 1	Рівень безпеки 2	Рівень безпеки 3	Рівень безпеки 4
			Ведення документації та застосування методів пом'якшення наслідків згідно з вимогами додатка F до ДСТУ ISO/IEC 19790		Тестування пом'якшення наслідків	
8.	Управління чутливими параметрами безпеки		Генератори випадкових бітів; генерація, створення, введення, виведення, зберігання та знищення ЧПБ			
			Автоматизоване передавання або узгодження ЧПБ з використанням схвалених 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 процедури поділу даних	
9.	Самотестування		Перед початком експлуатації перевіряється цілісність ПЗ/ВПЗ, правильність роботи обхідної функції та критичних функцій			
			Виконуються умови: реалізовано криптографічний алгоритм, подвійну логіку, 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	
		Проєктування	Передбачено тестування всіх послуг, пов'язаних із безпекою			
		Модель кінцевих станів	Модель кінцевих станів			
		Опис	Анотовані вихідний код, схеми або мова	Мова опису програмного забезпечення високого рівня.		Документація, що має анотації попередніх

№ з/п	Компонент		Рівень безпеки 1	Рівень безпеки 2	Рівень безпеки 3	Рівень безпеки 4
			опису апаратних засобів	Мова опису апаратного забезпечення високого рівня		умов під час введення в компоненти модуля та очікуваних успішних післяумов для завершеного компонента
		Тестування	Функціональне тестування		Тестування на низькому рівні	
		Доставка та експлуатація	Ініціалізація процедур	Опис процедур доставки		Автентифікація оператора з використанням інформації автентифікації постачальника
		Настанова	Адміністративні та неадміністративні настанови			
11.	Пом'якшення атак		Специфікація пом'якшення наслідків атак, для яких не існує вимог щодо тестування			Специфікація пом'якшення наслідків атак з вимогами до перевірки

Додаток 2
до Технічного регламенту засобів
криптографічного захисту інформації
(пункт 50)

Модуль А
(внутрішній контроль виробництва)

1. Внутрішній контроль виробництва є процедурою оцінки відповідності, за допомогою якої виробник виконує обов'язки, визначені у пунктах 2 – 5 цього додатка, та гарантує і заявляє під свою виключну відповідальність, що засоби КЗІ відповідають вимогам Технічного регламенту засобів криптографічного захисту інформації (далі – Технічний регламент), які застосовуються до зазначених засобів КЗІ.

Технічна документація

2. Виробник складає технічну документацію згідно з пунктами 62 – 63 Технічного регламенту.

Виробництво

3. Виробник вживає всіх заходів, необхідних для того, щоб виробничий процес і його моніторинг забезпечували відповідність виготовлених засобів КЗІ технічній документації, зазначеній у пункті 2 цього додатка, та Суттєвим вимогам, визначеним у пунктах 7 – 12 Технічного регламенту.

Маркування знаком відповідності та декларація про відповідність

4. Виробник наносить знак відповідності згідно з пунктами 58 – 61, 63 Технічного регламенту на кожну окрему одиницю засобів КЗІ, що відповідає вимогам Технічного регламенту, які застосовуються до зазначених засобів КЗІ.

5. Виробник складає письмову декларацію про відповідність для кожного типу засобів КЗІ і зберігає її разом із технічною документацією для надання на запити органів державного ринкового нагляду доки не мине потреба, але не менше ніж 10 років після введення в обіг останньої одиниці засобів КЗІ. У декларації про відповідність зазначається інформація, яка дає змогу ідентифікувати засоби КЗІ, для яких її складено.

Копія декларації про відповідність подається відповідним органам державного ринкового нагляду на їх запити.

Уповноважений представник

6. Обов'язки виробника, визначені у пунктах 4 і 5 цього додатка, від його імені та під його відповідальність можуть бути виконані його уповноваженим представником за умови визначення цих обов'язків у документі, що засвідчує такі повноваження.

Додаток 3
до Технічного регламенту засобів
криптографічного захисту інформації
(пункт 50)

Модулі B і C
(експертиза типу в поєднанні з відповідністю типові на основі внутрішнього контролю виробництва)

Якщо є посилання на цей додаток, то процедура оцінки відповідності повинна виконуватися за модулями B (експертиза типу засобу КЗІ) і C (відповідність типові на основі внутрішнього контролю виробництва) цього додатка.

Модуль B
(експертиза типу)

1. Експертиза типу є частиною процедури оцінки відповідності, за якої призначений орган досліджує технічний проєкт засобів КЗІ, перевіряє і засвідчує, що технічний проєкт засобів КЗІ відповідає Суттєвим вимогам, визначеним у пунктах 7 – 12 Технічного регламенту засобів криптографічного захисту інформації (далі - Технічний регламент).

2. Експертиза типу виконується способом оцінки адекватності технічного проєкту засобів КЗІ шляхом експертизи технічної документації та підтвердних документів, зазначених у пункті 3 цього додатка, без дослідження зразка (моделі конструкції).

3. Виробник подає заявку на проведення експертизи типу засобу КЗІ лише одному призначеному органу за своїм вибором.

Заявка повинна містити:

найменування та адресу виробника, а у разі подання заявки уповноваженим представником – також його найменування та адресу;

письмову заяву про те, що така сама заявка не була подана жодному іншому призначеному органу;

технічну документацію, яка повинна давати можливість оцінити відповідність засобів КЗІ застосовним вимогам Технічного регламенту та містити опис проведення і результати належного аналізу та оцінки ризику (ризиків). У технічній документації повинні бути зазначені застосовні вимоги та охоплені (наскільки це стосується такої оцінки) питання проєктування, виробництва та функціонування засобів КЗІ. Технічна документація повинна в належних випадках містити елементи, наведені у додатку 5 до Технічного регламенту;

підтвердні документи щодо адекватності рішення технічного проєкту. Такі підтвердні документи повинні містити посилання на будь-які використані документи, особливо у разі, коли відповідні національні стандарти не були застосовані або були застосовані не повністю. Підтвердні документи повинні

містити за потреби результати випробувань, проведених згідно з іншими технічними специфікаціями відповідною лабораторією виробника або іншою випробувальною лабораторією від імені виробника та під його відповідальність.

4. Призначений орган проводить експертизу технічної документації та підтвердних документів для оцінки адекватності технічного проєкту засобів КЗІ.

5. Призначений орган складає звіт про оцінювання, в якому наводяться результати експертизи, виконаної згідно з пунктом 4 цього додатка. У межах своїх зобов'язань, визначених у пункті 8 цього додатка, призначений орган може оприлюднювати зміст зазначеного звіту в повному обсязі або частково лише за згодою виробника.

6. Якщо тип засобів КЗІ відповідає вимогам цього Технічного регламенту, призначений орган надає виробнику сертифікат експертизи типу засобу КЗІ. У такому сертифікаті зазначаються найменування та адреса виробника, висновки дослідження, особливості застосовних вимог, охоплених експертизою, умови чинності сертифіката (якщо такі є) та дані, необхідні для ідентифікації оціненого типу засобу КЗІ. До сертифіката експертизи типу засобу КЗІ можуть додаватися один чи більше додатків.

У сертифікаті експертизи типу засобу КЗІ та додатках до нього повинна міститися вся відповідна інформація, яка дає змогу оцінювати відповідність виготовленого засобу КЗІ дослідженому типу засобу КЗІ та здійснювати контроль під час експлуатації.

Якщо тип засобу КЗІ не відповідає застосовним вимогам цього Технічного регламенту, призначений орган відмовляє у видачі сертифіката експертизи типу засобу КЗІ та повідомляє про це заявнику з наданням докладного обґрунтування своєї відмови.

7. Призначений орган повинен постійно відслідковувати будь-які зміни в загальновизнаному сучасному стані розвитку інформаційних технологій, які свідчать про те, що затверджений тип засобу КЗІ може вже не відповідати застосовним вимогам Технічного регламенту, та повинен визначити, чи такі зміни потребують подальшого дослідження. Якщо зазначені зміни потребують подальшого дослідження, призначений орган повинен повідомити про це виробнику.

Виробник повинен інформувати призначений орган, який зберігає технічну документацію, що пов'язана із сертифікатом експертизи типу засобу КЗІ, про всі модифікації затвердженого типу засобу КЗІ, що можуть вплинути на відповідність засобу КЗІ Суттєвим вимогам Технічного регламенту або на умови чинності зазначеного сертифіката. Такі модифікації потребують додаткового дослідження типу засобу КЗІ та його затвердження у формі доповнення до первинного сертифіката експертизи типу засобу КЗІ.

Продовження додатка 3

8. Кожен призначений орган інформує орган, що призначає, про видані або скасовані ним сертифікати експертизи типу засобу КЗІ та/або про будь-які доповнення до них, а також періодично чи на запит органу, що призначає, надає йому список таких сертифікатів та/або будь-яких доповнень до них, у видачі яких він відмовив або дію яких зупинив чи встановив щодо них інші обмеження.

Кожен призначений орган інформує інші призначені органи про сертифікати експертизи типу засобу КЗІ та/або будь-які доповнення до них, у видачі яких він відмовив, або дію яких скасував, зупинив чи встановив інші обмеження, а на запит – також про видані ним сертифікати експертизи типу засобу КЗІ та/або доповнення до них.

Кожен призначений орган інформує Адміністрацію Держспецзв'язку щодо виданих сертифікатів експертизи типу засобу КЗІ та/або доповнень до них у разі, коли стандарти із переліку національних стандартів не застосовувалися або застосовувалися частково.

Орган, що призначає, відповідні органи державного ринкового нагляду та інші призначені органи мають право за запитами одержувати від призначеного органу копію сертифіката експертизи типу засобу КЗІ та/або доповнень до них.

Орган, що призначає, відповідні органи державного ринкового нагляду та Адміністрація Держспецзв'язку мають право за запитами одержувати копію технічної документації та результати досліджень, проведених призначеним органом.

Призначений орган зберігає копію сертифіката експертизи типу засобу КЗІ, додатків і доповнень до нього, протоколів випробувань, технічну інформацію згідно з пунктом 1 додатка 4 до Технічного регламенту доки не мине потреба, але не менше ніж 10 років після введення в обіг останньої одиниці засобів КЗІ.

9. Виробник зберігає копію сертифіката експертизи типу засобу КЗІ, додатків і доповнень до нього разом із технічною документацією для надання на запити органів державного ринкового нагляду доки не мине потреба, але не менше ніж 10 років після введення в обіг останньої одиниці засобу КЗІ.

10. Уповноважений представник виробника може подати заявку, зазначену у пункті 3 цього додатка, та виконати обов'язки, визначені в пунктах 7 і 9 цього додатка, за умови визначення таких обов'язків у документі, що засвідчує його повноваження.

Модуль С

(відповідність типу на основі внутрішнього контролю виробництва)

11. Відповідність типу засобу КЗІ на основі внутрішнього контролю виробництва є тією частиною процедури оцінки відповідності, за допомогою якої виробник виконує обов'язки, визначені в пунктах 12 – 14 цього додатка, та гарантує і заявляє, що засіб КЗІ відповідає типові засобу КЗІ, зазначеному в

сертифікаті експертизи типу, та вимогам цього Технічного регламенту, які застосовуються до цього засобу КЗІ.

Виробництво

12. Виробник вживає всіх заходів, необхідних для того, щоб виробничий процес і його моніторинг забезпечували відповідність виготовлених засобів КЗІ затвердженому типові засобу КЗІ, зазначеному у сертифікаті експертизи типу засобу КЗІ, та вимогам цього Технічного регламенту, які застосовуються до цих засобів КЗІ.

Маркування знаком відповідності та декларація про відповідність

13. Виробник наносить знак відповідності згідно з пунктами 56 – 59 Технічного регламенту на кожну одиницю засобу КЗІ, який відповідає затвердженому типові засобу КЗІ, зазначеному у сертифікаті експертизи типу засобу КЗІ, та застосовним вимогам Технічного регламенту.

14. Виробник складає письмову декларацію про відповідність для кожного типу засобу КЗІ і зберігає її разом з технічною документацією для надання на запити органів державного ринкового нагляду доки не мине потреба, але не менше ніж 10 років після введення в обіг останньої одиниці засобу КЗІ. Декларація про відповідність повинна містити інформацію щодо ідентифікації засобу КЗІ, для якого вона була складена.

Копія декларації про відповідність надається відповідним органам державного ринкового нагляду за їх запитами.

Уповноважений представник

15. Обов'язки виробника, визначені у пунктах 13 і 14 цього додатка, від його імені та під його відповідальність можуть бути виконані його уповноваженим представником за умови визначення цих обов'язків у документі, що засвідчує такі повноваження.

Додаток 4
до Технічного регламенту засобів
криптографічного захисту інформації
(пункт 50)

Модуль Н
(відповідність на основі цілковитого забезпечення якості)

1. Відповідність на основі цілковитого забезпечення якості є процедурою оцінки відповідності, за допомогою якої виробник виконує обов'язки, визначені у пунктах 2, 12 і 13 цього додатка, та гарантує і заявляє під свою виключну відповідальність, що засоби криптографічного захисту інформації відповідають Суттєвим вимогам, визначеним у пунктах 7 – 12 Технічного регламенту засобів криптографічного захисту інформації (далі – Технічний регламент), які до нього застосовуються.

Виробництво

2. Виробник забезпечує функціонування схваленої призначеним органом відповідно до пункту 3 цього додатка системи управління якістю для проєктування, виробництва, контролю та проведення випробувань виготовлених засобів КЗІ і підлягає нагляду відповідно до пунктів 8 – 11 цього додатка.

Система управління якістю

3. Виробник подає обраному ним органу заявку на проведення оцінки своєї системи управління якістю щодо відповідності засобу КЗІ.

Заявка повинна містити:

найменування та адресу виробника, а у разі подання заявки уповноваженим представником – також його найменування та адресу;

технічну документацію для кожного типу засобів КЗІ. Технічна документація повинна в належних випадках містити елементи, наведені у додатку 5 до Технічного регламенту;

документацію стосовно системи управління якістю;

письмову заяву про те, що така сама заявка не була подана жодному іншому призначеному органу.

4. Упроваджена система управління якістю повинна забезпечувати відповідність засобів КЗІ застосовним до нього вимогам Технічного регламенту.

Усі прийняті виробником елементи, вимоги та положення системи управління якістю повинні бути задокументовані систематичним і упорядкованим чином у вигляді політик, процедур та інструкцій, викладених у письмовій формі. Документація щодо системи управління якістю повинна давати можливість однозначного тлумачення програм, планів, настанов і протоколів (записів) щодо якості.

Зазначена документація повинна містити належний опис:

цілей у сфері якості та організаційної структури, обов'язків і повноважень керівництва виробника щодо забезпечення якості проєктування та засобів КЗІ;

технічних специфікацій на проєктування, у тому числі стандартів, що будуть застосовуватися, а у разі, коли відповідні стандарти з переліку національних стандартів застосовані частково, – опис заходів, що будуть використані з метою забезпечення відповідності засобів КЗІ застосованим до нього вимогам Технічного регламенту;

методів контролю та перевірки проєкту, процесів і системних заходів, які будуть застосовуватися під час проєктування засобів КЗІ, що належать до відповідного типу засобів КЗІ;

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

досліджень і випробувань, які будуть проводитися до, під час і після виготовлення засобів КЗІ, із зазначенням періодичності їх проведення;

протоколів (записів) щодо якості (звітів про інспектування, даних випробувань і калібрувань, звітів про кваліфікацію відповідного персоналу тощо);

засобів моніторингу, які дають змогу контролювати досягнення необхідної якості проєктування і засобів КЗІ та ефективне функціонування системи управління якістю.

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

Призначений орган повинен на основі презумпції відповідності робити припущення про відповідність вимогам, зазначеним у пункті 4 цього додатка, тих елементів системи управління якістю, які відповідають відповідним вимогам національного стандарту, що є ідентичним відповідному гармонізованому європейському стандарту.

Група аудиту, визначена призначеним органом, повинна володіти досвідом оцінювання у сфері систем управління якістю та мати у своєму складі принаймні одного члена з досвідом роботи експертом з оцінки відповідності засобів КЗІ та технології його виробництва, а також зі знанням застосовних вимог Технічного регламенту.

Оцінка системи управління якістю повинна передбачати відвідування підприємства - виробника.

Група аудиту вивчає технічну документацію, зазначену в абзаці четвертому пункту 3 цього додатка, з метою перевірки здатності виробника ідентифікувати застосовні вимоги цього Технічного регламенту і проводити необхідні дослідження для забезпечення відповідності засобів КЗІ цим вимогам.

Призначений орган повідомляє виробнику або його уповноваженому представнику про прийняте рішення.

Продовження додатка 4

Зазначене повідомлення повинно містити висновки аудиту та обґрунтоване рішення щодо оцінки.

6. Виробник повинен виконувати обов'язки, пов'язані із забезпеченням функціонування схваленої системи управління якістю, та підтримувати її в адекватному та ефективному стані.

7. Виробник зобов'язаний інформувати призначений орган, який схвалив систему управління якістю, про будь-які заплановані зміни в такій системі.

Призначений орган оцінює будь-які запропоновані зміни і приймає рішення щодо здатності зміненої системи управління якістю надалі відповідати вимогам, зазначеним у пункті 4 цього додатка, чи необхідності проведення повторної оцінки.

Призначений орган повідомляє виробнику про прийняте рішення. Зазначене повідомлення повинно містити висновки дослідження та обґрунтоване рішення щодо оцінки.

Нагляд за відповідальністю призначеного органу

8. Мета нагляду полягає в тому, щоб пересвідчитися в належному виконанні виробником обов'язків, пов'язаних із забезпеченням функціонування схваленої системи управління якістю.

9. Для цілей нагляду виробник зобов'язаний надавати призначеному органу доступ до місць проєктування, виробництва, контролю, проведення випробувань і зберігання засобів КЗІ, а також усю необхідну інформацію, зокрема:

документацію щодо системи управління якістю;

протоколи (записи) щодо якості, передбачені тією частиною системи управління якістю, яка стосується проєктування (результати аналізу, розрахунків, випробувань тощо);

протоколи (записи) щодо якості, передбачені тією частиною системи якості, яка стосується виробництва (звіти про інспектування, дані випробувань і калібрувань, звіти про кваліфікацію відповідного персоналу тощо).

10. Призначений орган повинен проводити періодичні аудити, щоб пересвідчитися в тому, що виробник застосовує та підтримує в належному стані схвалену систему управління якістю, та надавати виробнику звіт про аудит.

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

Продовження додатка 4

Маркування знаком відповідності та декларація про відповідність

12. Виробник наносить знак відповідності згідно з пунктами 70 – 73 Технічного регламенту та ідентифікаційний номер призначеного органу, зазначеного в пункті 3 цього додатка, на кожну одиницю засобів КЗІ, що відповідає застосовним вимогам Технічного регламенту.

13. Виробник складає письмову декларацію про відповідність для кожного типу засобів КЗІ і зберігає її разом із технічною документацією для надання на запити органів державного ринкового нагляду доки не мине потреба, але не менше ніж 10 років після введення в обіг останньої одиниці засобів КЗІ. Декларація про відповідність повинна містити інформацію щодо ідентифікації засобів КЗІ, для якого вона була складена.

Копія декларації про відповідність надається відповідним органам державного ринкового нагляду за їх запитами.

14. Виробник повинен протягом 10 років після введення в обіг останньої одиниці засобів КЗІ зберігати та надавати державним органам на їх запити:

технічну документацію, зазначену в абзаці четвертому пункту 3 цього додатка;

документацію стосовно системи управління якістю, зазначену в абзаці п'ятому пункту 3 цього додатка;

затверджені виробником зміни до системи управління якістю, зазначені у пункті 7 цього додатка (за наявності таких змін);

рішення, звіти та протоколи призначеного органу, зазначені у пунктах 7, 10 і 11 цього додатка.

15. Кожний призначений орган повинен інформувати орган, що призначає, про видані або скасовані ним документи щодо систем управління якістю, а також періодично чи на запит надавати йому перелік відмов у видачі документа щодо схвалення системи, а також документів щодо схвалених систем управління якістю, дію яких він зупинив чи встановив щодо них інші обмеження.

Кожний призначений орган інформує інші призначені органи про відмови у схваленні систем якості, зупинення, скасування або встановлення щодо них інших обмежень, а на запит – також про схвалені системи якості.

Уповноважений представник

16. Обов'язки виробника, зазначені у пунктах 3, 7, 12 – 14 цього додатка, від його імені та під його відповідальність можуть бути виконані його уповноваженим представником за умови визначення цих обов'язків у документі, що засвідчує такі повноваження.

Додаток 5
до Технічного регламенту засобів
криптографічного захисту інформації
(пункт 62)

ЗМІСТ
технічної документації

1. Технічна документація повинна містити щонайменше такі елементи:

1) специфікація типу засобу КЗІ (обладнання, ПЗ, ВПЗ, гібридне ПЗ або ВПЗ гібридного засобу);

2) специфікація криптографічної межі засобу КЗІ;

3) специфікація обладнання, ПЗ і компонентів ВПЗ засобу КЗІ й опис фізичної конфігурації засобу КЗІ;

4) специфікація обладнання, ПЗ або компонентів ВПЗ засобу КЗІ, які вилучено з вимог безпеки ДСТУ ISO\IEC 19790:2015, і обґрунтування для вилучення;

5) специфікація фізичних портів і логічних інтерфейсів засобу КЗІ;

6) специфікація ручних або логічних елементів управління засобу КЗІ, фізичних або логічних індикаторів стану й відповідних фізичних, логічних і електричних характеристик;

7) специфікація всіх функцій безпеки, реалізованих у засобі КЗІ, і специфікації всіх режимів роботи;

8) блок-схема, що зображає всі основні апаратні компоненти засобу КЗІ і їх взаємозв'язки, у тому числі мікропроцесори, буфери введення/виведення, буфери відкритих/зашифрованих даних, буфери управління, сховище ключів, робочу пам'ять і пам'ять програм;

9) специфікація конструкції апаратного забезпечення, ПЗ та ВПЗ засобу КЗІ;

10) специфікація всієї пов'язаної з безпекою інформації, у тому числі секретних і особистих криптографічних ключів (відкритих та зашифрованих), дані аутентифікації, ППБ, ППБ та іншої захищеної інформації, розкриття або модифікація якої може скомпрометувати безпеку засобу КЗІ;

11) специфікація деградованого режиму засобу КЗІ;

12) специфікація політики безпеки засобу КЗІ, зокрема правила, вилучені з вимог цього стандарту і з будь-яких додаткових вимог постачальника;

13) специфікація введення даних, виведення даних, введення керування, виведення керування, виведення стану та інтерфейсів живлення (фізичних і логічних), інтерфейсу надійного каналу (застосовується для засобів КЗІ рівнів безпеки 3 та 4);

14) специфікація винятків (помилок) і обґрунтування, якщо інтерфейс виведення керування не вимикається у помилковому стані;

15) специфікація усіх авторизованих ролей, які підтримуються засобом КЗІ;

16) специфікація послуг, операцій або функцій, що надаються засобом КЗІ для кожної послуги, специфікації її введення, відповідного виведення та авторизованих користувачів, які можуть його використовувати;

17) специфікація послуг засобу КЗІ, для яких оператор може не мати авторизованої ролі, і як ці послуги не змінюють, не розкривають або не замінюють криптографічних ключів та інших ЧПБ, або іншим чином впливають на безпеку засобу КЗІ;

18) специфікація механізмів автентифікації, які підтримуються засобом КЗІ, типи даних автентифікації, що потрібні для реалізації механізмів автентифікації, методи авторизації, які використовуються для управління першим доступом до засобу й ініціалізації механізмів автентифікації, стійкість механізмів автентифікації, які підтримуються засобом КЗІ, у тому числі обґрунтування підтримки кількох механізмів автентифікації;

19) специфікація послуг засобу КЗІ, які зазначають інформацію про версії засобу, відображають його стан, виконують самотестування, виконують схвалені функції безпеки і виконують анулювання;

20) специфікація механізмів обходу;

21) специфікація механізмів завантаження ПЗ або ВПЗ;

22) специфікація управління й інтерфейсів можливості самостійного виведення даних засобом КЗІ;

23) специфікація схвалених методик забезпечення цілісності;

24) специфікація дій оператора для виконання на вимогу схваленої методики перевірки цілісності;

25) специфікація вигляду коду, придатного до виконання;

26) специфікація операційного середовища засобу КЗІ, включаючи там де це доцільно операційну систему, яка використовується засобом КЗІ (застосовується для засобів КЗІ рівнів безпеки 1 та 2);

27) специфікація правил безпеки, налаштувань або обмежень конфігурації операційного середовища (застосовується для засобів КЗІ рівнів безпеки 1 та 2);

28) настанова адміністратора для налаштування операційної системи відповідно до вимог специфікації (застосовується для засобів КЗІ рівня безпеки 2);

29) специфікація фізичного втілення і рівень безпеки реалізованого фізичного механізму безпеки засобів КЗІ;

30) специфікація фізичних механізмів безпеки, які використовує засіб КЗІ;

31) специфікація інтерфейсу доступу для обслуговування і механізм анулювання КПБ або використання інтерфейсу доступу для обслуговування (якщо засіб КЗІ виконує роль технічного обслуговування, що потребує фізичного доступу до вмісту засобу, або якщо засіб призначено для забезпечення фізичного доступу);

32) специфікація нормальних робочих діапазонів засобу КЗІ, функцій захисту від відмов середовища або тестів на відому середовища (застосовується для засобів КЗІ рівня безпеки 4);

33) специфікація методів послаблення відмов, які використовуються (застосовується для засобів КЗІ рівня безпеки 4);

34) специфікація методів послаблення, які використовуються для протидії неінвазивним атакам, зокрема визначеним в додатку F до ДСТУ ISO\IEC 19790:2015;

35) специфікація всіх КПБ і ППБ, які використовує засіб КЗІ;

36) специфікація всіх ГВБ і їх використання;

37) специфікація мінімальної ентропії, якої потребує засіб КЗІ для кожного вхідного параметра;

38) специфікація кожного ГВБ (схваленого і несхваленого, а також джерела ентропії), які використовує засіб КЗІ;

39) специфікація мінімальної ентропії і способу генерації заявленої мінімальної ентропії, якщо ентропію отримують всередині криптографічної межі засобу КЗІ;

40) специфікація кожного методу генерації ЧПБ, який використовує ГВБ;

41) специфікація всіх методів створення ЧПБ, які використовує засіб КЗІ;

42) специфікація кожного методу ЧПБ покоління, використовуваного засобом КЗІ;

43) специфікація кожного з методів генерації ключів (схвалених і несхвалених), які використовує засіб КЗІ;

44) специфікація методів створення ЧПБ, що використовуються у засобі КЗІ;

45) специфікація методів введення і виведення ЧПБ, що використовуються у засобі КЗІ;

46) специфікація основних методів введення і виведення, що використовуються у засобі КЗІ;

47) довідка про виконання умови: якщо знання n компонента потрібно для відновлення КПБ, то n – 1 компонент не дає інформації про КПБ, крім його довжини (застосовується для засобів КЗІ рівнів безпеки 3 та 4, якщо ними використовуються процедури розподілу знань);

48) специфікація процедур розподілу знань, що використовуються у засобів КЗІ (застосовується для засобів КЗІ рівнів безпеки 3 та 4);

49) специфікація ЧПБ, які зберігаються в засобі КЗІ;

50) специфікація захищеності КПБ від неавторизованого доступу, використання, розголошення, зміни і заміни під час зберігання в засобі КЗІ;

51) специфікація захищеності ППБ від неавторизованої модифікації і заміни під час зберігання в засобі КЗІ;

52) специфікація взаємозв'язків ППБ, які зберігають у засобі КЗІ, з оператором, роллю або процесом, для яких призначено цей параметр;

53) специфікація методу(ів) анулювання, які використовує засіб КЗІ, і обґрунтування того, як метод(и) запобігає вилученню та повторному використанню анульованих значень;

54) специфікація самотестування, яке виконує засіб КЗІ, зокрема передопераційні й умовні тести;

55) специфікація індикаторів задовільних і незадовільних результатів самотестування;

56) специфікація помилкового стану засобу КЗІ, в який він може увійти у разі незадовільного самотестування, а також умови й дії, необхідні для виходу з помилкового стану і відновлення нормальної роботи засобу КЗІ;

57) специфікація всіх функцій безпеки, важливих для безпечної експлуатації криптографічного засобу та ідентифікації тестів, які виконуються під час увімкнення живлення й умовних тестів, які виконує засіб КЗІ;

58) специфікація механізму або логіки, що регулює процедуру перемикання (якщо засіб КЗІ реалізує можливість обходу);

59) специфікація системи управління конфігурацією, яка використовується для засобу КЗІ;

60) специфікація документів, які підтримують розробку засобу КЗІ і пов'язаних із ним документів, що надає система управління конфігурацією;

61) специфікація процедур безпечної інсталяції, генерації й запуску засобу КЗІ;

62) специфікація процедур підтримки безпеки під час постачання і доставки версій засобу КЗІ авторизованим оператором;

63) специфікація відповідності між архітектурою АЗ, ПЗ та/або компонентами ВПЗ засобу КЗІ і політикою безпеки засобу КЗІ та моделлю кінцевих станів);

64) специфікації початкового коду ПЗ, анотованого коментарями, які чітко відображають відповідність ПЗ архітектурі засобу КЗІ (застосовується, якщо засіб КЗІ містить ПЗ);

65) специфікація схеми та/або HDL апаратних засобів КЗІ (застосовується, якщо засіб КЗІ містить апаратні засоби);

66) специфікація функціональної специфікації, яка неформально описує засіб КЗІ, функціональність засобу КЗІ, зовнішні фізичні порти і логічні інтерфейси засобу КЗІ, а також мету побудови фізичних портів і логічних інтерфейсів (застосовується для засобів КЗІ рівнів безпеки 2, 3 та 4);

67) специфікація детального проєктування, яка описує внутрішні функції основних компонентів засобу КЗІ, внутрішні інтерфейси компонентів, мету побудови інтерфейсів компонентів і внутрішній потік інформації (в цілому в межах криптографічного кордону, а також в рамках основних компонентів) (застосовується для засобів КЗІ рівнів безпеки 3 та 4);

68) специфікація (у тому числі передумов і післяумов) відповідності між архітектурою засобу КЗІ і функціональною специфікацією (застосовується для засобів КЗІ рівня безпеки 4);

69) специфікація моделі кінцевих станів (або еквівалент) із допомогою діаграми станів і таблиці станів, які охоплюють: операційні і помилкові стани криптографічного засобу; відповідні переходи з одного стану в інший; вхідні події, у тому числі вхідні дані і вхідні контролі, які призводять до переходу з одного стану в інший; вихідні події, у тому числі внутрішні умови засобу, вихідні дані й вихідні стани, які виникають в результаті переходу з одного стану в інший;

70) специфікація початкового коду ПЗ або ВПЗ;

71) анотації для початкових кодів кожного програмного або апаратного компонента криптографічного засобу КЗІ, які визначають: передумови, необхідні параметри компонентів, функції та процедури засобу для коректного виконання; очікувані успішні післяумови завершення виконання кожного компонента, функції і процедури засобу (застосовується для засобів КЗІ рівня безпеки 4);

72) специфікації для настанови адміністратора, що містять: функції адміністратора, події безпеки, параметри безпеки (значення параметрів, якщо потрібно), фізичні порти й логічні інтерфейси засобу КЗІ, доступні для адміністративних ролей; безпечні процедури адміністрування криптографічного засобу; припущення про поведінку користувача, релевантні до безпечної експлуатації засобу КЗІ;

73) специфікації для неадміністративних настанов, що містять: затверджені функції безпеки, фізичні порти і логічні інтерфейси, доступні для користувачів засобу КЗІ; всі обов'язки користувача, потрібні для безпечної експлуатації засобу;

74) опис механізмів безпеки, які використовує засіб КЗІ для послаблення атак (застосовується для засобів КЗІ рівня безпеки 1, 2, та 3, призначених для послаблення однієї або більше конкретних атак, які не визначені ДСТУ ISO\IEC 19790:2015);

75) опис методів, які використовуються для послаблення атак, і методи тестування ефективності методів послаблення атак (застосовується для засобів КЗІ рівня безпеки 4, призначених для послаблення однієї або більше атак, які не визначені ДСТУ ISO\IEC 19790:2015);

76) політика безпеки засобу КЗІ згідно з вимогами пункту 13 Технічного регламенту;

77) список стандартів із переліку національних стандартів, які є ідентичними гармонізованим європейським стандартам і відповідність яким надає презумпцію відповідності засобів КЗІ Суттєвим вимогам, а також застосовуються, повністю або частково, а у разі, коли такі стандарти не застосовувалися, – опис рішень, прийнятих з метою забезпечення відповідності Суттєвим вимогам Технічного регламенту засобів криптографічного захисту інформації (далі – Технічний регламент), у тому числі перелік інших застосованих технічних специфікацій. У разі часткового застосування зазначених стандартів у технічній документації повинні бути наведені ті частини стандартів, які були застосовані;

78) копія декларації про відповідність;

79) якщо оцінка відповідності проводилася із застосуванням модуля, наведеного в додатку 2 до Технічного регламенту, – копія сертифіката експертизи типу та додатки до нього, які було видано призначеним органом;

80) результати проєктних розрахунків, проведених перевірок та інша подібна інформація;

81) протоколи випробувань;

82) пояснення згідно з вимогами пункту 15 Технічного регламенту та пояснення щодо наведення чи ненаведення інформації на упаковці відповідно до пункту 24 Технічного регламенту.

2. Елементи технічної документації, зазначені в абзаці четвертому підпункту 1, у підпунктах 76, 77, 78, 79 і 82 пункту 1 цього додатка, оформляються відповідно до Закону України «Про забезпечення функціонування української мови як державної».

Додаток 6
до Технічного регламенту засобів
криптографічного захисту інформації
(пункт 52)

ДЕКЛАРАЦІЯ ПРО ВІДПОВІДНІСТЬ (№ XXX)*

1. Засіб криптографічного захисту інформації (виріб, тип, номер партії чи серійний номер)

_____

_____

2. Найменування та адреса виробника або його уповноваженого представника

_____

_____

3. Цю декларацію відповідності видано під особисту відповідальність виробника.

4. Об'єкт декларації (ідентифікація засобу КЗІ, яка дає змогу забезпечити його простежуваність; може містити кольорове чітке зображення у разі потреби для ідентифікації зазначеного засобу КЗІ)

_____

_____

5. Об'єкт декларації відповідає вимогам таких технічних регламентів:
Технічного регламенту засобів КЗІ;
іншого технічного регламенту (за потреби).

6. Посилання на відповідні стандарти з переліку національних стандартів, що були застосовані, або посилання на інші технічні специфікації, щодо яких декларується відповідність (із зазначенням ідентифікаційного номера, версії та дати видання)

_____

_____

7. Призначений орган з оцінки відповідності

_____

_____

(найменування, ідентифікаційний номер згідно з реєстром призначених органів)

виконав

_____

(опис виконаних ним дій)

та видав сертифікат експертизи типу засобу криптографічного захисту інформації № _____ від ___ _____ 20__ р.

(у разі залучення призначеного органу з оцінки відповідності).

Продовження додатка 6

8. У відповідних випадках опис компонентів та обладнання, у тому числі програмного забезпечення, завдяки якому засіб криптографічного захисту інформації функціонує за призначенням і на яке поширюється дія декларації про відповідність.

9. Додаткова інформація

Підписано від імені та за дорученням

(_____ 20__ р.) (місце та дата видачі)

_____ _____

(ім'я прізвище, посада) (підпис)

*Присвоєння виробником номера декларації про відповідність є необов'язковим.

Додаток 7
до Технічного регламенту засобів
криптографічного захисту інформації
(пункт 52)

СПРОЩЕНА ДЕКЛАРАЦІЯ
про відповідність

Спрощена декларація про відповідність, зазначена в пункті 27 Технічного регламенту засобів криптографічного захисту інформації, повинна бути представлена таким чином:

(найменування виробника) заявляє, що тип засобів криптографічного захисту інформації (позначення типу засобів криптографічного захисту інформації) відповідає Технічному регламенту засобів криптографічного захисту інформації;

повний текст декларації про відповідність доступний на вебсайті за такою адресою:_____