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

23.04.18 № 04/02/03-7294

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

*Щодо погодження проекту постанови КМУ*

Направляємо на погодження розроблений Адміністрацією Державної служби спеціального зв'язку та захисту інформації України проект постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації».

Просимо погодити зазначений проект згідно положень статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Додатки: 1. Проект постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації», № 04/02/03-1288 від 23.04.2018, прим. № 3 на 121 арк.;

2. Аналіз регуляторного впливу до проекту постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації», № 04/02/03-1292 від 23.04.2018, прим. № 2 на 13 арк.;

3. Повідомлення про оприлюднення проекту нормативно-правового акта, № 04/02/03-1290 від 23.04.2018, прим. № 3 на 2 арк.;

4. Порівняльна таблиця до проекту постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації», № 04/02/03-1291 від 23.04.2018, прим. № 3 на 2 арк.

Перший заступник Голови Служби О.М. Чаузов

Вик. Сметович О.Б.
т. 281-92-36

Державна регуляторна служба України
№ 6185/0/19-18 від 25.04.2018

пр. 3

ПРОЕКТ

**КАБІНЕТ МІНІСТРІВ УКРАЇНИ**
**ПОСТАНОВА**

**від 2018 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 затвердженого цією постановою Технічного регламенту.

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

4. Ця постанова набирає чинності через шість місяців з дня її опублікування.

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

*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 засобів криптографічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом (далі – засоби криптографічного захисту інформації або засоби КЗІ або продукція), оцінки їх відповідності та обігу на ринку України.

2. Технічний регламент засновано на національному стандарті України ДСТУ ISO/IEC 19790:2015 «Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів», прийнятому наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (далі - ДСТУ ISO/IEC 19790).

3. Вимоги щодо засобів КЗІ з обмеженим доступом у державній сфері, оцінки їх відповідності та їх обігу охоплюють положення цього Технічного регламенту, але не ототожнюються з ним. Особливості побудови засобів КЗІ визначаються нормативно-правовими актами спеціально уповноваженого органу у сфері спеціального зв'язку та захисту інформації.

4. В цілях виконання вимог цього Технічного регламенту, під час тлумачення положень міжнародних та європейських стандартів, які мають вітчизняний гармонізований аналог, перевага віддається мові оригіналу.

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

вилучення з обігу - будь-який захід, спрямований на запобігання наданню на ринку продукції, що знаходиться в ланцюгу постачання продукції;

виробник - будь-яка фізична чи юридична особа (резидент чи нерезидент України), яка виготовляє продукцію або доручає її розроблення чи виготовлення та реалізує цю продукцію під своїм найменуванням або торговельною маркою або використовує таку продукцію для власних цілей;

відкликання - будь-який захід, спрямований на забезпечення повернення продукції, яка вже була надана споживачу (користувачу);

гармонізований європейський стандарт - стандарт, який прийнятий однією з європейських організацій стандартизації на основі запиту, зробленого Європейською Комісією, та номер і назву якого опубліковано в Офіційному віснику Європейського Союзу;

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

криптографічна продукція (далі - продукція) – програмні, апаратні та апаратно-програмні засоби та обладнання, що розроблені та призначені виключно для забезпечення криптографічного захисту інформації. Вимоги цього регламенту не поширюються на продукцію, що призначена для виконання функцій охоронних систем загального користування, для захисту контенту від неправомірного його використання в мережних засобах масової інформації, або в мережах кабельного і супутникового радіо та телебачення, а також для захисту технологічної інформації в системах управління технологіями виробництва від її несанкціонованої модифікації;

надання на ринку - будь-яке платне або безоплатне постачання продукції для розповсюдження, споживання чи використання на ринку України в процесі провадження господарської діяльності;

орган з оцінки відповідності - орган, що провадить діяльність з оцінки відповідності, зокрема, випробування, сертифікацію, інспектування та калібрування;

оцінка відповідності - процес доведення того, що суттєві вимоги цього Технічного регламенту, які стосуються продукції, були виконані;

розповсюджувач - будь-яка інша, ніж виробник або імпортер, фізична чи юридична особа в ланцюгу постачання продукції, яка надає продукцію на ринку України;

технічна специфікація - документ, що встановлює технічні вимоги, яким повинна відповідати продукція;

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

Інші терміни вживаються у значенні, наведеному в Законах України «Про технічні регламенти та оцінку відповідності», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про основні засади забезпечення кібербезпеки в Україні», «Про державний ринковий нагляд і контроль нехарчової продукції», а також у додатку 1 цього Технічного регламенту.

**Надання на ринку та введення в експлуатацію продукції**

6. Продукція може бути надана на ринку та введена в експлуатацію тільки в разі, коли вона відповідає вимогам цього Технічного регламенту, а також забезпечено її належний монтаж, інсталювання, обслуговування та використання за призначенням.

**Суттєві вимоги**

7. Продукція з урахуванням її призначення та особливостей (умов) застосування повинна відповідати вимогам ДСТУ ISO/IEC 19790 з урахуванням національних особливостей, встановлених в додатку 2 цього Технічного регламенту.

**Вільний рух продукції**

8. Надання на ринку та введення в експлуатацію на території України продукції, що призначена для застосування виключно для цілей електронної ідентифікації та відповідає вимогам цього Технічного регламенту, не може бути заборонено, обмежено чи створено будь-які інші перешкоди.

**Обов'язки виробників**

9. Виробники під час введення продукції в обіг або використання її у своїх цілях гарантують, що вона розроблена та виготовлена відповідно до вимог, встановлених у додатку 2 цього Технічного регламенту.

10. Виробники складають технічну документацію, визначену в додатках Технічного регламенту та проводять або доручають уповноваженому представнику проведення належної процедури оцінки відповідності згідно з вимогами цього Технічного регламенту.

У разі коли відповідність продукції, за винятком компонента, була доведена належною процедурою оцінки відповідності, виробники складають

декларацію про відповідність та наносять знак відповідності технічним регламентам.

Якщо відповідність компонента вимогам, що застосовані до нього, була доведена належною процедурою оцінки відповідності, виробники складають письмову заяву про відповідність згідно з пунктом 41 цього Технічного регламенту.

11. Виробники супроводжують кожну одиницю продукції копією декларації про відповідність або у відповідних випадках копією заяви про відповідність. Якщо одному споживачу (користувачу) постачається велика кількість продукції, така партія може супроводжуватися однією копією зазначених документів.

12. Виробники зберігають технічну документацію та декларацію про відповідність або у відповідному випадку заяву про відповідність протягом 10 років після введення останнього зразка продукції в обіг.

13. Виробники забезпечують дотримання процедур, необхідних для підтримання відповідності серійного виробництва продукції вимогам цього Технічного регламенту.

Повинні враховуватися зміни в конструкції чи характеристиках продукції та зміни в національних стандартах, які є ідентичними гармонізованим європейським стандартам та відповідність яким надає презумпцію відповідності продукції або в інших технічних специфікаціях, шляхом посилання на які декларується відповідність продукції.

14. Зважаючи на ризики, які становить продукція, виробники проводять вибіркові випробування зразків продукції, що надана на ринку, розглядають звернення споживачів (користувачів), досліджують продукцію, що не відповідає вимогам цього Технічного регламенту, і випадки відкликання продукції та за необхідності ведуть облік звернень щодо невідповідності продукції встановленим вимогам і випадків її відкликання, а також інформують розповсюджувачів про поточні результати такого моніторингу.

15. Виробники забезпечують, щоб на продукцію, яку вони ввели в обіг, було зазначено тип, номер партії чи серійний номер або інший елемент, який дозволяє здійснити її ідентифікацію, а в разі коли розміри або характер продукції не дає змоги цього зробити, - щоб необхідна інформація була зазначена на пакуванні або в документі, що супроводжує цю продукцію.

16. Виробники зазначають своє найменування, зареєстроване комерційне найменування чи зареєстровану торговельну марку (знак для товарів і послуг)

та контактну поштову адресу, за якою можна зв'язатися з ними, на продукції, а якщо це неможливо - на її пакуванні чи в документі, що супроводжує цю продукцію. Контактні дані наводяться згідно з вимогами закону про порядок застосування мов.

17. Продукція супроводжується документами та інформацією, передбаченою цим Регламентом та стандартом ДСТУ ISO/IEC 19790, що складені виробниками згідно з вимогами закону про порядок застосування мов. Зазначені інструкції та інформація про безпечність, а також будь-яке маркування повинні бути чіткими, зрозумілими та розбірливими.

18. У разі коли виробники вважають або мають підстави вважати, що продукція, яку ввели в обіг, не відповідає вимогам цього Технічного регламенту, вони негайно вживають коригувальних заходів, необхідних для приведення такої продукції у відповідність із встановленими вимогами, вилучення її з обігу та/або її відкликання (залежно від обставин). Якщо зазначена продукція становить ризик, виробники негайно повідомляють про це відповідному органу державного ринкового нагляду та подають йому детальні відомості, зокрема про невідповідність такої продукції вимогам цього Технічного регламенту та вжиті коригувальні заходи.

19. На обґрунтований запит органу державного ринкового нагляду виробники надають всю інформацію та документацію (в паперовій або електронній формі), необхідну для демонстрування відповідності продукції вимогам цього Технічного регламенту. На вимогу зазначеного органу державного ринкового нагляду виробники співпрацюють з ним стосовно будь-яких дій, які вживаються для усунення ризиків, що становить введена ними в обіг продукція.

**Обов'язки уповноважених представників**

20. Виробник на підставі письмового доручення може визначити уповноваженого представника. Обов'язки виробника, передбачені пунктами 12 і 13 цього Технічного регламенту, та обов'язок щодо складення технічної документації, встановлений в пункті 17 цього Технічного регламенту, не повинні включатися до предмету доручення, одержаного уповноваженим представником.

21. Уповноважений представник виконує завдання, визначені у дорученні, одержаному від виробника, зокрема:

зберігає технічну документацію для надання їх на запити органів державного ринкового нагляду протягом 10 років після введення останнього зразка продукції в обіг;

на обґрунтований запит органу державного ринкового нагляду надає всю інформацію та документацію, необхідну для демонстрування відповідності продукції вимогам цього Технічного регламенту;

на вимогу органу державного ринкового нагляду співпрацює з ним стосовно будь-яких заходів, які вживаються для усунення ризиків, що становить продукція, на яку поширюється дія доручення, одержаного уповноваженим представником.

**Обов'язки імпортерів**

22. Імпортери вводять в обіг лише продукцію, яка відповідає вимогам цього Технічного регламенту.

23. До початку введення продукції в обіг імпортери пересвідчуються в тому, що виробник виконав вимоги, встановлені в пунктах 10, 11, 15-17 цього Технічного регламенту.

Якщо імпортер вважає або має підстави вважати, що продукція не відповідає суттєвим вимогам, встановленим у додатку 2 цього Технічного регламенту, він не вводить цю продукцію в обіг до приведення її у відповідність з цими вимогами. Якщо зазначена продукція становить ризик, імпортер повідомляє про це виробнику та органам державного ринкового нагляду.

24. Імпортери зазначають своє найменування, зареєстроване комерційне найменування чи зареєстровану торговельну марку (знак для товарів і послуг) та контактну поштову адресу на продукції, а якщо це неможливо - на її пакуванні чи в документі, що супроводжує цю продукцію. Контактні дані наводяться згідно з вимогами закону про порядок застосування мов.

25. Імпортери забезпечують супроводження продукції документами та інформацією, передбаченою стандартом ДСТУ ISO/IEC 19790, які складені згідно з вимогами закону про порядок застосування мов.

26. Імпортери протягом 10 років після введення останнього зразка продукції в обіг зберігають копію декларації про відповідність або у відповідному випадку заяви про відповідність для надання її на запити органів державного ринкового нагляду та забезпечують можливість надання цим органам за їх запитами доступу до технічної документації.

27. На обґрунтований запит органу державного ринкового нагляду імпортери повинні надавати всю інформацію та документацію (в паперовій або електронній формі), необхідну для демонстрування відповідності продукції вимогам цього Технічного регламенту. На вимогу зазначеного органу державного ринкового нагляду імпортери співпрацюють з ним стосовно будь-яких дій, які вживаються для усунення ризиків, що становить введена ними в обіг продукція.

**Обов'язки розповсюджувачів**

28. Розповсюджувачі під час надання продукції на ринку діють згідно з вимогами цього Технічного регламенту.

29. Перед наданням продукції на ринку розповсюджувачі перевіряють, що продукція супроводжується необхідними документами, які складені згідно з вимогами закону про порядок застосування мов, а виробник та імпортер виконали вимоги, визначені в пунктах 11 і 17 цього Технічного регламенту.

Якщо розповсюджувач вважає або має підстави вважати, що продукція не відповідає суттєвим вимогам, встановленим у додатку 2 цього Технічного регламенту, він зобов'язаний не надавати цю продукцію на ринок до приведення її у відповідність з цими вимогами. Якщо зазначена продукція становить ризик, розповсюджувач повідомляє про це виробнику або імпортеру, а також відповідному органу державного ринкового нагляду.

30. Розповсюджувачі забезпечують, щоб умови зберігання чи транспортування продукції (доки вона перебуває під їх відповідальністю) не ставили під загрозу її відповідність суттєвим вимогам, встановленим у додатку 2 цього Технічного регламенту.

31. Розповсюджувачі, які вважають або мають підстави вважати, що продукція, яку вони надали на ринку, не відповідає вимогам цього Технічного регламенту, пересвідчуються, що вжито коригувальних заходів, необхідних для приведення такої продукції у відповідність з цими вимогами, вилучення її з обігу та/або відкликання (залежно від обставин). Якщо зазначена продукція становить ризик, розповсюджувачі негайно повідомляють про це відповідному органу державного ринкового нагляду та подають йому детальні відомості, зокрема про невідповідність такої продукції вимогам цього Технічного регламенту та вжиті коригувальні заходи.

32. На обґрунтований запит органу державного ринкового нагляду розповсюджувачі надають всю інформацію та документацію (в паперовій або електронній формі), необхідну для демонстрування відповідності продукції

вимогам цього Технічного регламенту. На вимогу зазначеного органу державного ринкового нагляду розповсюджувачі співпрацюють з ним стосовно будь-яких заходів, які вживаються для усунення ризиків, що становить надана ними на ринку продукція.

**Випадки, в яких обов'язки виробників покладаються на імпортерів або розповсюджувачів**

33. У разі коли імпортер або розповсюджувач вводить продукцію в обіг під своїм найменуванням чи торговельною маркою (знаком для товарів і послуг) або модифікує вже введену в обіг продукцію в такий спосіб, що може вплинути на її відповідність вимогам цього Технічного регламенту, він вважається виробником та виконує обов'язки виробника, встановлені в пунктах 10-19 цього Технічного регламенту.

**Ідентифікація суб'єктів господарювання**

34. Суб'єкти господарювання надають органам державного ринкового нагляду за їх запитами інформацію, що дає змогу ідентифікувати:

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

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

Суб'єкти господарювання надають інформацію, визначену в цьому пункті, протягом 10 років після того, як їм було поставлено продукцію, та протягом 10 років після того, як вони поставили продукцію.

**Презумпція відповідності продукції**

35. Презумпцію відповідності продукції суттєвим вимогам, встановленим додатком 2 Технічного регламенту є відповідність продукції вимогам:

нормативно-правових актів спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації, розроблених для виконання вимог цього Технічного регламенту;

нормативних документів згідно з Переліком нормативних документів, які визначають суттєві вимоги до криптографічних модулів та оцінки їх відповідності (таблиця 2 додатку 2 цього Технічного регламенту);

нормативних документів в частині, що стосуються функціонального призначення продукції, згідно з Переліком нормативних документів, які визначають додаткові (опціональні вимоги) до криптографічних модулів (таблиця 3 додатку 2 Технічного регламенту).

**Процедури оцінки відповідності**

36. Оцінка відповідності криптографічної продукції здійснюється шляхом застосування наступних процедур оцінки відповідності:

1) для засобів, що призначені для захисту цілісності та авторства відкритої інформації, шляхом застосування процедур визначених у додатках 3-9 Технічного регламенту;

2) для засобів, призначені для захисту цілісності та авторства відкритої інформації у державних органах, шляхом застосування процедур визначених у додатках 3-9 Технічного регламенту;

3) для засобів, що призначені для захисту комерційної таємниці, шляхом застосування процедур визначених у додатках 3-9 цього Технічного регламенту;

4) для засобів, що призначені для захисту конфіденційної інформації та персональних даних, які обробляються у державних органах, шляхом застосування процедур визначених у додатках 3-9 цього Технічного регламенту.

37. Оцінка відповідності захисних систем здійснюється шляхом застосування процедур визначених у додатках 3-9 цього Технічного регламенту.

38. Процедури оцінки відповідності, зазначені в пункті 39 цього Технічного регламенту, застосовуються до компонентів, але без нанесення знаку відповідності технічним регламентам і складення декларації про відповідність.

Для компонентів виробник надає письмову заяву про відповідність, яка засвідчує відповідність зазначених компонентів застосовним вимогам цього Технічного регламенту, із зазначенням їх характеристик, а також того, яким чином вони повинні бути вмонтовані в обладнання чи в захисні системи, щоб не вплинути на відповідність готового обладнання або захисних систем суттєвим вимогам, встановленим у додатку 2 цього Технічного регламенту.

**Декларація про відповідність**

39. У декларації про відповідність заявляється про те, що виконання суттєвих вимог, встановлених у додатку 2 цього Технічного регламенту, доведено.

40. Декларація про відповідність складається згідно з примірною структурою, встановленою в додатку 10 цього Технічного регламенту, містить відомості, визначені у відповідних процедурах оцінки відповідності,

встановлені в додатках 3-9 цього Технічного регламенту та постійно оновлюється. Декларація про відповідність складається державною мовою, а у разі, коли вона складена іншою мовою, - перекладається на державну мову.

41. У разі коли на деяку продукцію, яка включає криптографічну продукцію, поширюється дія кількох технічних регламентів, що вимагають складення декларації про відповідність, складається єдина декларація про відповідність стосовно всіх таких технічних регламентів. У такій декларації про відповідність зазначаються відповідні технічні регламенти, включаючи відомості про їх офіційне опублікування.

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

42. Виробник, який складає декларацію про відповідність, бере на себе відповідальність за відповідність продукції вимогам, установленим у цьому Технічному регламенті.

**Загальні принципи маркування знаком відповідності технічним регламентам, правила та умови його нанесення, в також іншого маркування**

43. Знак відповідності технічним регламентам застосовується згідно із загальними принципами маркування зазначеним знаком, установленими законом.

44. Знак відповідності технічним регламентам наноситься на продукцію або на табличку з технічними даними та має бути видимим, розбірливим і стійким до стирання. Якщо це є неможливим або невиправданим через характер продукції, знак відповідності технічним регламентам наноситься на пакування та на документ, що супроводжує продукцію.

45. Знак відповідності технічним регламентам наноситься перед введенням продукції в обіг.

46. Знак відповідності технічним регламентам супроводжується ідентифікаційним номером призначеного органу, якщо такий орган був залучений на етапі контролю виробництва.

Ідентифікаційний номер призначеного органу наноситься самим органом або за його вказівкою виробником або уповноваженим представником.

47. Знак відповідності технічним регламентам та ідентифікаційний номер призначеного органу (у разі його нанесення) супроводжується інформацією, зазначеною в додатку 2 цього Технічного регламенту.

48. У разі неналежного застосування маркування вживаються заходи в установленому законом порядку.

**Призначення органів з оцінки відповідності**

49. Призначення органів з оцінки відповідності для виконання ними як третіми сторонами завдань з оцінки відповідності згідно з цим Технічним регламентом здійснюється національним органом по акредитації за погодженням спеціально уповноваженого органу у галузі зв'язку та захисту інформації.

50. Призначені органи повинні відповідати вимогам Закону України «Про технічні регламенти та оцінку відповідності» пунктам 51-62 цього Технічного регламенту.

51. Орган з оцінки відповідності криптографічної продукції повинен відповідати ліцензійним умовам провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України.

52. Орган з оцінки відповідності криптографічної продукції повинен бути незалежним від особи, що надає об'єкт оцінки відповідності, та від особи, що заінтересована в такому об'єкті як споживач чи користувач.

Орган з оцінки відповідності, який є членом об'єднання підприємців, що представляє юридичних осіб та/або фізичних осіб - підприємців, які беруть участь у проектуванні, виготовленні, реалізації, монтажі, використанні чи обслуговуванні продукції, яку він оцінює, може вважатися третьою стороною за умови доведення незалежності такого органу та відсутності будь-якого конфлікту інтересів.

53. Орган з оцінки відповідності (його керівник, заступники керівника та персонал, відповідальний за виконання завдань з оцінки відповідності):

не повинен бути проектувальником, виробником, імпортером, розповсюджувачем, монтажником, покупцем, власником, користувачем чи відповідальним за обслуговування продукції, яку він оцінює, або представником будь-якої з цих сторін. Зазначена вимога не виключає можливості використання оцінюваної продукції, яка є необхідною для роботи органу з оцінки відповідності, чи використання такої продукції в особистих цілях;

не повинен брати безпосередньої участі у проектуванні, виготовленні, спорудженні, реалізації, монтажі, використанні чи обслуговуванні продукції, яку він оцінює, або представляти сторони, що беруть участь у такій діяльності. Такий орган не повинен провадити будь-яку діяльність, яка може суперечити незалежності його суджень або його доброчесності стосовно діяльності з оцінки відповідності, на провадження якої він призначається або призначений. Така вимога, зокрема, стосується послуг з консультування.

Орган з оцінки відповідності забезпечує, щоб діяльність субпідрядників або дочірніх підприємств, які ним залучаються до виконання робіт з оцінки відповідності, не впливала на конфіденційність інформації, об'єктивність і неупередженість діяльності з оцінки відповідності такого органу.

54. Орган з оцінки відповідності повинен провадити діяльність з оцінки відповідності належним чином та з технічною компетентністю, бути вільним від будь-якого тиску та спонукання, зокрема фінансового характеру, які могли б впливати на його судження або результати його діяльності з оцінки відповідності, особливо з боку осіб чи груп осіб, заінтересованих у результатах такої діяльності.

55. Орган з оцінки відповідності повинен бути здатним виконувати всі завдання, які покладені на нього згідно з додатками 3-9 цього Технічного регламенту та стосовно яких він призначається чи був призначений, незалежно від того, чи такі завдання виконуються самим органом з оцінки відповідності, чи від його імені та під його відповідальність.

Орган з оцінки відповідності у будь-який час і для кожної процедури оцінки відповідності та кожного виду чи категорії продукції, стосовно якої він призначається чи був призначений, повинен мати необхідні:

кваліфікований та досвідчений персонал для виконання завдань з оцінки відповідності;

описи процедур, згідно з якими проводиться оцінка відповідності, що забезпечують прозорість і відтворюваність таких процедур. Орган з оцінки відповідності повинен застосовувати відповідні правила, методики, настанови та процедури тощо, що дають змогу розрізняти завдання, які він виконує як призначений орган, та іншу діяльність;

процедури для провадження діяльності з оцінки відповідності з належним урахуванням розміру суб'єкта господарювання, що замовляє роботи з оцінки відповідності, галузі, в якій він провадить діяльність, його структури, ступеня

складності технології виробництва відповідної продукції та масового чи серійного характеру виробничого процесу.

Орган з оцінки відповідності повинен мати необхідні для виконання в належний спосіб технічних і адміністративних завдань з оцінки відповідності засоби, а також мати доступ до всього іншого необхідного обладнання чи матеріально-технічної бази.

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

технічну і професійну підготовку, що охоплює всю діяльність з оцінки відповідності, стосовно якої орган з оцінки відповідності був призначений;

достатні знання вимог, які стосуються робіт з оцінки відповідності, які він проводить, та відповідні повноваження для проведення таких робіт;

відповідні знання та розуміння суттєвих вимог, встановлених у додатку 2 цього Технічного регламенту, стандартів з переліку національних стандартів, що застосовуються, положень законодавства України щодо умов обігу на ринку продукції, яку він оцінює, а також відповідних положень законодавства Європейського Союзу;

досвід із складення сертифікатів, протоколів та звітів, які підтверджують проведення робіт з оцінки відповідності.

57. Повинна бути забезпечена неупередженість органу з оцінки відповідності, його керівника, заступників керівника та 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 робіт з оцінки відповідності чи їх результатів.

58. Персонал органу з оцінки відповідності повинен забезпечувати дотримання вимог щодо поширення інформації з обмеженим доступом, захист якої гарантується законом, одержаної під час виконання своїх завдань згідно з додатками 3-7 і 9 цього Технічного регламенту, крім її надання у визначених законом випадках відповідним уповноваженим органам.

59. У разі коли призначений орган залучає до виконання конкретних робіт, пов'язаних з оцінкою відповідності, субпідрядника або дочірнє підприємство, він повинен пересвідчитися у тому, що зазначений субпідрядник

чи дочірнє підприємство відповідає вимогам, визначеним у пунктах 55-63 цього Технічного регламенту, та повідомити про це орган, що призначає.

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

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

62. Призначені органи повинні зберігати для надання на запити органу, що призначає, відповідні документи стосовно оцінювання кваліфікації залучених субпідрядників або дочірніх підприємств і робіт, що виконуються ними згідно з додатками 3-7 і 9 цього Технічного регламенту.

**Обов'язки призначених органів стосовно їх діяльності**

63. Призначені органи здійснюють оцінку відповідності згідно з процедурами оцінки відповідності, встановленими в додатках 3-7 і 9 цього Технічного регламенту.

64. Оцінка відповідності повинна проводитися у пропорційний спосіб, без покладення зайвого навантаження на суб'єктів господарювання. Призначені органи повинні провадити свою діяльність з належним урахуванням величини суб'єкта господарювання, що замовляє роботи з оцінки відповідності, галузі, в якій він провадить діяльність, його структури, ступеня складності технології виробництва певної продукції та масового чи серійного характеру виробничого процесу.

Призначені органи повинні дотримуватися ступеня вимогливості та рівня захисту, що є необхідними для відповідності продукції вимогам цього Технічного регламенту.

65. У разі коли призначений орган вважає, що виробником не були виконані суттєві вимоги, встановлені в додатку 2 цього Технічного регламенту або у відповідних стандартах з переліку національних стандартів чи інших технічних специфікаціях, зазначений орган вимагає від виробника вжити відповідних коригувальних заходів та не видає документ про відповідність.

66. У разі коли під час проведення моніторингу відповідності продукції після видачі документа про відповідність призначений орган виявить, що продукція вже не відповідає вимогам, зазначений орган вимагає від виробника вжити відповідних коригувальних заходів і в разі необхідності зупиняє дію або скасовує виданий документ про відповідність.

67. Якщо коригувальних заходів не було вжито або вони не дали необхідних результатів, призначений орган залежно від обставин обмежує сферу дії, зупиняє дію або скасовує будь-який документ про відповідність.

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

**Обов'язки призначених органів стосовно надання інформації**

69. Призначені органи інформують орган, що призначає, про:

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

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

запити щодо надання інформації стосовно діяльності з оцінки відповідності, одержані ними від органів державного ринкового нагляду.

Призначені органи на запит органу, що призначає, інформують його про діяльність з оцінки відповідності, проведену в межах сфери їх призначення, та будь-яку іншу проведену діяльність, зокрема транскордонну діяльність, та роботи за договорами субпідряду.

70. Призначені органи надають іншим органам з оцінки відповідності, які призначені згідно з цим Технічним регламентом та провадять подібну діяльність з оцінки відповідності, що охоплює таку саму продукцію, відповідну інформацію з питань, які стосуються негативних результатів оцінки відповідності та на їх запит - також позитивних результатів оцінки відповідності.

**Державний ринковий нагляд і контроль продукції**

71. Державний ринковий нагляд і контроль введеної в обіг продукції здійснюється відповідно до закону з урахуванням вимог цього Технічного регламенту.

72. Заходи щодо усунення формальної невідповідності вживаються в разі, коли орган державного ринкового нагляду встановить будь-яку таку невідповідність:

не було нанесено знак відповідності технічним регламентам;

органу державного ринкового нагляду не надано доступу до технічної документації або вона є не в повному обсязі;

не виконано будь-яку іншу з адміністративних вимог, установлених у пунктах 09-19 або 22-27 цього Технічного регламенту.

04/02/03 -1288
23.04.18

Додаток 1
Технічного регламенту засобів криптографічного захисту інформації

## Терміни та їх визначення

Для цілей Технічного регламенту засобів криптографічного захисту інформації використовуються терміни та їх визначення тотожні визначенням міжнародного стандарту ISO/IEC 19790, що наведені у таблиці №1.

Таблиця № 1

| Номер пункту ISO/IEC 19790 | Термін та скорочення | Англомовний термін та скорочення | Визначення |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| A.1 #3.3 | Автоматичний | Automated | (Процес або функція), що виконуються без втручання людини. |
| A.2 #3.76 | Автономний криптографічний модуль із декількома чіпами | Multiple-chip standalone cryptographic module | Фізичне об'єднання, в якому дві або декілька інтегральних мікросхем з'єднані між собою і весь корпус фізично захищений, наприклад, маршрутизатори з шифруванням. |
| A.3 #3.50 | Апаратне забезпечення | Hardware | Фізичне устаткування/компоненти в межах криптосхеми, що використовується для виконання програм і обробки даних |
| A.4 #3.51 | Апаратний модуль | Hardware module | Модуль, що складається в основному з апаратних засобів, які можуть містити вбудоване програмне забезпечення |
| A.5 #3.98 | (Асиметричний) криптографічний | Public key (asymmetric) | Криптографічний алгоритм, який використовує пов'язану пару ключів: відкритий і приватний ключ. |

до N 04/02/03-1283

Продовження додатка 1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | алгоритм з відкритим ключем | cryptographic algorithm | |
| A.6 #3.9 | Асиметричне криптографічне перетворення | Asymmetric cryptographic technique | Криптографічна функція (алгоритм) така, що ключі прямого та зворотного перетворення не співпадають, а находження одного з іншого в заданих умовах є практично не розв'язною обчислювальною задачею. При цьому один з ключів, за визначенням, є приватним та зберігається у таємниці, інший - відкритий – використовується ідентифікованими користувачами. |
| A.7 #3.78 | Атака без підключення (до криптосхеми) | Non-invasive attack | атака на криптографічний модуль, що може виконуватися без прямого фізичного контакту с компонентами в межах криптосхеми модуля. Ця атака не змінює стану криптографічного модуля. |
| A.8 #3.74 | Багатофакторна автентифікація | Multi-factor authentication | Автентифікація із використанням принаймні двох незалежних факторів автентифікації. |
| A.9 #3.31 | Безпосередній ввід | Direct entry | Введення ЧПБ або компонента ключа у криптографічний модуль за допомогою пристрою, такого як клавіатура. |
| A.10 #3.10 | Біометричний | Biometric | (Метод, засіб), що заснований на вимірюванні фізичної характеристики особи або рисах поведінки та використаний для процедур автентифікації та ідентифікації |
| A.11 #3.75 | Вбудований криптографічний модуль із декількома чіпами | Multiple-chip embedded cryptographic module | Фізичний пристрій, в якому дві або декілька інтегральних мікросхем з'єднані між собою і вбудовані в корпус або продукт, які не можуть бути фізично захищені, наприклад. адаптери та плати розширення. |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| A.12 #3.45 | Вбудоване програмне забезпечення | ВПЗ | Firmware | | Незмінний код (прошивка), який виконується криптографічним модулем та зберігається у апаратних засобах (PROM, EEPROM, FLASH тощо) в межах криптосхеми. Цей код є статичним і не може змінюватися під час виконання у немодифікованому або обмеженому операційному середовищі. |
| A.13 #3.42 | Вид, придатний для виконання | | Executable form | | Вид коду, в якому програмне забезпечення або вбудоване програмне забезпечення повністю управляється і контролюється операційним середовищем модуля і не вимагає компіляції (наприклад, немає початкового коду, об'єктного коду або коду, здатного до компіляції за першої необхідності) |
| A.14 #3.86 | Вихідні дані | | Output data | | Вихідна інформація, що отримана за допомогою криптографічного модуля |
| A.15 #3.113 | Вихід послуги | | Service output | | Усі дані та інформація про стан, які є результатом операцій або функцій, ініційованих або отриманих входом послуги. |
| A.16 #3.125 | Виявлення вторгнення | | Tamper detection | | Автоматичне визначення криптографічним модулем спроби подолання системи безпеки модуля |
| A.17 #3.96 | Відкритий ключ | | Public key | | Один з пари асиметричних ключів криптографічного перетворення, який може бути загально доступним. |
| A.18 #3.99 | Відкритий параметр безпеки | ВПБ | Public security parameter | PSP | Пов'язана з безпекою відкрита інформація, модифікація якої може негативно вплинути на безпеку криптографічного модуля. До ВПБ, зокрема, відносять відкриті криптографічні ключі, сертифікати відкритих ключів, само підписані сертифікати, довірчі точки, одноразові паролі, пов'язані з лічильником, внутрішньо підтримувані дата та час. |
| A.19 | Відповідь на | | Tamper response | | Автоматичні дії криптографічного модуля у разі виявлення |

Продовження додатка І

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| #3.127 | вторгнення | | | | вторгнення |
| A.20<br>#3.35 | Всеохоплюючий підпис | | Encompassing signature | | Єдиний підпис для всієї структури коду |
| A.21<br>#3.121 | Встановлення ЧПБ | | SSP establishment | | Процес створення доступності спільного ЧПБ для однієї або декількох осіб. Встановлення ЧПБ охоплює узгодження, передачу і вводу або виводу ЧПБ. |
| A.22<br>#3.57 | Вхідні дані | | Input data | | Інформація, яка вводиться в криптографічний модуль і вона може використовуватися для перетворення або обчислення із використанням затвердженої функції безпеки |
| A.23<br>#3.112 | Вхід послуги | | Service input | | Усі дані або керуюча інформація, що використовуються в криптографічному модулі, який ініціює або отримує конкретні операції або функції |
| A.24<br>#3.100 | Генератор випадкових бітів | ГВБ | Random bit generator | RBG | Пристрій або алгоритм, який видає послідовність бітів, які є незалежними та рівномірно розподіленими. |
| A.25<br>#3.53 | Геш-значення | | Hash value | | Результат застосування криптографічної геш-функції |
| A.26<br>#3.54 | Гібридний модуль | | Hybrid module | | Модуль, чий криптографічний кордон розмежовує компонент комбінованого програмного забезпечення або вбудованого програмного забезпечення і розчленований компонент апаратного забезпечення |
| A.27<br>#3.29 | Диференційний аналіз споживання | | Differential power analysis | DPA | Аналіз зміни споживання електроенергії криптографічного модуля з метою отримання інформації, яка корелює з криптографічною операцією |
| A.28<br>#3.93 | Доексплуатаційне самотестування | | Pre-operational self-test | | Тестування, що виконується криптографічним модулем до переходу в робочий стан після його включення або перезавантаження |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| A.29 #3.126 | Доказ вторгнення | | Tamper evidence | | Спостережувана ознака спроби подолання системи безпеки криптографічного модуля |
| A.30 | Гарантоздатність | | | | Комплексна характеристика, що визначає здатність засобу КЗІ надавати потрібні послуги, яким виправдано можна довіряти. Включає наступні первісні складові:<br>Безвідмовність (reliability) – властивість безперервно надавати коректні послуги;<br>Готовність (availability) – властивість доступності ресурсів засобу КЗІ для надання потрібних послуг;<br>Живучість (survivability) властивість мінімізувати зниження та зберігати у припустимих межах обсяг і якість послуг, що надаються, в погіршених умовах функціонування;<br>Функціональна безпека (safety) – властивість виключати або мінімізувати шкідливі наслідки в уразі відмов для користувачів та систем, у складі яких вони працюють;<br>Цілісність (integrity) – властивість виключати непередбачувані зміни криптосхеми та послуг, які надаються;<br>Конфіденційність (confidentiality) – властивість уникати несанкціонованого доступу до чутливих параметрів і даних, а також про послуги, які надаються;<br>Достовірність (high confidence) – властивість вірно оцінювати коректність послуг, що надаються, тобто визначати степінь довіри до них;<br>Обслуговуваність (maintainability) – властивість придатності до ремонту та модифікацій. |
| A.31 | Експлуатаційний | | Operational state | | Стан, коли послуги або функції можуть викликатися |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| #3.84 | стан | | | | оператором і отримані в результаті дані виводяться з інтерфейсу виводу даних криптографічного модуля |
| A.32<br>#3.34 | Електронний ввід | | Electronic entry | | Ввід ЧПБ або компонентів ключа в криптографічний модуль. електронними методами без втручання оператора. |
| A.33<br>#3.30 | (Електронний) цифровий підпис | | Digital signature | | Дані, що додані до блоку даних, отримані у результаті криптографічного перетворення цього блоку та дозволяють довести його авторство і цілісність, а також захистити від підробки. |
| A.34<br>#3.38 | Ентропія | | Entropy | | Міра безладу, випадковості або мінливості в замкнутій системі, зокрема, ентропія випадкової величини X є характеристикою кількості інформації, отриманої при спостереженні за X. |
| A.35<br>#3.5 | Затверджений метод автентифікації даних | | Approved data authentication technique | | Затверджений метод, який може застосовувати електронний цифровий підпис, імітовставку / код автентифікації повідомлення або гешування з ключем. |
| A.36<br>#3.6 | Затверджений метод контролю цілісності | | Approved integrity technique | | Затверджений метод, який може застосовувати електронний цифровий підпис, імітовставку / код автентифікації повідомлення. |
| A.37<br>#3.7 | Затверджений режим роботи | | Approved mode of operation | | Затверджений набір функціональних та/або безпекових послуг, що охоплює принаймні одну послугу, яка використовує затверджений процес або функцію безпеки. |
| A.38<br>#3.8 | Затверджена (схвалена) функція безпеки | | Approved security function | | Функція безпеки, що визначена цим регламентом або погоджена органом затвердження, зокрема, рекомендований криптографічний алгоритм |
| A.39 | Захист від відмов, | | Environmental | EFP | Використання функцій для захисту від компрометації безпеки |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| #3.39 | спричинених середовищем | | failure protection | | криптографічного модуля, спричиненою змінами середовища, які не відповідають вимогам типового робочого діапазону модуля |
| A.40 #3.36 | Зашифрований ключ | | Encrypted key | | Криптографічний ключ, який був зашифрований з використанням затвердженої функції безпеки та ключем шифрування ключів. |
| A.41 #3.101 | Знімний кожух | | Removable cover | | Фізична оболонка,що спеціально створена для виключення можливості несанкціонованого доступу до вмісту криптографічного модуля без її руйнування |
| A.42 #3.59 | Інтерфейс | | Interface | | Логічна точка входу або виходу криптографічного модуля, яка забезпечує доступ до модуля для логічних потоків інформації |
| A.43 #3.52 | Інтерфейс апаратного модуля | | Hardware module interface | HMI | Скінчена множина команд, що використовуються для запиту послуг апаратного модуля, у тому числі параметрів, які перетинають в обох напрямках межі крипто схеми модуля в рамках використання його послуги |
| A.44 #3.55 | Інтерфейс гібридного модуля вбудованого програмного забезпечення | | Hybrid firmware module interface | HFMI | Скінчена множина команд, що використовується для запиту послуг гібридного модуля вбудованого програмного забезпечення, у тому числі параметрів, які перетинають в обох напрямках межі криптосхеми модуля в рамках використання його послуги |
| A.45 #3.56 | Інтерфейс гібридного модуля програмного забезпечення | | Hybrid software module interface | HSMI | Скінчена множина команд, що використовується для запиту послуг гібридного модуля програмного забезпечення, у тому числі параметрів, які перетинають в обох напрямках межі криптосхеми модуля в рамках використання його послуги |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| A.46 #3.119 | Інтерфейс модуля програмного забезпечення/ вбудованого програмного забезпечення | | Software / firmware module interface | SFMI | Множина команд, що використовується для запиту послуг програмного модуля або вбудованого програмного забезпечення, у тому числі параметрів, які перетинають в обох напрямках межу криптосхеми модуля в рамках використання його послуги |
| A.47 #3.17 | Інформація керування | | Control information | | Інформація, яка вводиться у криптографічний модуль з метою управління його роботою |
| A.48 #3.122 | Інформація про стан | | Status information | | Інформація, яка виводиться з криптографічного модуля з метою індикації його деяких експлуатаційних характеристик чи стану. |
| A.49 #3.64 | Керування ключами | | Key management | | Сукупність функцій адміністрування ключів під час їх життєвого циклу, включаючи генерацію, реєстрацію, сертифікацію, зняття з обліку, поширення, зберігання, інсталювання, використання архівування, відкликання, вивід і знищення ключів (ключового матеріалу) у відповідності до політики безпеки |
| A.50 | Ключовий матеріал | | Key materials | | Вихідні дані із заданими характеристиками, що використовуються для побудови конкретних ключів, зокрема підстановок та перестановок |
| A.51 #3.63 | Ключовий носій | | Key loader | | Автономний пристрій, здатний зберігати щонайменше один ЧПБ у відкритому або зашифрованому вигляді, або компонент ключа, який може бути завантажений оператором КЗІ в криптографічний модуль. |
| A.52 #3.91 | Ключ у відкритому | | Plaintext key | | Незашифрований криптографічний ключ або криптографічний ключ, зашифрований не затвердженим методом. |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| | вигляді | | | | |
| A.53 #3.107 | Ключ генерації ключів | | Seed key | | Секретний параметр, що використовується для ініціалізації генераторів псевдовипадкових бітів |
| A.54 #3.62 | Ключ шифрування ключів | | Key encryption key | KEK | Криптографічний ключ, який використовується для шифрування або розшифрування інших ключів |
| A.55 #3.70 | Код автентифікації повідомлення (імітовставка) | | Message authentication code | MAC | Результат криптографічного перетворення даних, що отриманий з використанням секретного ключа симетричного алгоритму та призначений для виявлення випадкових і навмисних змін даних. |
| A.56 #3.13 | Компрометація | | Compromise | | Випадок помилкових або зловмисних дій, відмов або збоїв програм та обладнання що призвів до розкриття, модифікації або несанкціонованого використання критичних параметрів безпеки, модифікації або втрати автентичності відкритих параметрів безпеки |
| A.57 #3.103 | Контроль доступу, що ґрунтується на ролях | | Role-based access control | RBAC | Метод управління доступом, який ґрунтується на визначенні ролей, яким надається право доступу до певного об'єкту |
| A.58 #3.15 | Конфіденційність | | Confidentiality | | Властивість, за якої інформація не стає доступною або не розкривається несанкціонованим сторонам |
| A.59 #3.18 | Критичний параметр безпеки | КПБ | Critical security parameter | CSP | Дані, що пов'язані з безпекою криптографічного модуля або інформації, яка захищається, розкриття або зміна яких може призвести до повної або часткової втрати властивостей КЗІ. До КПБ належать, зокрема, секретні (приватні) криптографічні ключі, дані автентифікації, такі як паролі, PIN-коди, |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| | | | | | сертифікати або інші точки довіри. |
| А.60 | Криптографічний захист інформації | КЗІ | Cryptographic protection | | Вид захисту інформації, який реалізується за допомогою її математичних перетворень з використанням секретних параметрів - ключів |
| А.61 #3.20 | Криптографічний алгоритм (криптоалгоритм) | | Cryptographic algorithm | | Коректно визначена та належним чином специфікована обчислювальна процедура, яка на підставі її опису може бути реалізована у програмному або апаратному вигляді та використана з метою КЗІ |
| А.62 | Криптографічна схема (криптосхема) | | Cryptographic scheme | | Сукупність взаємодіючих криптографічних перетворень, що забезпечують виконання завдань за призначенням та безпеку криптографічного модуля |
| А.63 #3.22 | Криптографічна геш-функція | | Cryptographic hash function | | Обчислювально ефективна функція, що відповідає заданим криптографічним вимогам та відображає двійкові рядки довільної довжини у двійкові рядки фіксованої довжини. |
| А.64 | Криптографічне перетворення (функція) | | Cryptographic function | | Функція, за допомогою якої реалізується криптографічний захист інформації. Криптографічні перетворення, зокрема, охоплюють зашифрування та розшифрування даних, генерацію та перевірку електронного цифрового підпису, генерацію ключів. |
| А.65 #3.23 | Криптографічний ключ (ключ) | | Cryptographic key (key) | | Параметр криптографічного перетворення, який за умов належної процедури генерації та тестування забезпечує криптографічну стійкість перетворення. |
| А.66 #3.24 | Компонент криптографічного ключа (компонент | | Cryptographic key component (key component) | | Параметр, який використовується в поєднанні з іншими компонентами ключа у функції безпеки для формування КПБ у відкритому вигляді або для виконання криптографічної функції |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| | ключа) | | | | |
| A.67 #3.25 | Криптографічний модуль (модуль) | | Cryptographic module (module) | | Сукупність апаратного, програмного та/або вбудованого програмного забезпечення, яке реалізовує функції безпеки і міститься в межах криптосхеми |
| A.68 #3.41 | Код виявлення помилки | | Error detection code | EDC | Величина, обчислена з даних, що складається з надлишкових бітів інформації, призначених для виявлення, але не виправлення, ненавмисних змін в даних |
| A.69 #3.130 | Користувач | | User | | Роль особи чи процесу (суб'єкта), який діє від імені особи, яка отримує доступ до криптографічного модуля для використання криптографічних послуг |
| A.70 #3.21 | Межа криптосхеми | | Cryptographic boundary | | Однозначно визначений неперервний периметр, який встановлює фізичні та/або логічні межі усіх компонентів (множини компонентів апаратного, програмного або вбудованого програмного забезпечення) криптографічного модуля |
| A.71 #3.124 | Метод симетричної криптографії | | Symmetric cryptographic technique | | Метод криптографії, яка використовує один і той же секретний ключ як для зашифрування, так і для розшифрування |
| A.72 #3.71 | Мікрокод | | Microcode | | Інструкції процесора, які відповідають інструкції програми, що виконується, наприклад, код асемблеру. |
| A.73 #3.72 | Мінімальна ентропія | | Minimum entropy | | Нижня межа ентропії, яка є корисною при визначенні найгіршої оцінки ентропії вибірки |
| A.74 #3.44 | Модель скінченого автомату | MCA | Finite state model | FSM | Модель скінченого автомату, яка складається зі скінчених множин вхідного та вихідного алфавіту, скінченої множини станів, функції, яка відображає стани і вхід у вихід, функція, яка відображає стани і входи на стани (функція зміни станів), і |

Продовження додатка 1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | | | специфікації, яка описує початковий стан. |
| A.75 #3.73 | Модифікуємо операційне середовище | Modifiable operational environment | Операційне середовище, що допускає функціональні зміни, які можуть містити неконтрольоване (тобто ненадійне) програмне забезпечення. |
| A.76 #3.46 | Модуль вбудованого програмного забезпечення | Firmware module | Модуль, який складається виключно з вбудованого програмного забезпечення |
| A.77 #3.11 | Можливість обходу | Bypass capability | Наявність вразливості, яка створює передумови для часткового або повного ігнорування функції безпеки, включаючи криптографічні функції |
| A.78 #3.129 | Надійний канал | Trusted channel | Надійний та безпечний спосіб передачі між криптографічним модулем і відправником (одержувачем) незахищених КПБ, компонентів ключа і даних автентифікації. Надійні канали захищені від підслуховування, а також від фізичних або логічних маніпуляцій небажаними операторами/сутностями, процесами або іншими пристроями, між портами вводу або виводу модуля і вздовж лінії зв'язку до цільової точки. |
| A.79 #3.2 | Настанова адміністратора | Administrator guidance | Керівний документ який використовується оператором КЗІ та/або іншими адміністративними особами (ролями) для правильного конфігурування, технічного обслуговування та адміністрування криптографічного модуля |
| A.80 #3.77 | Неадміністративна настанова | Non-administrator guidance | Затверджений документ, що використовується користувачем і/або іншими не адміністративними ролями для експлуатації криптографічного модуля в затвердженому режимі. Ця настанова описує функції безпеки криптографічного модуля і |

Продовження додатка 1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | | | містить інформацію і процедури для безпечного його використання, у тому числі у вигляді інструкцій, правил і попереджень. |
| A.81 #3.82 | Непрозорий | Opaque | Непроникний для світла в видимій області спектру з довжиною хвилі від 50 нм до 400 нм. |
| A.82 #3.81 | Нормальне функціонування | Normal operation | Функціонування, при якому вся множина алгоритмів, функцій безпеки, послуг або процесів доступні і/або сконфігуровані |
| A.83 #3.14 | Обумовлене самотестування | Conditional self-test | Тестування власної працездатності та безпеки, що автоматично виконується криптографічним модулем у разі настання визначених для тестування умов |
| A.84 #3.66 | Обмежене операційне середовище | Limited operational environment | Операційне середовище, яке створене для визнання тільки контрольованих змін вбудованого програмного забезпечення, які успішно проходять тест завантаження програмного забезпечення/ вбудованого програмного забезпечення |
| A.85 #3.134 | Обнуління | Zeroisation | Найслабкіший метод знищення даних і незахищених ЧНБ з метою запобігання відновлення і повторного використання |
| A.86 #3.115 | Однокристальний криптографічний модуль | Single-chip cryptographic module | Фізичне вбудований в модуль однієї інтегральної мікросхеми яку можна використовувати як автономний пристрій або можна вбудувати в корпус чи продукт, які не можуть бути фізично захищені, зокрема, однокристальні чіпи (IC) або смарт-карти з однією мікросхемою. |
| A.87 #3.132 | Орган затвердження | Validation authority | Орган, що затверджує результати тестування на відповідність цьому регламенту |
| A.88 #3.85 | Оператор | Operator | Особа, яка уповноважена на виконання однієї або декількох ролей |
| A. 89 | Оператор | Crypto officer | Роль, яку виконує особа або процес (суб'єкт), що діє від імені |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| #3.19 | безпеки | | | | особи, яка звертається до криптографічного модуля для виконання криптографічної ініціалізації або функцій управління криптографічним модулем |
| A.90<br>#3.83 | Операційне середовище | | Operational | | Множина програмного та апаратного забезпечення, що складається з операційної системи та апаратної платформи, які потрібні для безпечної роботи модуля |
| A.91<br>#3.79 | Операційне середовище, що не модифікується | | Non-modifiable operational environment | | Операційне середовище, розробник якого не передбачив можливості зміни вбудованого програмного забезпечення |
| A.92<br>#3.4 | Орган затвердження | | Approval authority | | Орган / організація / установа, що уповноважена затверджувати та/або оцінювати функції безпеки |
| A.93<br>#3.87 | Пасивація | | Passivation | | Ефект реактивного процесу в напівпровідниках, поверхнях або компонентах і інтегральних схемах, що може змінити поведінку схеми.(?) |
| A.94<br>#3.88 | Пароль | | Password | | Послідовність символів, що використовується для автентифікації користувачів та визначення прав доступу. |
| A.95<br>#3.131 | Перевірено (затверджено) | | Validated | | Статус гарантування перевіреної відповідності органом затвердження |
| A.96<br>#3.89 | Персональний ідентифікаційний номер | | Personal identification number | PIN | Цифровий код, який використовується для автентифікації ролей |
| A.97<br>#3.133 | Постачальник | | Vendor | | Організація/ компанія, що має доступ до всієї документації та проектних даних незалежно від того, чи вони розробляли, чи ні криптографічний модуль,та надають його для тестування та затвердження. |
| A.98 | (Побічне) | ПЕМ | Electromagnetic | EME | Сигнал, що утворюється підчас роботи криптографічного |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| #3.33 | електромагнітне випромінювання | В | emanations | | модуля, перехоплення і аналіз якого потенційно дозволяє спростити задачу криптоаналізу, розкрити інформацію, яка передається, отримується, трактується або обробляється будь-яким обладнанням. |
| A.99 #3.28 | Погіршене функціонування | | Degraded operation | | Функціонування пристрою, коли підмножина множини алгоритмів, функцій безпеки, послуг або процесів доступні і/або сконфігуровані після відновлення з помилкового стану |
| A.100 #3.26 | Політика безпеки криптографічного модуля (політика безпеки) | | Cryptographic module security policy (security policy) | | Точна специфікація правил безпеки, які має виконувати криптографічний модуль під час виконання своїх функцій, охоплюючи правила, похідні від вимог цього регламенту та додаткових правил, накладених органом затвердження |
| A.101 #3.92 | Порт | | Port | | Точка фізичного/логічного входу або виходу криптографічного модуля, яка забезпечує доступ до модуля та охоплює відповідний роз'їм та електронну схему. |
| A.102 #3.111 | Послуга | | Service | | Операція, яка викликається ззовні оператором, і/або функція, яка може бути виконана криптографічним модулем/ |
| A.103 #3.94 | Приватний ключ | | Private key | | Один з пари асиметричних ключів криптографічного перетворення, який повинен використовуватися тільки відповідною особою – його власником. |
| A.104 #3.95 | Придатний до застосування | | Production-grade | | Продукт, компонент або програмне забезпечення, яке було перевірено на відповідність функціональній специфікації. |
| A.105 #3.60 | Прийнята ISO/IEC | | ISO/IEC adopted | | Функція безпеки, яка визначена в стандарті ISO/IEC ,або прийнята / рекомендується в стандарті ISO/IEC і визначена або в додатку до стандарту ISO/IEC або в документі, на який посилається стандарт ISO/IEC |
| A.106 | Програмне | ПЗ | Software | | Код, придатний до виконання криптографічним модулем, який |

Продовження додатка 1

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| #3.116 | забезпечення | | | | зберігається на носіях, які можуть видаляти дані. Цей код може бути динамічним і може змінюватися під час виконання у операційному середовищі, придатному до змін. |
| A.107 #3.117 | Програмний модуль | | Software module | | Модуль, який складається виключно з програмного забезпечення |
| A.108 #3.114 | Простий аналіз живлення | | Simple power analysis | SPA | Аналіз закономірностей виконання набору команд (або виконання окремих команд), щодо споживання електроенергії криптографічним модулем з метою отримання інформації, яка корелює з криптографічними операціями |
| A.109 #3.102 | Роль | | Role | | Атрибут безпеки, пов'язаний з користувачем, який визначає права доступу або обмеження користувача до послуг криптографічного модуля. З роллю можуть бути пов'язані одна або декілька послуг. Роль може бути пов'язана з одним або декількома користувачами і користувач може мати одну або декілька ролей. |
| A.110 #3.80 | Не релевантне до безпеки | | Non-security relevant | | Реалізоване у спосіб, який не заважає і не компрометує затверджене безпечне функціонування криптографічного модуля |
| A.111 #3.120 | Розділення знання | | Split knowledge | | Процес, в якому деякий секрет (ключ) розбивається на кілька компонентів, окремо не розділяючи знання первісного ключа, які можуть бути згодом введені в криптографічний модуль або із криптографічного модуля окремими особами і в поєднанні відтворюють первісний криптографічний ключ. |
| A.112 #3.32 | Розчленований підпис | | Disjoint signature | | Один або декілька підписів, які разом представляють всю структуру коду |
| A.113 | Роль технічного | | Maintenance role | | Роль особи, яка виконує технічне обслуговування та/або |

Продовження додатка 1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| #3.68 | обслуговування | | логічне обслуговування та діагностику апаратного та/або програмного забезпечення. |
| A.114 #3.69 | Ручний | Manual | Метод, що вимагає втручання людини-оператора. |
| A.115 #3.123 | Стійкість (криптографічна) | Strong | Здатність криптосистеми, криптографічного модуля або окремого крипто алгоритму протистояти атакам, що спрямовані на порушення конфіденційності, цілісності та автентичності інформації, яка захищається |
| A.116 #3.108 | Самотестування | Self-test | Доексплуатаційне або обумовлене тестування, що автоматично виконується криптографічним модулем |
| A.117 #3.105 | Секретний ключ | Secret key | Криптографічний ключ, що використовується криптографічним алгоритмом з секретним ключем, який однозначно пов'язаний з одним або декількома сутностями і повинен зберігатися у таємниці. |
| A.118 #3.104 | Середовище виконання | Runtime environment | Середовище комп'ютера, яке надає послуги для процесів або програм під час роботи комп'ютера. Це може відноситися до самої операційної системи або програмного забезпечення, що працює нижче неї. |
| A.119 #3.12 | Сертифікат | Certificate | 1. Дані об'єкта, що не піддаються підробці завдяки використанню приватного (секретного) ключа органу сертифікації,<br>2. Документ, що виданий уповноваженим органом, який підтверджує відповідність продукту / послуги вимогам нормативних документів (стандартів) |
| A.120 #3.97 | Сертифікат відкритого ключа | Public key certificate | Дані про відкритий ключ особи, що підписані центром сертифікації ключів, який сформував цей сертифікат |

Продовження додатка І

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| А.121 #3.16 | Система управління конфігурацією, | | Configuration management system | CMS | Управління особливостями і гарантіями безпеки за допомогою контролювання змін, що вносяться у апаратне обладнання, програмне забезпечення і документацію криптографічного модуля |
| А.122 #3.1 | Список контролю доступу | СКД | Access control list | ACL | Список дозволів для надання доступу до об'єкта |
| А.123 #3.43 | Стимулювання збою | | Fault induction | | Метод наведення змін в операційній поведінці апаратних засобів шляхом застосування методів впливу фізичних полів та умов застосування. |
| А.124 #3.37 | Сутність | | Entity | | Людина, група, пристрій або процес |
| А.125 #3.118 | Тестування завантаження програмного забезпечення /вбудованого програмного забезпечення | | Software / firmware load test | | Множина тестів, що виконуються програмним забезпеченням або вбудованим програмним забезпеченням, які необхідно успішно пройти, перш ніж воно буде виконане криптографічним модулем. Не застосовується, якщо програмне забезпечення або вбудоване програмне забезпечення є повною заміною знімку і виконується тільки після увімкнення живлення модуля. |
| А.126 #3.49 | Твердість | | Hard/hardness | | Відносний опір матеріалу з якого зроблений захисний кожух до нарізки, подряпин або вигину. |
| А.127 | Тематичні дослідження | | Special research | | Дослідження криптографічних, інженерно-криптографічних та спеціальних властивостей криптографічних модулів з метою їх допуску до експлуатації. |
| А.128 #3.40 | Тестування відмов, спричинених | ТВС | Environmental failure testing | EFT | Використання конкретних методів для забезпечення достатньої впевненості у захисті від компрометації безпеки криптографічного модуля, спричиненої змінами середовища, |

Продовження додатка 1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | середовищем | | які не відповідають вимогам типового робочого діапазону модуля. |
| A.129 #3.67 | Тестування низького рівня | Low-level testing | Тестування окремих компонентів або груп компонентів криптографічного модуля і їх фізичних портів і логічних інтерфейсів |
| A.130 #3.65 | Транспортування ключа | Key transport | Процес передачі ключа від однієї сутності до іншої за допомогою автоматизованих методів. |
| A.131 #3.61 | Узгодження ключів | Key agreement | Процедура створення ЧПБ, при якій результуючий ключ є функцією інформації від двох або декількох учасників, яка гарантує, що жодна із сторін, використовуючи автоматичні методи ,не може визначити наперед значення ключа, незалежно від вкладу іншого учасника. |
| A.132 #3.90 | Фізичний захист | Physical protection | Сукупність засобів фізичного захисту криптографічного модуля, та його КПБ і ВПБ. |
| A.133 #3.47 | Функціональна специфікація | Functional specification | Високорівневий опис портів і інтерфейсів, видимих оператору, та високорівневий опис поведінки криптографічного модуля. |
| A.134 #3.48 | Функціональне тестування | Functional testing | Тестування функцій криптографічного модуля, визначених у функціональній специфікації. |
| A.135 #3.106 | Функція безпеки | Security function | Затверджені уповноваженим органом криптографічні алгоритми з симетричними або асиметричними ключами, коди автентифікації повідомлень, геш-функції або інші функції безпеки, генератори випадкових бітів, автентифікація сутності і генерація ЧПБ. |
| A.136 #3.58 | Цілісність | Integrity | Властивість, що дані не були змінені або видалені у несанкціонований і невиявлений спосіб. |
| A.137 | Червона/ чорна | Red/ black | Поділ сукупності електронних компонентів та провідників, що |

Продовження додатка І

| 1 | 2 | | 3 | | 4 |
|---|---|---|---|---|---|
| | зона (засобу КЗІ) | | separation | | їх з'єднують, засобу КЗІ на дві зони:<br>Червону – в якій циркулює (може циркулювати) у відкритому вигляді інформація з обмеженим доступом (чутливі дані) та чутливі параметри безпеки, а також<br>Чорну – в якій, не присутні сигнали чутливих параметрів або чутливої інформації. |
| A.138<br>#3.109 | Чутливі дані | | Sensitive data | | Дані користувачів, що потребують захисту. |
| A.139<br>#3.110 | Чутливі параметри безпеки | ЧПБ | Sensitive security parameters | SSP | Критичні параметри безпеки (КПБ) і відкриті параметри безпеки (ВПБ). |
| A.140<br>#3.27 | Шлях даних | | Data path | | Фізичний або логічний шлях, по якому передаються дані, при цьому, фізичний шлях даних може використовуватися декількома логічними шляхами. |
| A.141<br>#3.128 | Якір довіри | | Trust anchor | | Надійна інформація, яка охоплює алгоритм з відкритим ключем, значення відкритого ключа, назву емітента і, опціонально, інші параметри. Деякі параметри можуть охоплювати період чинності, але не обмежуватись ним. Якір довіри може бути наданий у вигляді самопідписаного сертифіката. |

Додаток 2
Технічного регламенту засобів криптографічного захисту інформації

**Вимоги**
**до засобів криптографічного захисту інформації, їх проектування і виготовлення, оцінки відповідності та аудиту**

## 1. Вимоги безпеки (суттєві вимоги) до криптографічних модулів

### 1.1. Рівні безпеки криптографічних модулів

Надалі наведено короткий огляд чотирьох рівнів безпеки криптографічних модулів. Типові приклади, що наведені у стандарті ДСТУ ISO/IEC 19790 слугують для ілюстрації того, як вимоги можуть бути задоволені, та не обмежують розробників криптографічних модулів та тестувальників і не є вичерпними.

Залежно від виду інформації, яка захищається, та умов застосування криптографічних модулів до них можуть висуватися наступні групи суттєвих вимог: криптографічні - математичні вимоги щодо застосованих перетворень, інженерно-криптографічні - вимоги щодо гарантоздатності технічної реалізації, організаційно-технічні - вимоги щодо фізичної безпеки та спеціальні – вимоги щодо блокування/ придушення ПЕМВ. При цьому криптографічні вимоги ідентичні для всіх чотирьох рівнів безпеки.

З урахуванням моделі загроз, кожен наступний рівень безпеки висуває додатковий комплекс вимог щодо захисту самого модуля (наприклад, можливість доступу порушника та його знання внутрішніх компонентів і специфіки експлуатації) і ЧПБ, які містяться і контролюються в межах криптосхеми модуля. Визначення суттєвих вимог до криптографічних модулів, схвалення (затвердження) функцій безпеки, включаючи криптографічні алгоритми та генератори випадкових біт, здійснюється спеціально уповноваженим органом у галузі зв'язку та захисту інформації.

#### 1.1.1. Рівень безпеки 1

Рівень безпеки 1 забезпечує початковий рівень захисту та встановлює базові вимоги безпеки для криптографічного модуля (наприклад, повинні використовуватися щонайменше одна схвалена функція безпеки або схвалений метод створення конфіденційного параметру безпеки).

На цьому рівні модулі, що виконані у вигляді програмного забезпечення або вбудованого програмного забезпечення, можуть працювати в незмінному, обмеженому або змінному операційному середовищі.

Від апаратного криптографічного модуля рівня безпеки 1 не вимагаються конкретні механізми забезпечення фізичної безпеки поза межами основних вимог для промислових компонентів. Задокументовано реалізовані методи послаблення атак без підключення до криптографічного модуля та інших атак. Прикладами криптографічного модуля із рівнем безпеки 1 є апаратне шифрування у персональному комп'ютері (ПК) або криптографічний інструментарій портативного пристрою або комп'ютера загального призначення.

Такі реалізації більш підходять для практичних застосувань, коли заходи безпеки,такі як фізична безпека, мережева безпека та адміністративні процедури надаються за межами модуля, але в середовищі, в якому він функціонує. Зокрема, реалізація криптографічного модуля із рівнем безпеки 1 може бути економічно більш ефективною, ніж відповідний модуль з більш високим рівнем гарантій, який забезпечує вищий рівень безпеки ЧПБ модулів, що дозволяє вибирати альтернативні криптографічні рішення для задоволення вимог безпеки, де увага до середовища модуля має вирішальне значення для забезпечення загальної безпеки.

### 1.1.2. Рівень безпеки 2

Рівень безпеки 2 посилює механізми фізичної безпеки рівня безпеки 1, додавши вимогу наявності доказів спроб несанкціонованого доступу до криптосхеми, шляхом використання захисного кожуху, або розміщення на панелях (дверцятах), що знімаються, модуля контрольних печаток (пломб) чи стійких до перебору замків.

Захисний кожух (покриття) для виявлення несанкціонованого доступу до криптосхеми або печатки розташовуються на модулі так, щоб спроба фізичного доступу до ЧПБ всередині модуля неодмінно призведе до їх пошкодження.

На цьому рівні безпеки до криптографічного модуля також висувається вимога автентифікації оператора (особи) для виконання певної ролі та надання відповідної множини послуг.

Рівень безпеки 2 дозволяє програмному криптографічному модулю працювати в середовищі, що змінюється, за умов реалізації контролю доступу на основі ролей, або, як мінімум, дискреційного контролю доступу з надійним механізмом визначення нових груп і призначення обмежених прав доступу

через списки контролю доступу з можливістю присвоєння кожному користувачеві більш ніж однієї групи. Зазначена вимога спрямована на захист криптографічного програмного забезпечення від несанкціонованого виконання, модифікації і читання. За суттю рівень безпеки 2 є найвищим рівнем безпеки програмного криптографічного модуля.

**1.1.3. Рівень безпеки 3**

На додаток до механізмів фізичної безпеки, що визначені на рівні безпеки 2 та надають докази спроб вторгнення, на рівні безпеки 3 висуваються додаткові вимоги для послаблення наслідків несанкціонованого доступу до ЧПБ модуля.

На рівні безпеки 3 мають бути реалізовані механізми фізичної безпеки, що забезпечують високу ймовірність виявлення та реагування на спроби фізичного вторгнення, використання або модифікації криптографічного модуля, зокрема, шляхом зондування через вентиляційні отвори або прорізи. Механізми фізичної безпеки можуть охоплювати використання міцних корпусів і схем виявлення/протидії зламу, які обнуляють КПБ, коли відчиняють знімні корпуси/дверцята криптографічного модуля.

Рівень безпеки 3 вимагає механізмів автентифікації, які ґрунтуються на ідентичності особи, посилюючи безпеку механізмів аутентифікації на основі ролей, визначених для рівня безпеки 2. Криптографічний модуль встановлює справжність ідентичності оператора і перевіряє, що ідентифікований оператор має визначену роль і уповноважений виконувати відповідну множину послуг.

Рівень безпеки 3 вимагає для вводу чи виводу встановлених вручну у відкритому вигляді КПБ, їх шифрування, використання надійного каналу або використання процедури поділу знань.

На рівні безпеки 3 також вимагається захист криптографічного модуля від компрометації його безпеки внаслідок навмисних змін характеристик середовища функціонування, виходу поза межі нормальних робочих діапазонів напруги і температури. Умисні дії за межами нормальних діапазонів можуть бути використані зловмисником, щоб перешкодити захисту криптографічного модуля. Криптографічний модуль має містити спеціальні функції захисту середовища, призначені для виявлення недопустимих значень напруги і температури, які обнуляють КПБ, або виконують обумовлене тестування для забезпечення впевненості у надійності модуля, що працює за межами нормального робочого діапазону.

Методи послаблення атак без підключення до модуля (неінвазивні атаки), які реалізовані в модулі, мають бути протестовані у відповідності до метрик рівня безпеки 3.

Для рівня безпеки 3 всіма розділами стандарту ISO/IEC 19790 не рекомендується програмна реалізація криптографічних модулів, а отже найвищим рівнем безпеки програмного криптографічного модуля є рівень безпеки 2.

На рівні безпеки 3 вимагаються додаткові гарантії життєвого циклу модуля, такі як автоматизоване управління конфігурацією, детальне проектування, тестування низького рівня і автентифікація оператора із використанням інформації автентифікації, наданої постачальником.

**1.1.4. Рівень безпеки 4**

Рівень безпеки 4 є найвищим рівнем, який визначений у стандарті ISO/IEC 19790. Цей рівень охоплює всі вимоги безпеки більш низьких рівнів, а також включає додаткові (розширені) умови.

На рівні 4 механізми фізичної безпеки повинні забезпечувати навколо криптографічного модуля, що містить ЧПБ (параметри завантажені в модуль), повну оболонку захисту з метою виявлення та реагування на всі спроби несанкціонованого фізичного доступу із врахуванням чи без врахування застосування зовнішньої міцності. При цьому забезпечується максимальна ймовірність виявлення вторгнення, що призводить до миттєвого обнуління всіх незахищених ЧПБ. Застосування криптографічних модулів із рівнем безпеки 4 є бажаним для роботи у фізично незахищеному середовищі.

Рівень безпеки 4 висуває вимогу багатофакторної автентифікації оператора, як мінімум, шляхом застосування двох з трьох наведених атрибутів:

знання певної інформації, наприклад, секретного паролю;

володіння певним пристроєм, наприклад, фізичним ключем (токеном);

наявність фізичної властивості, наприклад, застосування біометрики.

Криптографічний модуль із Рівнем безпеки 4 має містити спеціальні функції захисту середовища, призначені для виявлення недопустимих значень напруги і температури, які обнулюють КПБ для забезпечення впевненості у надійності модуля, який працює за межами нормального робочого діапазону. Методи послаблення атак без підключення до модуля (неінвазивні атаки), , які реалізовані в модулі, мають бути протестовані у відповідності до метрик рівня безпеки 4.

Для модулі рівня безпеки 4 не виконуються у програмні реалізації.

Проектування модуля із рівнем безпеки 4 перевіряється на відповідність між незмінністю станів і функціональною специфікацією.

### 1.2. Загальні вимоги до криптографічних модулів

1.2.1 (Рівні 1-4) Для криптографічного модуля, який має пройти незалежну верифікацію або схему оцінювання, надається вся документація, в тому числі настанови користувача і інсталяції, проектна документація, документація життєвого циклу.

### 1.3. Специфікація криптографічного модуля

1.3.1. (Рівні 1-4) Криптографічний модуль складається з множини апаратних засобів, програмного забезпечення, вбудованого програмного забезпечення або будь-якої їх комбінації, яка, як мінімум, реалізовує визначену криптографічну послугу, що використовує затверджений криптографічний алгоритм, функцію безпеки або процес і міститься в межах криптосхеми.

1.3.2. (Рівні 1-4) Повинні бути явно визначені межі і суть криптографічної схеми (як сукупності усіх криптоперетворень), реалізованої множиною апаратних, апаратно-програмних и програмних компонентів криптомодуля .

1.3.3. (Рівні 1-4) Оператор повинен мати можливість експлуатувати модуль в затвердженому режимі роботи.

1.3.4. (Рівні 1-4) Затверджений режим роботи повинен визначатись як множина послуг, яка охоплює принаймні одну послугу, що використовує схвалений (рекомендований) криптографічний алгоритм, функцію безпеки або процес.

1.3.5. (Рівні 1-4) Входження в стан погіршеного функціонування має відбуватися тільки після виходу зі стану помилки.

1.3.6. (Рівні 1-4) Модуль повинен надавати інформацію про його стан під час переконфігурування і входження у стан погіршеного функціонування.

1.3.7. (Рівні 1-4) Механізм або функція, які є джерелом помилки, мають бути ізольовані.

1.3.8. (Рівні 1-4) Усі обумовлені самотестування алгоритму повинні бути виконані до першого експлуатаційного використання криптографічного алгоритму після входження в стан погіршеного функціонування.

1.3.9. (Рівні 1-4) Послуги мають вказати на спроби використовувати неробочий алгоритм, функцію безпеки або процес.

1.3.10. (Рівні 1-4) Криптографічний модуль має залишатися в стані погіршеного функціонування доти, поки криптографічний модуль успішно проходитеме усі доексплуатаційні самотестування.

1.3.11. (Рівні 1-4) Якщо криптографічному модулю не вдається успішно пройти доексплуатаційне самотестування, модуль не повинен входити у стан погіршеного функціонування.

### 1.4. Інтерфейси криптографічного модуля

1.4.1. (Рівні 1-4) Криптографічний модуль має обмежити всі логічні потоки інформації лише до тих фізичних точок доступу і логічних інтерфейсів, які визначені як точки вводу у межу і виводу з межі криптосхеми модуля.

1.4.2. (Рівні 1-4) Криптографічний модуль має мати такі п'ять інтерфейсів "вводу" і "виводу":

1.4.3. (Рівні 1-4) *Інтерфейс вводу даних.* Усі дані (за винятком команд управління, що вводяться через інтерфейс вводу цих команд), які вводяться у криптографічний модуль і обробляються ним (у тому числі дані у відкритому вигляді, зашифровані дані, ЧПБ, а також інформація про стан модуля) мають вводитися через інтерфейс "вводу даних ". Дані можуть бути прийняті модулем через інтерфейс вводу даних на вході при виконанні самотестування.

1.4.4. (Рівні 1-4) *Інтерфейс виводу даних.* Усі дані (за винятком виводу даних стану через інтерфейс виводу даних стану і виводу команд управління через інтерфейс виводу команд управління), які виводяться з криптографічного модуля (у тому числі дані у відкритому вигляді, зашифровані дані і ЧПБ) мають виводитись через інтерфейс "виводу даних".

1.4.5. (Рівні 1-4) Усі дані, які проходять через інтерфейс "виводу даних" мають бути заборонені під час виконання ручного вводу, доексплуатаційного самотестування, завантаження і обнуління програмного забезпечення/ вбудованого програмного забезпечення; або коли криптографічний модуль знаходиться в помилковому стані.

1.4.6. (Рівні 1-4) *Інтерфейс вводу команд управління.* Усі вхідні команди, сигнали (наприклад, годинник) і дані управління (у тому числі, виклики функцій і ручне керування, такі як перемикачі, кнопки і клавіші), що використовуються для керування роботою криптографічного модуля, мають вводитися через інтерфейс "ввід управління"

1.4.7. (Рівні 1-4) *Інтерфейс виводу команд управління.* Всі вихідні команди, сигнали і дані управління (наприклад, команди управління іншим

модулем), які використовуються для керування роботою криптографічного модуля або вказування його стану, мають виводитися через інтерфейс "вивід управління".

1.4.8. (Рівні 1-4) Вивід усіх команд управління через інтерфейс "вивід управління" має бути заборонений, якщо криптографічний модуль знаходиться в помилковому стані, за винятком ситуацій, які явно визначені і задокументовані у політиці безпеки.

1.4.9. (Рівні 1-4) *Інтерфейс виводу статусу.* Усі вихідні сигнали, індикатори (наприклад, індикатор помилки, і дані про статус (у тому числі коди повернення і фізичні показники, такі як візуальні (дисплей, індикаторні лампи), аудіо (зумер, тон, дзвоник) і механічні (вібрація)), що використовуються для вказування статусу криптографічного модуля, мають виводитися через інтерфейс "виводу статусу". Вивід статусу може бути явним чи неявним.

1.4.10. (Рівні 1-4) Програмні криптографічні модулі також повинні мати такий інтерфейс:

1.4.11. (Рівні 1-4) *Інтерфейс живлення.* Все зовнішнє живлення, яке вводиться в криптографічний модуль, повинне вводитися через інтерфейс живлення. Інтерфейс живлення не потрібен, коли все живлення забезпечується або підтримується всередині самого криптографічного кордону криптографічного модуля (наприклад, внутрішня батарея).

1.4.12. (Рівні 1-4) Криптографічний модуль має розділяти вхідні дані, інформацію управління і живлення,з вихідними даними, вихідною інформацією управління, інформацією статусу і виходом живлення.

1.4.13. (Рівні 1-4) Специфікація криптографічного модуля має однозначно визначити формат вхідних даних і інформації управління, у тому числі обмеження довжини для всіх входів змінної довжини.

1.4.14. (Рівні 3,4) Для передачі незахищених (у відкритому вигляді) КПБ, компонентів ключів і даних автентифікації між криптографічним модулем та точками відправника або отримувача криптографічний модуль має реалізувати надійний канал.

1.4.15. (Рівні 3,4) Надійний канал має запобігати несанкціонованій модифікації та розкриттю інформації що передається.

1.4.16. (Рівні 3,4) Фізичні порти, що використовуються для надійного каналу, мають бути фізично відокремлені від усіх інших портів.

1.4.17. (Рівні 3,4) Логічні інтерфейси, які використовуються для надійного каналу, мають бути логічно відокремлені від усіх інших інтерфейсів.

1.4.18. (Рівні 3,4) Автентифікація на основі ідентичності має використовуватися для всіх послуг надійного каналу.

1.4.19. (Рівні 3,4) Повинен бути наданий індикатор використання надійного каналу.

1.4.20. (Рівень 4) На додаток до вимог безпеки рівня 3 на рівні безпеки 4 для всіх послуг, які використовують надійний канал, має застосовуватися багатофакторна автентифікація на основі ідентичності.

### 1.5. Ролі, послуги і автентифікація

1.5.1. (Рівні 1-4) Криптографічний модуль має підтримувати санкціоновані ролі для операторів і відповідних послуг в рамках кожної ролі.

1.5.2. (Рівні 1-4) Криптографічний модуль має], як мінімум, підтримувати роль оператора безпеки (Crypto Officer Role).

1.5.3. (Рівні 1-4) Роль оператора безпеки має припускати здійснення криптографічної ініціалізації або функції менеджменту і загальних послуг безпеки (наприклад, ініціалізації модуля, менеджменту КПБ, ВПБ і функцій аудиту).

1.5.4. (Рівні 1-4) Якщо криптографічний модуль підтримує роль користувача, то ця роль має припускати здійснення загальних послуг безпеки , у тому числі криптографічних операцій та інших схвалених функцій безпеки

1.5.5. (Рівні 1-4) Криптографічний модуль має операторам надавати такі послуги.

1.5.6. (Рівні 1-4) *Відобразити інформацію про версію модуля.* Криптографічний модуль має вивести назву або ідентифікатор модуля і інформацію про версію, які можуть бути пов'язані із записом затвердження (наприклад, інформацію про версію апаратного забезпечення, програмного забезпечення та/або вбудованого програмного забезпечення).

1.5.7. (Рівні 1-4) *Відобразити статус.* Криптографічний модуль має вивести поточний статус. Він може охоплювати вивід індикаторів статусу у відповідь на запит послуги.

1.5.8. (Рівні 1-4) *Виконати самотестування.* Криптографічний модуль має ініціювати і запустити *доексплуатаційне самотестування.*

1.4.9. (Рівні 1-4) *Виконати схвалені функції безпеки.* Криптографічний модуль має виконати принаймні одну схвалену функцію безпеки, що використовується в схваленому режимі.

1.5.10. (Рівні 1-4) *Виконати обнуління.* Криптографічний модуль має виконати обнуління параметрів.

1.5.11. (Рівні 1-4) Якщо модуль може виводити певну інформацію або елемент статусу в криптографічно захищеному вигляді або (як результат конфігурації модуля або втручання оператора) також може виводити елемент в не захищеному вигляді, то має бути визначена можливість обходу.

1.5.12. (Рівні 1-4) Якщо криптографічний модуль реалізує можливість *обходу*, то до конфігурування можливості обходу оператор повинен мати санкціоновану роль.

1.5.13. (Рівні 1-4) Якщо криптографічний модуль реалізує можливість обходу, то для активізації можливості запобігти випадковому обходу відкритих даних через помилку повинні бути виконаними дві незалежні внутрішні дії.

1.5.14. (Рівні 1-4) Якщо криптографічний модуль реалізує можливість обходу, то дві незалежні внутрішні дії повинні змінити програмне забезпечення й/або поведінку апаратного забезпечення для налаштування можливості обходу (наприклад, встановлення двох різних програмних або апаратних прапорів, один з яких може бути встановлений користувачем).

1.5.15. (Рівні 1-4) Якщо криптографічний модуль реалізує можливість обходу, то модуль повинен відобразити статус можливості обходу:

1) *не активований*, модуль виключно надає послуги *з* криптографічною обробкою (наприклад, відкриті дані *шифруються*); або

2) *активний*, модуль виключно надає послуги *без* криптографічної обробки (наприклад, відкриті дані *не* шифруються); або

3) *поперемінно* включається і вимикається, модуль надає деякі послуги *з* криптографічною обробкою та деякі послуги *без* криптографічної обробки (наприклад, для модулів з декількома каналами зв'язку, відкриті дані *шифруються* або *не* шифруються залежно від конфігурації кожного каналу).

1.5.16. (Рівні 1-4) Якщо криптографічний модуль реалізує можливість *самоініційованого криптографічного виводу*, то модуль повинен відобразити статус, що вказуватиме, чи активована можливість самоініційованого криптографічного виводу.

1.5.17. (Рівні 1-4) Якщо криптографічний модуль має можливість завантаження програмного забезпечення або вбудованого програмного забезпечення із зовнішнього джерела, то для гарантування придатності перед завантаженням завантажуване програмне забезпечення або вбудоване програмне забезпечення має пройти затвердження органом затвердження.

1.5.18. (Рівні 2-4) *Автентифікація* на основі ролей. Якщо цей механізм підтримується криптографічним модулем, модуль має] вимагати наявність у оператора однієї або декількох ролей.

1.5.19. (Рівні 3,4) Автентифікація на основі ідентичності. Якщо цей механізм підтримується криптографічним модулем, модуль має вимагати однозначну індивідуальну ідентифікацію оператора.

1.5.20. (Рівні 1-4) Коли криптографічний модуль скидається, перезавантажується, вимикається, а потім вмикається, модуль має вимагати від оператора автентифікації.

1.5.21. (Рівні 1-4) Дані автентифікації, що знаходяться всередині криптографічного модуля, мають бути захищені від несанкціонованого використання, розкриття, модифікації і заміни.

1.5.22. (Рівні 2-4) Якщо криптографічний модуль не містить даних автентифікації, необхідних для першої автентифікації оператора при доступі до модуля, то інші санкціоновані методи (наприклад, процедурні заходи або використання встановлених виробником даних автентифікації або даних автентифікації за промовчанням) мають використовуватися для контролю доступу до модуля і ініціалізації його механізмів автентифікації.

1.5.23. (Рівні 2-4) Якщо для контролю доступу до модуля використовуються дані автентифікації за промовчанням, то ці дані автентифікації мають бути замінені при першій автентифікації.

1.5.24. (Рівні 2-4) Якщо криптографічний модуль використовує функції безпеки для автентифікації оператора, то ці функції безпеки повинні бути схваленими функціями безпеки.

1.5.25. (Рівні 2-4) Зворотній зв'язок від даних автентифікації до оператора не має бути неясним під час процесу автентифікації (наприклад, не видно відображення символів при введенні пароля).

### 1.6. Безпека ПЗ/ВПЗ

1.6.1. (Рівні 1-4) Криптографічний механізм, який використовує схвалені методики забезпечення цілісності має застосовуватись для всіх компонентів ПЗ

і ВПЗ у визначеному криптографічному кордоні модуля у один із таких способів:

самим криптографічним модулем; або

іншим затвердженим криптографічним модулем, що працює в схваленому режимі роботи.

1.6.2. (Рівні 2-4) Компоненти ПЗ та ВПЗ криптографічного модуля мають охоплювати тільки код, здатний до виконання (наприклад, це не початковий код, об'єктний код або код, здатний до компіляції за першої необхідності).

1.6.3. (Рівні 2-4) Схвалені цифрові підписи або код автентифікації повідомлення із ключем мають] застосовуватись для всього ПЗ і ВПЗ у визначеному криптографічному кордоні модуля.

1.6.4. (Рівні 3,4) Криптографічний механізм, який використовує схвалені цифрові підписи має застосовуватись для всіх компонент ПЗ і ВПЗ у визначеному криптографічному кордоні модуля.

1.6.5. (Рівні 3,4) Якщо обчислений результат не дорівнює згенерованому раніше результату, тест - не успішний, і модуль має увійти в помилковий стан.

1.6.6. (Рівні 3,4) Приватний ключ підпису має зберігатися за межами модуля.

### 1.7. Операційне середовище

1.7.1. (Рівень 2) Все криптографічне ПЗ, ЧПБ і інформація управління та статусу мають контролюватися операційною системою, яка реалізовує контроль доступу на основі ролей, або, як мінімум, вибірковий контроль доступу з надійним механізмом визначення нових груп і призначення обмежених прав доступу через списки контролю доступу, і з можливістю долучення кожного користувача до більш ніж однієї групи.

1.7.2. (Рівень 2) Операційна система має бути сконфігурованою для захисту від несанкціонованого виконання, модифікації і читання ЧПБ, даних управління і стану.

1.7.3. (Рівень 2) Операційна система має завадити процесам користувачів отримати доступ на читання або запис до ЧПБ, які перебувають у власності інших процесів, і до ЧПБ системи.

### 1.8. Фізична безпека

1.8.1. (Рівні 1-4) Криптографічний модуль має застосувати при інсталяції механізми фізичної безпеки з метою обмеження несанкціонованого фізичного

доступу до вмісту модуля та недопущення несанкціонованого використання або модифікації модуля (включаючи заміну всього модуля).

1.8.2. (Рівні 1-4) Залежно від механізмів фізичної безпеки криптографічного модуля, несанкціоновані спроби фізичного доступу, використання або модифікації повинні мати високу ймовірність виявлення:

1.8.3. (Рівні 1-4) після спроби через залишення видимих слідів (тобто доказів спроб зламу) та при спробі доступу і відповідні негайні дії мають бути виконані криптографічним модулем для захисту КПБ.

1.8.4. (Рівні 1-4) Коли виконується обнуління для цілей фізичної безпеки, то обнуління має бути виконане за досить малий період часу з метою запобігання відновлення конфіденційних даних між часом виявлення і фактичним обнулінням.

1.8.5. (Рівні 1-4) Якщо модуль охоплює роль обслуговування, що вимагає фізичного доступу до вмісту модуля, або, якщо модуль спроектований з можливістю отримати фізичний доступ (наприклад, за допомогою постачальника модуля або іншої уповноваженої особи), то має бути визначений інтерфейс доступу для обслуговування.

1.8.6. (Рівні 1-4) Інтерфейс доступу для обслуговування має охоплювати всі фізичні шляху доступу до вмісту криптографічного модуля, у тому числі будь-які знімні кришки або дверцята.

1.8.7. (Рівні 1-4) Будь-які знімні кришки або дверцята, включені в інтерфейс доступу для обслуговування, мають бути захищені за допомогою відповідних механізмів фізичної безпеки.

1.8.8. (Рівень 3) Тестування середовища на наявність збоїв (ТВС) має охоплювати поєднання аналізу, моделювання і тестування криптографічного модуля з метою забезпечення розумної впевненості в тому, що умови середовища стосовно температури і напруги, які (випадково або навмисно) знаходяться за межами нормальних робочих діапазонів модуля, не скомпрометують його безпеку.

### 1.9. Безпека проти атак без підключення

1.9.1. (Рівні 1-4) Для рівнів безпеки 1 та 2, документація має містити всі методи послаблення, що використовуються для захисту КПБ модуля від методів запобігання атак без підключення (неінвазивних).

1.9.2. (Рівні 1-4) Документація має містити докази ефективності кожного з методів запобігання атакам.

**1.10. Керування чутливими параметрами безпеки**

1.10.1. (Рівні 1-4) КПБ мають бути захищені в модулі від несанкціонованого доступу, використання, розголошення, зміни і заміни.

1.10.2. (Рівні 1-4) Модуль має зв'язати згенерований, введений у модуль або виведений із модуля ЧПБ, із сутністю (тобто людиною, групою, роллю або процесом), для якої призначений ЧПБ.

1.10.3. (Рівні 1-4) Геш-значення паролів, інформація про стан ГВБ і проміжні значення генерації ключа, мають вважатися КПБ.

1.10.4. (Рівні 1-4) Якщо схвалена функція безпеки, генерація ЧПБ або метод встановлення ЧПБ вимагають випадкових значень, то для надання цих значень має використовуватися затверджений ГВБ.

1.10.5. (Рівні 1-4) Якщо ентропія збирається поза межами кордону криптографічного модуля, потік даних, який генерується з використанням введення цієї ентропії, має вважатися КПБ.

1.10.6. (Рівні 1-4) Всі криптографічно захищені ЧПБ, що вводяться в модуль або виводяться із модуля, мають бути зашифровані з використанням схваленої функції безпеки.

1.10.7. (Рівні 1-4) Введені напряму (у відкритому або зашифрованому вигляді) ЧПБ мають перевірятися під час введення в модуль для точності, використовуючи тест обумовленого ручного введення.

1.10.8. (Рівень 3) Якщо модуль використовує процедури поділу знань, модуль має окремо використовувати автентифікацію оператора, яка ґрунтується на ідентичності, для вводу або виводу кожного компонента ключа і, принаймні два компоненти ключа повинні існувати, щоб відновити початковий криптографічний ключ.

1.10.9. (Рівні 1-4) ЧПБ у модулі можуть зберігатися у відкритому чи зашифрованому вигляді. Модуль має зв'язати кожен ЧПБ, який зберігається у ньому, з сутністю (наприклад, оператором, роллю або процесом), до якої відноситься ЧПБ.

1.10.10. (Рівні 1-4) Доступ неавторизованих осіб до КПБ, які зберігаються у відкритому вигляді, повинен бути заборонений.

1.10.11. Модифікація ЧПБ неавторизованим особами має бути заборонена.

1.10.12. Модуль має забезпечити методи обнуління всіх незахищених ЧПБ і компонентів ключа в модулі. Тимчасово збережені ЧПБ та інші збережені значення, що належать модулю, повинні бути обнулені, коли вони більше не потрібні для використання в майбутньому.

1.10.13. Обнулені ЧПБ не повинні відновлюватися або бути здатними до багаторазового використання.

**1.11. Самотестування**

1.11.1. (Рівні 1-4) Всі самотестування мають виконуватися.

1.11.2. (Рівні 1-4) Визначення успішності або не успішності має виконуватися модулем без зовнішнього контролю, зовнішнього введення текстових векторів, очікуваних результатів на виході, втручання оператора або, чи буде модуль працювати в затвердженому або не затвердженому режимі.

1.11.3. (Рівні 1-4) Доексплуатаційне самотестування має бути успішно виконане до виводу модулем даних через інтерфейс виводу даних.

1.11.4. (Рівні 1-4) Обумовлені самотестування мають виконуватися, коли викликається застосовна функція безпеки або процес (тобто функції безпеки, для яких необхідне самотестування).

1.11.5. (Рівні 1-4) Всі самотестування, що містяться в основних алгоритмічних стандартах, мають бути реалізовані у криптографічному модулі.

1.11.6. (Рівні 1-4) Якщо криптографічний модуль не проходить самотестування, модуль має перейти в помилковий стан.

1.11.7. (Рівні 1-4) Якщо криптографічний модуль не проходить самотестування, модуль має вказати на помилку.

1.11.8 (Рівні 1-4) Криптографічний модуль в стані помилки не має виконувати криптографічні операції або виводити команди управління і дані через інтерфейс виводу команд управління і інтерфейс виводу даних.

1.11.9. (Рівні 1-4) Криптографічний модуль не має використовувати функціональність, яка спирається на функції або алгоритми, що не пройшли самотестування, поки відповідні тести не були повторно успішно виконані.

1.11.10. (Рівні 1-4) Якщо модуль не видає помилку у разі відмови самотестування модуля, оператор модуля має бути в змозі визначити неявно за допомогою однозначної процедури, задокументованій в політиці безпеки, те, що модуль перейшов в стан помилки.

1.11.11. (Рівні 3,4) На рівнях безпеки 3 і 4 модуль має підтримувати журнал помилок, який доступний санкціонованим операторам модуля.

1.11.12. (Рівні 3,4) Журнал помилок має містити інформацію, що найменш, про останні помилки (тобто, коли самотестування не вдалося).

1.11.13. (Рівні 1-4) Доексплуатаційні тести мають виконуватися криптографічним модулем в проміжок часу, коли криптографічний модуль увімкнений (після вимкнення, скидання, перезавантаження, холодного старту, відключення живлення тощо) і переходу в робочий стан

1.11.14. (Рівні 1-4) Криптографічний модуль має виконати такі доексплуатаційні тести, якщо це необхідно:

доексплуатаційний тест цілісності ПЗ/ВПЗ;

доексплуатаційний тест обходу;

доексплуатаційний тест критичних функцій.

1.11.15. (Рівні 1-4) Якщо криптографічний модуль реалізує можливість обходу, то модуль має забезпечити коректну роботу логічної активації можливості обходу.

1.11.16. (Рівні 1-4) *Обумовлене самотестування* має виконуватися криптографічним модулем, коли виникають умови, зазначені в таких тестах: самотестування криптографічного алгоритму, тест узгодженості пар, тест завантаження ПЗ/ВПЗ, тест ручного введення, обумовлений тест обходу та обумовлений тест критичних функцій.

1.11.17. (Рівні 1-4) *Самотестування криптографічного алгоритму.* Тест криптографічного алгоритму повинен проводитися для всіх криптографічних функцій (наприклад, функції безпеки, методів встановлення ЧПБ, автентифікації) кожного затвердженого криптографічного алгоритму, який реалізований в модулі.

1.11.18. (Рівні 1-4) Обумовлений тест повинен бути виконаний до першого робочого використання криптографічного алгоритму.

1.11.19. (Рівні 1-4) Тест виявлення збоїв охоплює впровадження механізмів виявлення збоїв, інтегрованих у реалізаціях криптографічного алгоритму, якщо несправність виявлена, тест виявлення несправностей криптографічного алгоритму має закінчитися невдачею.

1.11.20. (Рівні 1-4) Якщо криптографічний модуль генерує пари відкритих або приватних ключів, тест узгодженості пар має виконатися для кожної згенерованої пари відкритого і приватного ключів.

1.11.21. (Рівні 1-4) Криптографічний модуль має дозволити операторам ініціювати доексплуатаційні або обумовлені самотестування за запитом для періодичного тестування модуля. Прийнятними засобами для вимоги ініціювати періодичне самотестування є: надання послуги, скидання, перезавантаження або увімкнення.

1.11.22. (Рівні 3,4) На додаток до вимог рівні безпеки 1 та 2 модуль повинен кілька разів за певний період часу автоматично, без зовнішнього джерела або контролю, виконувати перед експлуатаційне або обумовлене само тестування.

### 1.12. Забезпечення життєвого циклу

1.12.1. (Рівні 1-4) Для розробки криптографічного модуля і компонентів модуля, які знаходяться в рамках криптографічного кордону має використовуватися система управління конфігураціями і пов'язана з нею документація модуля.

1.12.2. (Рівні 1-4) Система управління конфігураціями має відстежувати і зберігати зміни або перегляд ідентифікації та версії кожного елемента конфігурації протягом життєвого циклу затвердженого криптографічного модуля.

1.12.3. (Рівні 3,4) На додаток до вимог для рівнів безпеки 1 та 2 елементи конфігурації повинні управлятися за допомогою автоматизованої системи управління конфігурацією.

1.12.4. (Рівні 1-4) Функціонування криптографічного модуля має бути визначене з використанням моделі скінченних станів (або еквівалентом), представленої за допомогою діаграми переходів, таблиці переходів та описів станів.

1.12.5. (Рівні 1-4) Модель скінченого автомату (МСА) криптографічного модуля має охопити, як мінімум, такі робочі і помилкові стани:

*1) Стан живлення увімкнено/вимкнено*: стан, в якому модуль вимкнено або в якому первинне, вторинне, або резервне живлення подається на модуль.

*2) Стан загальної ініціалізації*: стан криптографічного модуля, в якому проходить його ініціалізація перед переходом модуля у схвалений стан.

*3) Стан оператора безпеки:* стан, в якому виконуються послуги оператора безпеки (наприклад, криптографічна ініціалізація, безпечне адміністрування і управління ключами).

*4) Стан введення КПБ*: стан для введення КПБ в криптографічний модуль.

5) *Стан користувача* (якщо реалізована роль користувача): стан, в якому санкціоновані користувачі використовують послуги безпеки, виконують криптографічні операції або виконують інші схвалені функції.

6) *Схвалений стан:* стан, в якому виконуються схвалені функції безпеки .

7) *Стан самотестування*: стан, в якому криптографічний модуль виконує самотестування.

8) *Помилковий стан*: стан криптографічного модуля при виникненні помилки (наприклад, не успішної самодіагностики). Може існувати одна або декілька помилок, які призводять до одного помилкового стану модуля. Помилковий стан може включати в себе "апаратні" помилки, які вказують на несправність обладнання і які можуть вимагати обслуговування або ремонту криптографічного модуля або «програмні» помилки, які можна виправити (відновитися), що можуть вимагати ініціалізації або скидання модуля.

1.12.6. (Рівні 1-4) Відновлення з помилкових станів має бути можливим, окрім випадків, викликаних апаратними помилками, які потребують обслуговування або ремонту криптографічного модуля.

1.12.7. (Рівні 1-4) Кожна окрема послуга криптографічного модуля, використання функції безпеки, помилковий стан, самотестування або автентифікація оператора повинні мати окремі стани.

1.12.8. (Рівні 1-4) Перехід до стану оператора КЗІ з будь-якої іншої ролі, окрім ролі оператора КЗІ, має бути заборонено.

1.12.9. (Рівні 1-4) Якщо криптографічний модуль містить ПЗ або ВПЗ, початковий код, посилання на мови, компілятори, версії компіляторів і параметри компілятора, компоновщики і опції компоновщика, бібліотеки і параметри бібліотек, параметри конфігурації, процеси і методи побудови, опції побудови, змінні середовища і всіх інших ресурсів, які використовуються для компіляції та компонування початкового коду у вигляд, придатний до виконання, мають відстежуватися за допомогою системи управління конфігурацією.

1.12.10. (Рівні 1-4) Якщо криптографічний модуль містить ПЗ або ВПЗ, початкові коли повинні бути анотовані коментарями, які зображують відповідність ПЗ або ВПЗ до архітектури модуля.

1.12.11. (Рівні 1-4) Якщо криптографічний модуль містить апаратні засоби, документація має містити схеми та/або або його опис на спеціалізованій мові програмування, що використовується для опису цифрових логічних схем HDL (hardware description language).

1.12.12. (Рівні 3,4) Для рівнів безпеки 1 та 2, документація має містити опис функціонального тестування криптографічного модуля постачальником.

1.12.13. (Рівні 1-4) Для програмних криптографічних модулів і програмних компонентів гібридного модуля, постачальник повинен використовувати автоматизовані інструменти діагностики безпеки (наприклад, виявити переповнення буфера).

1.12.14. (Рівні 3,4) На додаток до вимог для рівнів безпеки 1 та 2, документація криптографічного модуля має містити процедури і результати тестування низького рівня.

1.12.15. (Рівні 1-4) Документація має вказати процедури безпечної інсталяції, ініціалізації і запуску криптографічного модуля.

1.12.16. (Рівні 2-4) На додаток до вимоги рівня безпеки 1, документація має містити необхідні процедури для підтримки безпеки під час доставки, інсталяції і ініціалізації версій криптографічного модуля уповноваженим оператором.

1.12.17. (Рівні 2-4) Ці процедури повинні містити настанови для уповноважених операторів щодо виявлення спроб зламу в процесі доставки, інсталяції та ініціалізації модуля.

1.12.18. (Рівень 4) На додаток до вимог рівнів безпеки 1, 2 і 3 процедури мають вимагати, щоб модуль провів автентифікацію уповноваженого оператора, використовуючи дані автентифікації, надані постачальником.

1.12.19. (Рівні 1-4) Для рівнів безпеки 1 і 2 документація має містити процедури безпечного видалення конфіденційної інформації (наприклад, ЧПБ, даних користувача, тощо) з криптографічного модуля, внаслідок чого модуль можна передати іншим операторам або утилізувати.

1.12.20. (Рівні 3,4) На додаток до вимог рівнів безпеки 1 та 2 документація має містити процедури гарантованого знищення модуля.

1.12.21. (Рівні 1-4) Настанова адміністратора має містити:

адміністративні функції, події безпеки, параметри безпеки (і значення параметрів, у відповідних випадках), фізичні порти і логічні інтерфейси криптографічного модуля, які доступні для оператора КЗІ і/або інших адміністративних ролей;

процедури, які гарантують незалежність механізмів автентифікації операторів;

процедури адміністрування криптографічного модуля, який знаходиться в схваленому експлуатаційному режимі;

допущення щодо поведінки користувача, які мають відношення до безпечної експлуатації криптографічного модуля.

1.12.22 (Рівні 1-4) Не адміністративні настанови мають містити:

схвалені і не схвалені функції безпеки, фізичні порти і логічні інтерфейси, доступні для користувачів криптографічного модуля ;

всі обов'язки користувачів, необхідні для схваленого режиму роботи криптографічного модуля.

1.13. Послаблення інших атак

1.13.1. (Рівні 1-4) Якщо криптографічний модуль призначений для послаблення однієї або кількох конкретних атак, які не визначені в цьому регламенті, то документація модуля має містити опис атак, які здатні послабити безпеку модуля.

## 2 Суттєві вимоги до криптографічних модулів, які реалізують цифровий підпис

Суттєві вимоги до криптографічних модулів, які реалізують цифровий підпис наведено у таблиці 1.

## 3. Вимоги щодо проектування та виготовлення криптографічних модулів

Вимоги що проектування та виготовлення засобів КЗІ, включаючи криптографічні модулі, визначаються нормативно-правовими актами

спеціально уповноваженого органу у галузі спеціального зв'язку та захисту інформації.

## 4. Нормативні посилання (доказова база технічного регламенту)

Нормативні документи (стандарти), що застосовуються під час визначення вимог до засобів КЗІ, порядку їх проектування і виготовлення, оцінки відповідності та аудиту наведено у таблицях 2 та 3.

Будь-який стандарт з переліку наведених застосовується у частині, що не суперечить цілям, вимогам та визначенням Технічного регламенту засобів криптографічного захисту інформації. На час застосування використовується більш нова версія (редакція) стандарту, якщо вона вже набула чинності.

Ключовим, з точки зору досягнення цілей цього Технічного регламенту є стандарт ISO/IEC 24759 «Інформаційні технології. Методи захисту. Вимоги до випробувань криптографічних модулів» (таблиця 1), на підставі якого акредитовані органи оцінки відповідності розробляють конкретні програми та методики проведення досліджень та випробувань криптографічної продукції.

Метою стандарту ISO/IEC 24759 є опис методів, що використовуються акредитованими органами для перевіряння відповідності криптографічних модулів вимогам стандарту ISO/IEC 19790. Він охоплює детальні процедури, експертизи і тести, яких повинен дотримуватись перевіряльник, і очікувані результати, які мають бути досягнуті для того, щоб криптографічний модуль задовольняв вимоги ISO/IEC 19790. Детальні методи призначені для надання високого степеня об'єктивності під час виконання процесу випробування і для забезпечення узгодженості між акредитованими випробувальними лабораторіями.

Також цей документ визначає детальну інформацію, яку повинен надати постачальник як додатковий доказ для демонстрування відповідності вимогам ISO/IEC 19790. Постачальники можуть використовувати цей документ як настанову з метою визначення, чи задовольняє їхній криптографічний модуль вимогам ISO/IEC 19790 стосовно безпеки, до подання його у орган оцінки відповідності для проведення випробувань.

Таблиця 1
Додатку 2 Технічного регламенту засобів криптографічного захисту інформації

**Суттєві вимоги**
**до криптографічних модулів, які реалізують цифровий підпис**

| 1. Профіль безпеки для надійних засобів обчислення цифрового підпису | | | | |
|---|---|---|---|---|
| **1.1. Засоби з вбудованою генерацією ключів** | **1.2. Засоби з імпортом ключів** | **1.3 Додаткові вимоги для засобів з вбудованою генерацією ключів та довірчим каналом зв'язку з програмою генерації сертифікатів** | **1.4 Додаткові вимоги для засобів з вбудованою генерацією ключів та довірчим каналом зв'язку з програмою обчислення цифрового підпису** | **1.5 Додаткові вимоги для засобів з імпортом ключів та довірчим каналом зв'язку з програмою обчислення цифрового підпису** |
| Розділ визначає профіль безпеки для надійних засобів обчислення цифрового підпису, що мають внутрішні вбудовані механізми створення пари ключів для обчислення та | Розділ визначає профіль безпеки для надійних засобів обчислення цифрового підпису, які можуть імпортувати ключ підпису (дані для створення цифрового підпису) і | Розділ визначає профіль безпеки для надійних засобів обчислення цифрового підпису, що мають внутрішні вбудовані механізми створення пари ключів для обчислення та перевіряння цифрового | Розділ визначає профіль безпеки для надійних засобів обчислення цифрового підпису, що мають внутрішні вбудовані механізми створення пари ключів для | Розділ визначає профіль безпеки для надійних засобів обчислення цифрового підпису, які можуть імпортувати ключ підпису (дані для створення цифрового |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| перевіряння цифрового підпису.<br>Цей профіль безпеки описує основні вимоги безпеки для надійних засобів обчислення цифрового підпису, які можуть генерувати ключ обчислення цифрового підпису (дані для створення цифрового підпису) та використовувати згенерований ключ для створення електронних підписів. Засіб, що оцінюється відповідно до цього профілю безпеки та використовується в визначеному операційному середовищі, є надійним засобом обчислення будь-якого типу цифрового підпису.<br>Цей профіль безпеки може | використовуватися для створення електронних підписів за допомогою імпортованого ключа. Засіб, що оцінюється відповідно до цього профілю безпеки та використовується в визначеному операційному середовищі, є надійним засобом обчислення будь-якого типу цифрового підпису.<br>Цей профіль безпеки може використовуватися для будь-якого пристрою, налаштованого на створення цифрового підпису. Зокрема цей профіль безпеки дозволяє кваліфікувати товар як пристрій для створення удосконаленого електронного підпису.<br>В безпечному | підпису та експортують відкритий ключ через довірчий канал зв'язку до програми генерації сертифікатів.<br>Цей профіль безпеки визначає основні вимоги для надійних засобів обчислення цифрового підпису, які можуть генерувати ключ обчислення цифрового підпису (дані для створення цифрового підпису) та використовувати згенерований ключ для створення удосконалених цифрових підписів, які є кваліфікованими цифровими підписами, якщо вони базуються на дійсних кваліфікованих сертифікатах відкритого ключа.<br>Крім того, об'єкт оцінювання згідно з | обчислення та перевіряння цифрового підпису та взаємодіють з програмою обчислення цифрового підпису через довірчий канал зв'язку.<br>Цей профіль безпеки визначає основні вимоги для надійних засобів обчислення цифрового підпису, які можуть генерувати ключ обчислення цифрового підпису (дані для створення цифрового підпису) та використовувати згенерований ключ для створення удосконалених цифрових підписів, які є кваліфікованими цифровими підписами, якщо вони | підпису) і використовують довірчий канал для зв'язку з програмою обчислення цифрового підпису.<br>Цей профіль безпеки визначає основні вимоги для надійних засобів обчислення цифрового підпису, які можуть імпортувати ключ обчислення цифрового підпису (дані для створення цифрового підпису) та використовувати цей ключ для створення удосконалених цифрових підписів, які є кваліфікованими цифровими підписами, якщо вони базуються на дійсних кваліфікованих сертифікатах відкритого ключа. |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| використовуватися для будь-якого пристрою, налаштованого на створення цифрового підпису. Зокрема цей профіль безпеки дозволяє кваліфікувати товар як пристрій для створення удосконаленого електронного підпису. Відкритий ключ, що відповідає ключу обчислення цифрового підпису (дані для перевіряння цифрового підпису), надається як вхідні дані для створення сертифіката відкритого ключа. Вимоги безпеки для експорту даних для перевіряння цифрового підпису описано в профілі безпеки, який доповнює цей профіль безпеки (Профіль | середовищі для створення цифрового підпису підписувач може використовувати надійний засіб цифрового підпису, що відповідає тільки цим основним вимогам безпеки створення удосконаленого цифрового підпису. Засіб обчислення сертифікатів повинен генерувати пари даних для створення/перевіряння цифрового підпису у захищеному середовищі та імпортувати ці дані у надійний засіб обчислення цифрового підпису для подальшого надання його підписувачеві принаймні з одним набором даних для створення цифрового | цим профілем безпеки підтримує його автентифікацію як надійного засобу обчислення цифрового підпису за допомогою програми створення сертифікатів постачальника послуг сертифікації та надійного зв'язку з цією програмою створення сертифікатів для захисту даних для перевіряння цифрового підпису, згенерованих та експортованих об'єктом оцінювання та імпортованих програмою створення сертифікатів. Ці функції безпеки змінюють життєвий цикл об'єкту оцінювання. Цей профіль безпеки розширює та доповнює «Профіль безпеки для надійних засобів | базуються на дійсних кваліфікованих сертифікатах відкритого ключа. Крім того, додатково об'єкт оцінювання, що відповідає цьому профілю безпеки, повинен підтримувати встановлення довірчого каналу зв'язку з програмою обчислення цифрового підпису для захисту даних автентифікації та даних, що підписуються. Цей профіль безпеки розширює та доповнює «Профіль безпеки для надійних засобів обчислення цифрового підпису. Засоби з вбудованою генерацією ключів». | Крім того, додатково об'єкт оцінювання, що відповідає цьому профілю безпеки, повинен підтримувати встановлення довірчого каналу зв'язку з програмою обчислення цифрового підпису для захисту даних автентифікації та даних, що підписуються. Цей профіль безпеки розширює та доповнює «Профіль безпеки для надійних засобів обчислення цифрового підпису. Засоби з імпортом ключів». |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| безпеки для надійних засобів обчислення цифрового підпису. Додаткові вимоги для засобів з вбудованою генерацією ключів та довірчим каналом зв'язку з програмою генерації сертифікатів).<br>В безпечному середовищі для створення цифрового підпису підписувач може використовувати надійний засіб цифрового підпису, що відповідає тільки цим основним вимогам безпеки створення удосконаленого цифрового підпису. Вимоги для надійного засобу цифрового підпису, що використовується в середовищах, де зв'язок між цим | підпису та, можливо, інформацією про відповідний сертифікат.<br>Об'єкт оцінювання може надавати додаткові функції безпеки, наприклад, підтримувати захист цілісності даних, що підлягають підписанню. Відповідні вимоги безпеки описано в окремому профілі безпеки, який доповнює цей профіль безпеки (Профіль безпеки для надійних засобів обчислення цифрового підпису. Додаткові вимоги для засобів з імпортом ключів та довірчим каналом зв'язку з програмою обчислення цифрового підпису). | обчислення цифрового підпису. Засоби з вбудованою генерацією ключів». | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| засобом та програмою створення цифрового підпису вважається захищеним, описано в окремому профілі безпеки, який доповнює цей профіль безпеки (Профіль безпеки для надійних засобів обчислення цифрового підпису. Додаткові вимоги для засобів з вбудованою генерацією ключів та довірчим каналом зв'язку з програмою обчислення цифрового підпису). | | | | |

**2. Загальний опис об'єкту оцінювання**

**2.1. Функціонування об'єкту оцінювання**

В цьому розділі описано функціонування об'єкту оцінювання в різних операційних середовищах:

| | | | | |
|---|---|---|---|---|
| - середовищі підготовки, де він взаємодіє з постачальником послуг сертифікації через програму створення сертифікату | - середовищі підготовки, де він взаємодіє з постачальником послуг сертифікації через програму обчислення даних для | - середовищі підготовки, де він взаємодіє з постачальником послуг сертифікації через програму створення сертифікату відкритого | - середовищі підготовки, де він взаємодіє з постачальником послуг сертифікації через програму створення | - середовищі підготовки, де він взаємодіє з постачальником послуг сертифікації через програму обчислення даних для |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| відкритого ключа для отримання сертифікату для даних перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, які генерує об'єкт оцінювання. | створення/перевіряння цифрового підпису для отримання даних для створення підпису і програмою генерації сертифікатів для отримання сертифікату для даних для перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, які створив постачальник послуг сертифікації. Програма обчислення даних для створення/перевіряння цифрового підпису передає дані для перевіряння цифрового підпису до програми генерації сертифікату. | ключа для отримання сертифікату для даних перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, які генерує об'єкт оцінювання. Об'єкт оцінювання експортує дані для перевіряння цифрового підпису через довірчий канал, який дозволяє програмі обчислення сертифікатів перевірити автентичність цих даних. | сертифікату відкритого ключа для отримання сертифікату для даних перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, які генерує об'єкт оцінювання. Об'єкт оцінювання експортує дані для перевіряння цифрового підпису через довірчий канал, який дозволяє програмі обчислення сертифікатів перевірити автентичність цих даних. | створення/перевіряння цифрового підпису для отримання даних для створення підпису і програмою генерації сертифікатів для отримання сертифікату для даних для перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, які створив постачальник послуг сертифікації. Програма обчислення даних для створення/перевіряння цифрового підпису передає дані для перевіряння цифрового підпису до програми генерації сертифікату. |

Навколишнє середовище ініціалізації взаємодіє з об'єктом оцінювання, щоб персоналізувати його вихідними значеннями еталонних даних автентифікації.

- середовищі обчислення цифрового підпису, де він взаємодіє з підписувачем через програму створення цифрового підпису

Продовження таблиці 1

| | | | |
|---|---|---|---|
| для підписання даних після автентифікації підписувача. Програма створення підпису надає дані для підписання або їх унікальне зображення як вхід функції створення підпису об'єктом оцінювання та отримання обчисленого цифрового підпису. | | | |
| | | | Об'єкт оцінювання та програма обчислення цифрового підпису спілкуються через довірчий канал для забезпечення цілісності даних для підписування або унікального зображення цих даних. |
| - середовищі керування, де він взаємодіє з користувачем або постачальником послуг надійного цифрового підпису для виконання операцій управління.<br>Всі ці середовища захищені та забезпечують захист даних, якими вони обмінюються з об'єктом оцінювання. | | | |
| Об'єкт оцінювання зберігає дані для створення підпису та еталонні дані автентифікації. Об'єкт оцінювання може зберігати кілька екземплярів даних для створення підпису. У цьому випадку об'єкт оцінювання надає функцію ідентифікації кожного екземпляру даних для створення підпису, а засіб обчислення цифрового підпису може надавати підписувачеві інтерфейс для вибору конкретного екземпляру даних для створення підпису з використанням функції створення підпису. Об'єкт оцінювання захищає конфіденційність та цілісність даних для створення підпису і гарантує його використання під час створення підпису тільки підписувачем. Цифровий підпис, створений об'єктом оцінювання, може бути використаний для створення кваліфікованих засобів електронного підпису, як визначено в Законі України «Про електронні довірчі послуги». Визначення стану сертифіката як кваліфікованого виходить за рамки цього документу.<br>Припускається, що програма створення підпису забезпечує цілісність вхідних даних, які вона надає функціям створення підпису об'єкту оцінювання. Якщо в об'єкті оцінювання не визначено тип даних, що підписуються, то програма створення підпису має вказувати на тип таких даних, та обчислювати всі необхідні значення хеш-кода. Об'єкт оцінювання може доповнити отримані дані параметрами підпису, які він зберігає, а потім обчислити значення хеш-функції від вхідних даних, якщо цього вимагає тип вхідних даних та криптографічний алгоритм, що використовується. | | | |
| | | | Об'єкт оцінювання та програма обчислення цифрового підпису спілкуються через довірчий канал для забезпечення цілісності |

Продовження таблиці 1

| | | | |
|---|---|---|---|
| | | | даних для підписування або унікального зображення цих даних. |

Об'єкт оцінювання зберігає еталонні дані автентифікації для автентифікації користувача як підписувача. Як еталонні дані автентифікації можуть використовуватися, наприклад, PIN-код, біометричні дані або їх поєднання. Об'єкт оцінювання захищає конфіденційність та цілісність еталонних даних автентифікації. Об'єкт оцінювання може надавати користувачеві інтерфейс для безпосереднього вводу даних для перевірки автентифікації, або ж він може отримати ці дані від програми створення цифрового підпису. Якщо програма створення підпису обробляє, запитує або отримує дані для перевірки автентифікації від користувача, то вона повинна захищати конфіденційність та цілісність цих даних.

Постачальник послуг сертифікації відкритих ключів і постачальник довірчих послуг взаємодіють з об'єктом оцінювання в безпечному середовищі підготовки підчас підготовки об'єкта оцінювання для передачі цього об'єкту законному користувачеві. Ці функції можуть включати:
- ініціалізація еталонних даних автентифікації;
- створення пари ключів;
- зберігання особистої інформації законного користувача.

Об'єкт оцінювання та програма обчислення сертифікатів спілкуються через довірчий канал для захисту цілісності та автентичності даних для перевіряння цифрового підпису, експортованого з об'єкту оцінювання.

## 2.2. Об'єкт оцінювання

Об'єкт оцінювання це поєднання апаратного та програмного забезпечення, налаштованого на безпечне створення, використання та управління даними для створення підпису. Надійний засіб обчислення цифрового підпису захищає дані для створення цифрового підпису протягом всього свого життєвого циклу та забезпечує їх використання в процесі обчислення цифрового підпису виключно законним користувачем.

Об'єкт оцінювання має включати всі функції інформаційної безпеки, необхідні для забезпечення секретності даних для створення цифрового підпису та безпеки цифрового підпису.

Об'єкт оцінювання забезпечує наступні функції:

| | | | | |
|---|---|---|---|---|
| (1) обчислення даних для створення підпису та відповідних даних | (1) імпорт даних для створення підпису та відповідних даних для | (1) обчислення даних для створення підпису та відповідних даних | (1) обчислення даних для створення підпису та | (1) імпорт даних для створення підпису та відповідних даних для |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| для перевіряння цифрового підпису;<br>(2) експорт даних для перевіряння цифрового підпису для сертифікації;<br>(3) імпорт та зберігання інформації про сертифікат відкритого ключа (необов'язково);<br>(4) переключення об'єкту оцінювання з неробочого стану в робочий стан;<br>(5) якщо в робочому стані, створення цифрових підписів для даних з наступними етапами: | перевіряння цифрового підпису;<br>(2) імпорт та зберігання інформації про сертифікат відкритого ключа (необов'язково);<br>(3) переключення об'єкту оцінювання з неробочого стану в робочий стан;<br>(4) якщо в робочому стані, створення цифрових підписів для даних з наступними етапами: | для перевіряння цифрового підпису;<br>(2) експорт даних для перевіряння цифрового підпису для сертифікації;<br>(3) доведення ідентичності надійного засобу обчислення цифрового підпису зовнішнім організаціям;<br>(4) імпорт та зберігання інформації про сертифікат відкритого ключа (необов'язково);<br>(5) переключення об'єкту оцінювання з неробочого стану в робочий стан;<br>(6) якщо в робочому стані, створення цифрових підписів для даних з наступними етапами: | відповідних даних для перевіряння цифрового підпису;<br>(2) експорт даних для перевіряння цифрового підпису для сертифікації;<br>(3) імпорт та зберігання інформації про сертифікат відкритого ключа (необов'язково);<br>(4) переключення об'єкту оцінювання з неробочого стану в робочий стан;<br>(5) якщо в робочому стані, створення цифрових підписів для даних з наступними етапами: | перевіряння цифрового підпису;<br>(2) імпорт та зберігання інформації про сертифікат відкритого ключа (необов'язково);<br>(3) переключення об'єкту оцінювання з неробочого стану в робочий стан;<br>(4) якщо в робочому стані, створення цифрових підписів для даних з наступними етапами: |
| (а) вибір даних для створення підпису, якщо надійний засіб обчислення цифрового підпису містить декілька екземплярів таких даних;<br>(б) автентифікація підписувача та визначення його наміру обчислити цифровий підпис;<br>(в) отримування даних, що підлягають підписанню, або їх унікального зображення; | | | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| (г) застосовування відповідної функції обчислення цифрового підпису з використанням обраних даних для створення підпису для даних або їх унікального зображення . | | | | |
| Об'єкт оцінювання може реалізувати функцію для створення цифрового підпису відповідно до специфікацій ETSI TS 101 733 (CAdES), ETSI TS 101 903 (XAdES) та ETSI TS 102 778 (PAdES). | | | | |
| Об'єкт оцінювання підготовлено до використання, якщо | | | | |
| (1) обчислено принаймні одну пару даних для створення/перевіряння цифрового підпису;<br>(2) проведено персоналізацію підписувача шляхом зберігання в об'єкті оцінювання;<br>(а) еталонних даних автентифікації;<br>(б) необов'язково, інформації про сертифікат для принаймні одного набору даних для створення цифрового підпису. | (1) імпортовано принаймні одну пару даних для створення/перевіряння цифрового підпису;<br>(2) проведено персоналізацію підписувача шляхом зберігання в об'єкті оцінювання:<br>(а) еталонних даних автентифікації;<br>(б) необов'язково, інформації про сертифікат для принаймні одного набору даних для створення цифрового підпису. | (1) обчислено принаймні одну пару даних для створення/перевіряння цифрового підпису;<br>(2) проведено персоналізацію підписувача шляхом зберігання в об'єкті оцінювання;<br>(а) еталонних даних автентифікації;<br>(б) необов'язково, інформації про сертифікат для принаймні одного набору даних для створення цифрового підпису. | | (1) імпортовано принаймні одну пару даних для створення/перевіряння цифрового підпису;<br>(2) проведено персоналізацію підписувача шляхом зберігання в об'єкті оцінювання:<br>(а) еталонних даних автентифікації;<br>(б) необов'язково, інформації про сертифікат для принаймні одного набору даних для створення цифрового підпису. |
| Після підготовки дані для створення підпису мають бути в неробочому стані. Після одержання об'єкту оцінювання підписувач перевіряє, що вони знаходяться в неробочому стані, та змінює стан даних для створення цифрового підпису на робочий. | | | | |

Продовження таблиці 1

| |
|---|
| Після підготовки законний користувач повинен бути поінформований про дані підтвердження автентифікації, необхідні для використання об'єкта оцінювання під час підписання. Якщо це пароль або PIN-код, то спосіб надання такої інформації має забезпечити конфіденційність та цілісність цих даних.<br>Якщо дані для створення підпису більше не потрібні, вони мають бути знищені, підлягає знищенню також інформація про відповідний сертифікат, якщо така існує. |
| **2.3. Життєвий цикл об'єкту оцінювання** |
| Життєвий цикл об'єкту оцінювання складається з етапів розробки, підготовки та експлуатації. Етап розробки включає розробку та виробництво об'єкту оцінювання та завершується передачею об'єкту постачальнику довірчих послуг. |

| | | | | |
|---|---|---|---|---|
| На етапі підготовки постачальник довірчих послуг виконує наступні операції:<br>(1) Отримує інформацію про передбачуваного одержувача пристрою, як це потрібно для процесу підготовки та ідентифікації як законного користувача об'єкту оцінювання.<br>(2) Створює PIN-код та /або отримує біометричні дані законного користувача, зберігає ці дані як еталонні дані автентифікації в | На етапі підготовки постачальник довірчих послуг виконує наступні операції:<br>(1) Персоналізація об'єкту оцінювання для використання підписувачем, тобто введення еталонних даних для автентифікації в об'єкт оцінювання та передача даних для підтвердження автентифікації підписувачеві;<br>(2) Ініціалізація об'єкту оцінювання, тобто постачальник послуг сертифікації | Життєвий цикл об'єкту оцінювання такий самий, як визначено в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з вбудованою генерацією ключів», за винятком наступного:<br>На етапі підготовки до використання постачальник надійного засобу обчислення цифрового підпису додатково ініціює функції безпеки в об'єкті оцінювання для ідентифікації його як надійного засобу | Життєвий цикл об'єкту оцінювання такий самий, як визначено в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з вбудованою генерацією ключів». | Життєвий цикл об'єкту оцінювання такий самий, як визначено в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з імпортом ключів». |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| об'єкті оцінювання та готує дані для підтвердження автентифікації для доставки законному користувачеві.<br>(3) Генерує сертифікат для принаймні одного набору даних для створення цифрового підпису.<br>(4) Додатково, надає інформацію про сертифікат для набору даних для створення цифрового підпису.<br>(5) Надає об'єкт оцінювання та супровідні дані підтвердження автентифікації законному користувачеві.<br>Сертифікат для даних для перевіряння цифрового підпису принаймні має містити: | створює пару даних для створення/перевіряння цифрового підпису за допомогою пристрою генерації даних для створення/перевіряння, завантажує дані для створення цифрового підпису в об'єкт оцінювання і надсилає дані для перевіряння цифрового підпису до програми обчислення сертифікату. Об'єкт оцінювання імпортує та зберігає пару даних для створення/перевіряння цифрового підпису.<br>(3) Обчислення (кваліфікованого) сертифікату, що містить серед інших<br>(а) дані для перевіряння цифрового підпису, які відповідають даним | обчислення цифрового підпису, для доказу цієї ідентичності зовнішнім особам та для захищеного експорту даних для перевіряння цифрового підпису.<br>На етапі підготовки до використання постачальник надійного засобу обчислення цифрового підпису додатково пов'язує ідентичність об'єкту оцінювання як надійного засобу обчислення цифрового підпису та ідентичність законного користувача як потенційного заявника на сертифікати для даних для перевіряння цифрового підпису, створених об'єктом оцінювання.<br>На етапі використання обчислення даних для створення/перевіряння | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| (а) дані для перевіряння цифрового підпису, які відповідають даним для створення цифрового підпису, що належать підписувачеві;<br>(б) ім'я підписувача або псевдонім, який повинен бути визначений як такий;<br>(в) зазначення початку та закінчення терміну дії сертифіката. Дані, включені в сертифікат, можуть бути записані в надійний засіб обчислення цифрового підпису під час персоналізації;<br>Перед початком фактичного підпису сертифікату програма створення сертифікату перевіряє дані для перевіряння цифрового підпису, отримані від | для створення цифрового підпису, що належать підписувачеві;<br>(б) ім'я підписувача або псевдонім, який повинен бути визначений як такий;<br>(в) зазначення початку та закінчення терміну дії сертифіката.<br>(4) Дані, включені в сертифікат, можуть бути записані в надійний засіб обчислення цифрового підпису.<br>Постачальник послуг сертифікації створює пару даних для створення/перевіряння цифрового підпису і імпортує дані для створення цифрового підпису, а також, можливо, дані для перевіряння цифрового підпису, до надійного | цифрового підпису та експорт даних для перевіряння цифрового підпису з об'єкту оцінювання може відбуватися на етапі підготовки та/або на стадії експлуатації. Об'єкт оцінювання має забезпечити довірчий канал зв`язку з програмою обчислення сертифікатів для захисту цілісності даних для перевіряння цифрового підпису.<br>На етапі використання перед створенням сертифіката, що містить дані для перевіряння цифрового підпису, експортовані з об'єкту оцінювання, програма обчислення сертифікатів додатково встановлює:<br>(1) ідентичність об'єкту оцінювання як надійного засобу | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| об'єкту оцінювання;<br>(1) встановлює відправника як справжнього власника надійного засобу обчислення цифрового підпису;<br>(2) встановлює цілісність даних для перевіряння цифрового підпису, які повинні бути сертифіковані як такі, що надані вихідним надійним засобом обчислення цифрового підпису;<br>(3) встановлює, що вихідний надійний засіб обчислення цифрового підпису був персоналізований для законного користувача;<br>(4) встановлює відповідність між даними для створення цифрового підпису і даними для | засобу обчислення цифрового підпису.<br>Постачальник послуг сертифікації:<br>(а) встановлює відповідність між даними для створення цифрового підпису і даними для перевіряння цифрового підпису;<br>(б) встановлює, що алгоритм підпису та розмір ключа в даних для перевіряння цифрового підпису є затвердженим та відповідає типу сертифікату.<br>Перевіряння того, що заявлена ідентифікація підписувача зв'язує його з даним надійним засобом обчислення цифрового підпису, виконує постачальник послуг сертифікації, який керує програмою | обчислення цифрового підпису;<br>(2) персоналізацію об'єкту оцінювання для заявника на сертифікат відкритого ключа як законного користувача;<br>(3) відповідність даних для створення цифрового підпису, що зберігаються в надійному засобі обчислення цифрового підпису отриманим даним для перевіряння цифрового підпису. | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| перевіряння цифрового підпису;<br>(5) встановлює, що алгоритм підпису та розмір ключа в даних для перевіряння цифрового підпису є затвердженим та відповідає типу сертифікату.<br>Доказ відповідності між даними для створення цифрового підпису, що зберігаються в об'єкті оцінювання, та даними для перевіряння цифрового підпису, може бути неявним у механізмах безпеки, які застосовуються в програмі сертифікації.<br>Перед створенням сертифікату постачальник сертифікаційних послуг підтверджує особу підписувача, | обчислення сертифікату.<br>Якщо об'єкт оцінювання використовується для створення удосконалених цифрових підписів, то сертифікат має зв'язувати дані для перевіряння цифрового підпису з особою (підписувачем) та підтверджувати ідентичність цієї особи.<br>Вимагається, щоб об'єкт оцінювання забезпечував механізми імпорту даних для створення цифрового підпису, реалізацію операцій з даними для створення цифрового підпису та персоналізацію.<br>Передбачається, що операційне | | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| зазначену в запиті на сертифікацію, як законного користувача об'єкта оцінювання. | середовище забезпечує захист всіх процесів підготовки об'єкту оцінювання, такі як передача даних для створення цифрового підпису від пристрою генерації даних для створення/перевіряння цифрового підпису до об'єкту оцінювання, передача даних для перевіряння цифрового підпису від пристрою генерації даних для створення/перевіряння до програми обчислення сертифіката.<br>Постачальник послуг сертифікації може експортувати дані для перевіряння цифрового підпису до об'єкту оцінювання для внутрішнього використання (наприклад, | | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| | самотестування). Перед створенням (кваліфікованого) сертифікату постачальник послуг сертифікації повинен записати дані для створення цифрового підпису до об'єкту оцінювання. Для цього може бути використаний безпечний канал зв'язку з об'єктом оцінювання, що забезпечує цілісність даних для створення цифрового підпису під час передачі. | | | |
| На етапі експлуатації підписувач може використовувати об'єкт оцінювання для створення удосконалених електронних підписів. | | | | |
| Етап експлуатації об'єкта оцінювання починається тоді, коли підписувач одержав як дані для підтвердження автентифікації, так і об'єкт оцінювання. | Етап експлуатації об'єкту оцінювання починається, коли постачальник послуг сертифікації створив щонайменше одну пару даних для | | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| Використання об’єкта оцінювання для підписування вимагає наявності принаймні одного набору даних для створення цифрового підпису, що зберігаються в його пам'яті. | створення/перевіряння цифрового підпису, а дані цифрового підпису для створення цифрового підпису імпортовано до об’єкту оцінювання, і коли підписувач набуває контроль над об’єктом оцінювання і переводить його до робочого стану. Підписувач має використовувати об’єкт оцінювання з надійною програмою обчислення цифрового підпису тільки в захищеному середовищі. Надійна програма обчислення цифрового підпису має захищати дані для підписування або їх унікальне зображення під час передачі до об’єкту оцінювання. | | | |
| Підписувач може також взаємодіяти з надійним засобом обчислення цифрового підпису для виконання завдань | | | | |

управління, наприклад, для скидання значення еталонних даних автентифікації до початкового стану, якщо пароль або ПІН в еталонних даних було втрачено або заблоковано. Такі завдання управління вимагають безпечного середовища.

Підписувач може перевести будь який набір даних для створення цифрового підпису в об'єкті оцінювання в непридатний для використання стан. Переведення всіх наборів даних для створення цифрового підпису в об'єкті оцінювання в непридатний стан завершує життєвий цикл об'єкта оцінювання як надійного засобу обчислення цифрового підпису.

Об'єкт оцінювання може підтримувати функції для створення додаткових ключів підписування. Якщо об'єкт оцінювання підтримує ці функції, то він має підтримувати функції для безпечного отримання сертифікатів для нових ключів. Для додаткового ключа підписувачеві може бути дозволено вибрати тип сертифіката (кваліфікований чи ні) для даних перевіряння цифрового підпису для нового ключа. Підписувач може також мати право змінити деякі дані у запиті сертифіката, наприклад, використовувати в сертифікаті псевдонім, а не юридичну назву. Якщо виконуються умови для отримання кваліфікованого сертифіката, то новий ключ може також використовуватися для створення удосконалених електронних підписів. Додаткові функції об'єкту оцінювання для створення додаткових ключів та їх сертифікації можуть вимагати додаткових функцій безпеки в об'єкту оцінюванні та взаємодії з постачальником довірчих послуг у безпечному середовищі.

Термін експлуатації об'єкту оцінювання як надійного засобу обчислення цифрового підпису закінчується, коли знищено весь набір даних для створення цифрового підпису, що зберігаються в об'єкті оцінювання. Це може включати також знищення відповідних сертифікатів.

**3. Загрози, яким повинен протистояти об'єкт оцінювання**

| | | | | |
|---|---|---|---|---|
| | | Цей профіль безпеки включає всі загрози, перелічені в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з вбудованою генерацією ключів». Цей профіль безпеки не визначає ніяких | Цей профіль безпеки включає всі загрози, перелічені в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з вбудованою генерацією ключів». Цей профіль безпеки не визначає ніяких | Цей профіль безпеки включає всі загрози, перелічені в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з імпортом ключів». Цей профіль безпеки не визначає ніяких додаткових |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| | | додаткових загроз. | додаткових загроз. | загроз. |
| Зловмисник:<br>- копіює дані для обчислення цифрового підпису. Зловмисник може спробувати отримати ці дані під час їх генерації, зберігання або використання об'єкту оцінювання для обчислення цифрового підпису.<br>- отримує дані для обчислення цифрового підпису з загальнодоступних даних, таких як дані для перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, або підписи, створені за допомогою даних для створення цифрового підпису або будь-яких інших даних, що експортуються за межі об'єкту оцінювання.<br>- фізично взаємодіє з об'єктом оцінювання для використання вразливостей, що приводить до компрометації об'єкту оцінювання. Ця загроза може бути спрямована проти даних для створення цифрового підпису, даних для перевіряння цифрового підпису та даних, що підписуються.<br>- підробляє дані для перевіряння цифрового підпису, які постачальник довірчих послуг надає програмі обчислення сертифікату. Це приводить до втрати цілісності даних для перевіряння цифрового підпису в сертифікаті підписувача.<br>- зловживає функцією створення підпису для отримання цифрового підпису для даних, які підписувач не мав наміру підписувати. Це можливо, якщо зловмисник має високий технологічний потенціал та глибокі знання принципів побудування та концепцій безпеки, що використовуються в об'єкті оцінювання.<br>- змінює дані для підписування, що передаються програмою обчислення цифрового підпису до об'єкту оцінювання. Таким чином, об'єкт оцінювання підписує дані, що не збігається з даними, які підписувач мав намір підписати.<br>- підробляє цифровий підпис, можливо, використовуючи цифровий підпис, створений об'єктом оцінювання, таким чином, що порушення цілісності підписаних даних не може бути виявлено підписувачем або сторонніми особами. Це можливо, якщо зловмисник має високий технологічний потенціал та глибокі знання принципів побудування та концепцій безпеки, що використовуються в об'єкті оцінювання. | | | |
| **4. Організаційні заходи безпеки** | | | | |
| | | Цей профіль безпеки включає всі організаційні заходи безпеки, перелічені в «Профілі безпеки для надійних засобів | Цей профіль безпеки включає всі організаційні заходи безпеки, перелічені в «Профілі безпеки для надійних засобів | Цей профіль безпеки включає всі організаційні заходи безпеки, перелічені в «Профілі безпеки для надійних засобів |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| | | обчислення цифрового підпису. Засоби з вбудованою генерацією ключів». Цей профіль безпеки не визначає ніяких додаткових організаційних заходів безпеки. | обчислення цифрового підпису. Засоби з вбудованою генерацією ключів». Цей профіль безпеки не визначає ніяких додаткових організаційних заходів безпеки. | обчислення цифрового підпису. Засоби з імпортом ключів». Цей профіль безпеки не визначає ніяких додаткових організаційних заходів безпеки. |

Постачальник довірчих послуг має використовувати надійні засоби обчислення сертифікатів для створення кваліфікованого або некваліфікованого сертифікату для даних для перевіряння цифрового підпису, створених (імпортованих) об'єктом оцінювання. Сертифікати мають містити принаймні ім'я підписувача та дані для перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, обчисленим в об'єкті оцінювання під контролем саме підписувача. Постачальник довірчих послуг має гарантувати, що використання об'єкта оцінювання як надійного засобу обчислення цифрового підпису саме підписувачем однозначно визначається через сертифікат або іншу загальнодоступну інформацію.

Підписувач використовує систему створення підпису для підписання даних, яка обчислює кваліфікований цифровий підпис, тобто такий, що грунтується на дійсному кваліфікованому сертифікаті. Надійний засіб обчислення цифрового підпису створює цифровий підпис з використанням даних для створення цифрового підпису, які містяться в цьому засобі, під контролем саме підписувача таким чином, що будь-яка подальша зміна даних може бути виявлена.

Підписувач використовує лише надійні засоби обчислення цифрового підпису. Цей засіб створює та надсилає дані для обчислення цифрового підпису у формі, яку очікує об'єкт оцінювання.

Життєвий цикл надійного засобу обчислення цифрового підпису, даних для створення цифрового підпису та даних для перевіряння цифрового підпису повинен бути реалізований таким чином, щоб підписувач не міг відмовитися від підписаних даних, якщо підпис було успішно перевірено з використання даних для перевіряння цифрового підпису, що містяться в нескасованому сертифікаті.

| | | | | |
|---|---|---|---|---|
| Постачальник довірчих послуг захищає | Постачальник послуг сертифікації: | | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| автентичність імені або псевдоніма підписувача та даних для перевіряння цифрового підпису у (кваліфікованому) сертифікаті за допомогою кваліфікованого цифрового підпису постачальника довірчих послуг.<br>Об'єкт оцінювання:<br>- повинен мати функції безпеки для забезпечення того, щоб тільки авторизовані користувачі могли використовувати його для створення даних для створення та перевіряння цифрового підпису;<br>- має забезпечувати криптографічну якість пар даних для створення/перевіряння цифрового підпису, | - захищає автентичність імені або псевдоніма підписувача та даних для перевіряння цифрового підпису у (кваліфікованому) сертифікаті за допомогою кваліфікованого цифрового підпису постачальника довірчих послуг;<br>- має використовувати лише надійний пристрій генерації даних для створення/перевіряння цифрового підпису та гарантує, що цей пристрій може використовувати тільки авторизований користувач;<br>- має гарантувати унікальність даних для створення цифрового підпису, відповідність | | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| яку він створює для обчислення удосконаленого або кваліфікованого цифрового підпису. Дані для створення цифрового підпису мають бути практично унікальними і не можуть бути відновлені з даних для перевіряння цифрового підпису. У цьому контексті "практично унікальні" означає, що ймовірність обчислення однакових даних для створення цифрового підпису дуже мала;<br>- має забезпечити відповідність між даними для перевіряння цифрового підпису та даними для створення цифрового підпису, сформованими | даних для створення цифрового підпису та даних для перевіряння цифрового підпису одне одному та неможливість обчислення даних для створення цифрового підпису з даних для створення цифрового підпису;<br>- має гарантувати конфіденційність даних для створення цифрового підпису під час генерації та експорту до об'єкту оцінювання, виключати використовування цих даних для створення будь-якого підпису та незворотне знищення даних для створення цифрового підпису в операційному середовищі після експорту цих даних до | | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| об'єктом оцінювання. Це включає однозначне посилання на створену пару даних для перевіряння/створення цифрового підпису підчас експорту даних для перевіряння цифрового підпису та створенні цифрового підпису з використання даних для обчислення цифрового підпису.<br>- має забезпечувати конфіденційність даних для створення цифрового підпису на всіх етапах, зокрема під час генерації даних для створення/перевіряння, обчислення цифрового підпису, зберігання та безпечного знищення таких даних. Секретність даних для | об'єкту оцінювання. | | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| створення цифрового підпису повинна бути достатньою для протидії зловмисникові, який має високий технологічний потенціал. | | | | |

Об'єкт оцінювання:

- має виявляти помилки під час ініціалізації, персоналізації та експлуатації. Об'єкт оцінювання має безпечно знищувати дані для створення цифрового підпису на вимогу підписувала;
- повинен створювати цифрові підписи, які неможливо підробити без знання даних для створення цифрового підпису шляхом використання надійних криптографічних методів. Повинно бути унеможливлено відновлення даних для створення цифрового підпису з цифрових підписів або будь-які інших даних, що експортуються з об'єкта оцінювання. Цифрові підписи повинні бути стійкими до таких атак, навіть якщо зловмисник має високий технологічний потенціал;
- повинен забезпечити використання функції створення цифрового підпису тільки легітимним підписувачам та захищати дані для створення цифрового підпису від використання іншими. Об'єкт оцінювання повинен протидіяти високотехнологічним методам нападу;
- не повинен змінювати дані для підписування або їх унікальне зображення. Якщо надаються дані для підписування, то обчислення хеш-коду за такими даними в об`єкті оцінювання не суперечить цій вимозі;
- повинен бути спроектований та побудований таким чином, щоб побічні випромінювання знаходилися у визначених межах;
- повинен мати системні функції, які виявляють фізичне втручання в його компоненти, і використовують ці функції для обмеження порушень безпеки;
- повинен запобігати або протистояти фізичним втручанням шляхом використання відповідних системних пристроїв та компонентів.

**5. Безпека операційного середовища**

| | | | | |
|---|---|---|---|---|
| Операційне | Постачальник послуг | Цей профіль безпеки | Цей профіль безпеки | Цей профіль безпеки |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| середовище повинно забезпечувати цілісність даних для перевіряння цифрового підпису, надісланих до засобу обчислення сертифікатів постачальником довірчих послуг. Засіб обчислення сертифікатів має перевіряти відповідність між даними для створення цифрового підпису та даними для перевіряння цифрового підпису підписувача у кваліфікованому сертифікаті.<br>Засіб обчислення сертифікатів повинен генерувати кваліфікований сертифікат, який включає (серед інших): (а) ім'я підписувача, якому належить об'єкт | сертифікації:<br>- повинен надаватися функції безпеки для забезпечення того, щоб тільки авторизовані користувачі могли започаткувати обчислення даних для створення та перевіряння цифрового підпису.<br>- має забезпечувати конфіденційність даних для створення цифрового підпису на всіх етапах, зокрема під час генерації даних для створення/перевіряння, обчислення цифрового підпису, зберігання та безпечного знищення таких даних.<br>- має забезпечувати криптографічну якість пар даних для створення/перевіряння цифрового підпису, | включає всі вимоги до безпеки операційного середовища, перелічені в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з вбудованою генерацією ключів».<br>Крім того, цей профіль безпеки визначає наступні додаткові вимоги:<br>Постачальник послуг сертифікації повинен перевірити за допомогою програми обчислення сертифікатів, що (кваліфікований) сертифікат, наданий надійним засобом обчислення цифрового підпису, містить унікальні ідентифікаційні дані, які дозволяють перевірити його ідентичність як | включає всі вимоги до безпеки операційного середовища, перелічені в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з вбудованою генерацією ключів».<br>Крім того, цей профіль безпеки визначає наступні додаткові вимоги:<br>Інтерфейс взаємодії з користувачем має забезпечувати конфіденційність та цілісність даних для підтвердження автентифікації, як того вимагає обраний метод автентифікації, включаючи експорт до об'єкту оцінювання, за допомогою довірчого каналу. | включає всі вимоги до безпеки операційного середовища, перелічені в «Профілі безпеки для надійних засобів обчислення цифрового підпису. Засоби з імпортом ключів».<br>Крім того, цей профіль безпеки визначає наступні додаткові вимоги:<br>Інтерфейс взаємодії з користувачем має забезпечувати конфіденційність та цілісність даних для підтвердження автентифікації, як того вимагає обраний метод автентифікації, включаючи експорт до об'єкту оцінювання, за допомогою довірчого каналу.<br>Програма обчислення |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| оцінювання;<br>(б) дані для перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, що зберігаються в об'єкті оцінювання і знаходяться під контролем тільки підписувача;<br>(в) удосконалений цифровий підпис постачальника довірчих послуг. Засіб обчислення сертифікатів підтверджує через сформований кваліфікований сертифікат, що дані для створення цифрового підпису, що відповідають даним для перевіряння цифрового підпису, зберігаються в об'єкті | яку він створює для обчислення удосконаленого або кваліфікованого цифрового підпису. Дані для створення цифрового підпису мають бути практично унікальними і не можуть бути відновлені з даних для перевіряння цифрового підпису. У цьому контексті "практично унікальні" означає, що ймовірність обчислення однакових даних для створення цифрового підпису дуже мала.<br>- має забезпечити відповідність між даними для перевіряння цифрового підпису та даними для створення цифрового підпису, сформованими | надійного засобу обчислення цифрового підпису, і що ця ідентичність пов'язана з законним власником засобу;<br>Програма обчислення сертифікатів має виявляти порушення цілісності даних для перевіряння цифрового підпису, імпортованих з об'єкту оцінювання;<br>на етапі розробки розробник провадить попередню ініціалізацію об'єкту оцінювання для доставки клієнту (тобто постачальнику довірчих) в середовищі, яке не відповідає вимогам безпеки для операційного середовища.<br>Постачальник довірчих послуг виконує ініціалізацію та персоналізацію об'єкту | Програма обчислення цифрового підпису має надавати довірчий канал зв'язку з об'єктом оцінювання для захисту цілісності даних для підписування для того, щоб гарантувати виявлення порушення цілісності унікального зображення даних для підписування підчас передачі цих даних від програми обчислення цифрового підпису до об'єкту оцінювання. | цифрового підпису має надавати довірчий канал зв'язку з об'єктом оцінювання для захисту цілісності даних для підписування для того, щоб гарантувати виявлення порушення цілісності унікального зображення даних для підписування підчас передачі цих даних від програми обчислення цифрового підпису до об'єкту оцінювання. |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| оцінювання. | об'єктом оцінювання. Це включає однозначне посилання на створену пару даних для перевіряння/створення цифрового підпису підчас експорту даних для перевіряння цифрового підпису та створенні цифрового підпису з використання даних для обчислення цифрового підпису. Операційне середовище повинно забезпечувати автентичність даних для перевіряння цифрового підпису, що надсилаються до програми обчислення сертифікатів постачальника послуг сертифікації. Програма обчислення сертифікатів перевіряє | оцінювання для законного користувача (тобто власника засобу). Якщо об'єкт оцінювання передасться власникові засобу разом із даними для створення цифрового підпису, то об'єкт оцінювання є надійним засобом обчислення цифрового підпису. Мають виконуватися вимоги «Профілю безпеки для надійних засобів обчислення цифрового підпису. Засоби з вбудованою генерацією ключів» з додатковим проведенням ініціалізації об'єкту оцінювання для створення довірчого каналу зв'язку з програмою обчислення сертифікатів. Якщо об'єкт оцінювання постачається власникові | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| | відповідність даних для створення цифрового підпису у надійному засобі обчислення цифрового підпису даним для перевіряння цифрового підпису у кваліфікованому сертифікаті.<br>Засіб обчислення сертифікатів повинен генерувати кваліфікований сертифікат, який включає (серед інших):<br>(а) ім'я підписувача, якому належить об`єкт оцінювання;<br>(б) дані для перевіряння цифрового підпису, що відповідають даним для створення цифрового підпису, що зберігаються в об`єкті оцінювання і знаходяться під | засобу без даних для створення цифрового підпису, то об`єкт оцінювання становиться надійним засобом обчислення цифрового підпису тільки після створення першої пари даних для створення/перевіряння цифрового підпису. Оскільки обчислення цієї пари підписувач виконує на етапі експлуатації об`єкту оцінювання, додаткові функції безпеки, визначені цим профілем повинні бути ініційовані постачальником довірчих послуг. | | |

Продовження таблиці 1

| | | | | |
|---|---|---|---|---|
| | контролем тільки підписувача;<br>(в) удосконалений цифровий підпис постачальника довірчих послуг. Засіб обчислення сертифікатів підтверджує через сформований кваліфікований сертифікат, що дані для створення цифрового підпису, що відповідають даним для перевіряння цифрового підпису, зберігаються в об'єкті оцінювання. | | | |
| Постачальник надійних засобів цифрового підпису повинен ініціювати та персоналізувати для підписувача автентичну копію об'єкту оцінювання та надати цю копію підписувачеві як надійний засіб обчислення цифрового підпису.<br>Якщо зовнішній пристрій забезпечує користувачеві інтерфейс для його автентифікації, то цей пристрій повинен забезпечувати конфіденційність та цілісність даних підтвердження автентифікації, як того потрібує метод автентифікації, що використовується, на всьому шляху від введення даних підтвердження автентифікації через інтерфейс користувача до їх введення через інтерфейс об'єкту оцінювання. Зокрема, якщо об'єкт оцінювання потрібує надійний канал для імпорту даних підтвердження автентифікації, то пристрій взаємодії з користувачем повинен підтримувати використання цього надійного каналу.<br>Підписувач повинен використовувати надійний засіб обчислення цифрового підпису, який | | | | |

Продовження таблиці 1

генерує унікальне зображення даних для підписування, які підписувач має намір підписати, у формі, яка підходить для обробки об'єктом оцінювання;
відправляє унікальне зображення даних до об'єкту оцінювання та ініціює перевіряння цілісності унікального зображення даних об'єктом оцінювання;
додає підпис, обчислений об'єктом оцінювання, до даних для підписування або повертає його як окремий блок даних.
Надійний засіб обчислення цифрового підпису повинен підтримувати удосконалені цифрові підписи. В даний час існує три формати, визначені ETSI, що відповідають вимогам до удосконалених цифрових підписів: CAdES, XAdES та PAdES. Ці три формати передбачають включення хеш-кода сертифіката відкритого ключа підписувача в дані, що підлягають підписанню. Для підтримки мобільності підписувача рекомендується зберігати інформацію про сертифікат в об'єкті оцінювання для подальшого використання надійним засобом цифрового підпису та ідентифікації відповідних даних для створення цифрового підпису, якщо в об'єкті оцінювання зберігається більше одного набору даних для створення цифрового підпису.
Операційне середовище має гарантувати, що унікальне зображення даних для підписування не може бути змінено під час передачі від надійного засобу цифрового підпису до об'єкту оцінювання. Зокрема, якщо об'єкт оцінювання потребує надійний канал для введення унікального зображення даних для підписування, то надійний засіб обчислення цифрового підпису повинен підтримувати використання такого надійного каналу.
Підписувач повинен перевірити, що дані для створення цифрового підпису, що зберігається в об'єкті оцінювання, отриманому від постачальника надійних засобів обчислення цифрового підпису, знаходиться в робочому стані. Підписувач повинен зберігати свої дані для підтвердження автентифікації в секреті.

Таблиця 2
Додатку 2 Технічного регламенту засобів криптографічного захисту інформації

**Перелік нормативних документів, які визначають суттєві вимоги до криптографічних модулів та оцінки їх відповідності**

| № | Позначення | Назва |
|---|---|---|
| 1. | ДСТУ ISO/IEC 19790:2015 | Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів |
| 2. | ДСТУ ISO/IEC 24759:2015 | Інформаційні технології. Методи захисту. Вимоги до випробувань криптографічних модулів |
| 3. | ДСТУ ISO/IEC TR 15446:2015 | Інформаційні технології. Методи захисту. Настанова щодо продукування профілів захисту і цілей захисту |
| 4. | ДСТУ ISO/IEC 15408-1:2017 | Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель |
| 5. | ДСТУ ISO/IEC 15408-2:2017 | Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2 Функціональні вимоги |
| 6. | ДСТУ ISO/IEC 15408-3:2017 | Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3 Вимоги до гарантії безпеки |
| 7. | ДСТУ ISO/IEC 18045:2015 | Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ |

Таблиця 3
Додатку 2 Технічного регламенту засобів криптографічного захисту інформації

**Перелік нормативних документів, які визначають додаткові (опціональні) вимоги до криптографічних модулів**

| № | Позначення | Назва |
|---|---|---|
| | **Блокові шифри** | |
| 1. | ДСТУ 7624:2014 | Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення |
| 2. | ДСТУ ISO/IEC 18033-3:2015 | Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри |
| 3. | ДСТУ ГОСТ 28147:2009 | Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования |
| | **Потокові шифри** | |
| 4. | ДСТУ ISO/IEC 18033-4:2015 | Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри |
| | **Асиметричні алгоритми та технології** | |
| 5. | ДСТУ 4145:2002 | Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння |
| 6. | ДСТУ ISO/IEC 9796-2:2015 | Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел |
| 7. | ДСТУ ISO/IEC 9796-3:2015 | Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі |
| 8. | ДСТУ ISO/IEC 14888-1:2015 | Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення |
| 9. | ДСТУ ISO/IEC 14888-2:2015 | Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел |

Продовження таблиці 3

| № | Позначення | Назва |
|---|---|---|
| 10. | ДСТУ ISO/IEC 14888-3:2015 | Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні |
| 11. | ДСТУ ISO/IEC 15946-1:2015 | Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 1. Загальні положення |
| 12. | ДСТУ ISO/IEC 15946-5:2015 | Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерація еліптичних кривих |
| 13. | ДСТУ ISO/IEC 18033-2:2015 | Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри |
| **Коди автентифікації повідомлень** | | |
| 14. | ДСТУ ISO/IEC 9797-2:2015 | Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми, що використовують спеціалізовану геш-функцію |
| **Геш-функції** | | |
| 15. | ДСТУ 7564:2014 | Інформаційні технології. Криптографічний захист інформації. Функція хешування |
| 16. | ГОСТ 34.311-95 | Информационная технология. Криптографическая защита информации. Функция хеширования |
| 17. | ДСТУ ISO/IEC 10118-2:2015 | Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n-бітний блоковий шифр |
| 18. | ДСТУ ISO/IEC 10118-3:2005 | Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції |
| 19. | ДСТУ ISO/IEC 10118-4:2015 | Інформаційні технології. Методи захисту. Геш-функції. Частина 4. Геш-функції, що використовують модульну арифметику |
| **Автентифікація об'єктів** | | |
| 20. | ДСТУ ISO/IEC 9798-2:2015 | Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 2. Механізми, що використовують алгоритми симетричного шифрування |
| 21. | ДСТУ ISO/IEC 9798-3:2002 | Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3: Механізми з використанням методу цифрового підпису |
| 22. | ДСТУ ISO/IEC 9798-4:2015 | Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 4. Методи на базі криптографічних контрольних функцій |

Продовження таблиці 3

| № | Позначення | Назва |
|---|---|---|
| 23. | ДСТУ ISO/IEC 9798-5:2015 | Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 5. Механізми, що використовують методи нульової обізнаності |
| 24. | ДСТУ ISO/IEC 9798-6:2015 | Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 6. Механізми, що використовують ручну передачу даних |
| **Управління ключами** | | |
| 25. | ДСТУ ISO/IEC 11770-2:2015 | Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів |
| 26. | ДСТУ ISO/IEC 11770-3:2015 | Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів |
| 27. | ДСТУ ISO/IEC 11770-4:2015 | Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, що засновані на нестійких секретах |
| **Випадкова генерація біт** | | |
| 28. | ДСТУ ISO/IEC 18031:2015 | Інформаційні технології. Методи захисту. Випадкова генерація біт |
| 29. | ДСТУ 4145:2002 | Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння |
| **Створення чутливих параметрів безпеки** | | |
| 30. | ДСТУ ISO/IEC 11770-2:2015 | Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів |
| 31. | ДСТУ ISO/IEC 11770-3:2015 | Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів |
| **Профілі захисту та вимоги безпеки засобів електронного підпису** | | |
| 32. | ДСТУ ETSI TS 119 101:2016 | Електронні підписи й інфраструктури (ESI). Політика та вимоги з безпеки для застосунків для створення та валідації електронних підписів |
| 33. | ДСТУ ETSI TS 119 312:2015 | Електронні підписи й інфраструктури (ESI). Криптографічні комплекти. |
| 34. | ДСТУ ETSI EN 319 102-1:2016 | Електронні підписи й інфраструктури (ESI). Процедури створення та валідації удосконалених електронних підписів. Частина 1. Створення та валідація |
| 35. | ДСТУ ETSI EN 319 102-2:_____ | Електронні підписи й інфраструктури (ESI). Процедури створення та валідації удосконалених електронних підписів. Частина 2. Звіт про |

Продовження таблиці 3

| № | Позначення | Назва |
|---|---|---|
| | | валідацію |
| 36. | ДСТУ EN 419 111-2:___ | Профілі захисту застосунків створення та перевірки електронних підписів. Частина 2. Застосунки створення електронних підписів. Основні профілі захисту. |
| 37. | ДСТУ EN 419 111-3:___ | Профілі захисту застосунків створення та перевірки електронних підписів. Частина 3. Застосунки створення електронних підписів. Можливі розширення |
| 38. | ДСТУ EN 419 111-4:___ | Профілі захисту застосунків створення та перевірки електронних підписів. Частина 4. Застосунки перевірки електронних підписів. Основні профілі захисту. |
| 39. | ДСТУ EN 419 111-5:___ | Профілі захисту застосунків створення та перевірки електронних підписів. Частина 5. Застосунки перевірки електронних підписів. Можливі розширення |
| 40. | ДСТУ EN 419 211-1:2016 | Профілі захисту для засобу для створення захищеного підпису. Частина 1. Огляд |
| 41. | ДСТУ EN 419 211-2:2016 | Профілі захисту для засобу для створення захищеного підпису. Частина 2. Засіб з генерацією ключів |
| 42. | ДСТУ EN 419 211-3:2016 | Профілі захисту для засобу для створення захищеного підпису — Частина 3. Засіб з імпортуванням ключів |
| 43. | ДСТУ EN 419 211-4:2016 | 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 |
| 44. | ДСТУ EN 419 211-5:2016 | 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 |
| 45. | ДСТУ EN 419 211-6:2016 | Профілі захисту для засобу для створення захищеного підпису. Частина 6. Розширення для засобу з імпортуванням ключів і надійним каналом зв'язку з програмою створення підпису |
| 46. | ДСТУ EN 419 212-1:2016 | Інтерфейси застосунків для елементів безпеки для засобів кваліфікованого електронного підпису печатки. Частина 1. Огляд |
| 47. | ДСТУ EN 419 212-2:2016 | Інтерфейси застосунків для елементів безпеки для засобів кваліфікованого електронного підпису |

Продовження таблиці 3

| № | Позначення | Назва |
|---|---|---|
| | | печатки. Частина 2. Основні сервіси |
| 48. | ДСТУ EN 419 212-3:____ | Інтерфейси застосунків для елементів безпеки для засобів кваліфікованого електронного підпису печатки. Частина 3. Засоби автентифікації |
| 49. | ДСТУ EN 419 212-4:____ | Інтерфейси застосунків для елементів безпеки для засобів кваліфікованого електронного підпису печатки. Частина 4. Протоколи забезпечення конфіденційності |
| 50. | ДСТУ EN 419 212-5:____ | Інтерфейси застосунків для елементів безпеки для засобів кваліфікованого електронного підпису печатки. Частина 5. Довірчі електронні сервіси |
| 51. | ДСТУ EN 419 221-1:2017 | Профілі захисту для криптографічних модулів постачальника електронних довірчих послуг. Частина 1. Огляд |
| 52. | ДСТУ EN 419 221-2:2017 | Профілі захисту для криптографічних модулів постачальника електронних довірчих послуг. Частина 2. Криптографічний модуль постачальника електронних довірчих послуг для операції підписання з резервним копіюванням |
| 53. | ДСТУ EN 419 221-3:2017 | Профілі захисту для криптографічних модулів постачальника електронних довірчих послуг. Частина 3. Криптографічний модуль постачальника електронних довірчих послуг для сервісів генерації ключів |
| 54. | ДСТУ EN 419 221-4:2017 | Профілі захисту для криптографічних модулів постачальника електронних довірчих послуг. Частина 4. Криптографічний модуль постачальника електронних довірчих послуг для операції підписання без резервного копіювання |
| 55. | ДСТУ EN 419 221-5:____ | Профілі захисту для криптографічних модулів постачальника електронних довірчих послуг. Частина 5. Криптографічний модуль для довірчих сервісів |
| **Формат криптографічного повідомлення** | | |
| 56. | RFC 5652 | Cryptographic Message Syntax (CMS) |
| **Формат удосконаленого електронного підпису (печатки)** | | |
| 57. | ДСТУ ETSI EN 319 122-1:2016 | Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи CAdES |
| 58. | ДСТУ ETSI EN 319 122-2:2016 | Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES. Частина 2. Розширені підписи CAdES |

Продовження таблиці 3

| № | Позначення | Назва |
|---|---|---|
| 59. | ДСТУ ETSI EN 319 132-1:2016 | Електронні підписи й інфраструктури (ESI). Цифрові підписи XAdES. Частина 1. Структурні блоки та базові підписи XAdES |
| 60. | ДСТУ ETSI EN 319 132-2:2016 | Електронні підписи й інфраструктури (ESI). Цифрові підписи XAdES. Частина 2. Розширені підписи XAdES |
| 61. | ДСТУ ETSI EN 319 142-1:2016 | Електронні підписи й інфраструктури (ESI). Цифрові підписи PAdES. Частина 1. Структурні блоки та базові підписи PAdES |
| 62. | ДСТУ ETSI EN 319 142-2:2016 | Електронні підписи й інфраструктури (ESI). Цифрові підписи PAdES. Частина 2. Додаткові профілі підпису PAdES |
| 63. | ДСТУ ETSI EN 319 142-3:____ | Електронні підписи й інфраструктури (ESI). Цифрові підписи PAdES. Частина 3. Візуальне представлення цифрових підписів PAdES |
| 64. | ДСТУ ETSI EN 319 162-1:2016 | Електронні підписи й інфраструктури (ESI). Контейнери, пов'язані з підписом (ASiC). Частина 1. Структурні блоки та базові контейнери ASiC |
| 65. | ДСТУ ETSI EN 319 162-2:2016 | Електронні підписи й інфраструктури (ESI). Контейнери, пов'язані з підписом (ASiC). Частина 2. Додаткові контейнери ASiC |
| **Управління якістю виробничого процесу** | | |
| 66. | ДСТУ ISO 9001:2015 | Системи управління якістю. Вимоги |
| 67. | ДСТУ ISO/IEC 27001:2015 | Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги |
| 68. | ДСТУ ISO/IEC 27002:2015 | Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки |
| 69. | ДСТУ ISO/IEC 27003:_____ | Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Керівництво |
| 70. | ДСТУ ISO/IEC 27004:_____ | Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Моніторинг, оцінка, аналіз та розвиток |
| 71. | ДСТУ ISO/IEC 27005:2015 | Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки |
| 72. | ДСТУ ISO/IEC 27006:2015 | Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою |

Продовження таблиці 3

| № | Позначення | Назва |
|---|---|---|
| 73. | ДСТУ ISO/IEC 27007:_____ | Інформаційні технології. Методи захисту. Керівництво з аудиту систем управління інформаційною безпекою |
| 74. | ДСТУ ISO/IEC 14764:2015 | Розробка програмного забезпечення. Процеси життєвого циклу програмного забезпечення. Супровід |
| 75. | ДСТУ ISO 10007:2005 | Системи управління якістю. Настанови щодо управління конфігурацією |
| 76. | ДСТУ ISO/IEC 16350:2016 | Інформаційні технології. Розроблення систем і програмного забезпечення. Керування застосуваннями |

Додаток 3
Технічного регламенту засобів криптографічного захисту інформації

## 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 продукції та перевіряє і засвідчує, що технічний проект продукції відповідає вимогам Технічного регламенту засобів криптографічного захисту інформації (далі – Технічний регламент), які застосовуються до неї.

2. Експертиза типу виконується з проведенням обстеження зразка завершеної продукції (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 і включає належний аналіз та оцінку ризику (ризиків). У технічній документації зазначаються застосовні вимоги та охоплені, наскільки це стосується такої оцінки, питання проектування, виробництва та функціонування продукції. Технічна документація має містити, зокрема, такі елементи: результати виконаних проектних розрахунків, проведених досліджень тощо; протоколи випробувань;

зразки продукції, що є репрезентативними для передбаченого виробництва.

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

4. Призначений орган:

проводить експертизу технічної документації і перевіряє, що зразок (зразки) продукції було виготовлено відповідно до технічної документації, та визначає елементи зразка (зразків) продукції, що були розроблені згідно із застосованими положеннями відповідних стандартів із переліку національних

експертизи типу та повідомляє про це заявнику з наданням докладного обґрунтування своєї відмови.

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 орган, що призначає, про видані або скасовані ним сертифікати експертизи типу та/або будь-які доповнення до них, а також періодично чи на запит органу, що призначає, надавати 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.

Призначений орган повинен інформувати інші призначені органи про сертифікати експертизи типу та/або будь-які доповнення до них, у видачі яких він відмовив або дію яких зупинив чи встановив щодо них інші обмеження, а також на їх запит - про видані ним сертифікати та/або доповнення до них.

Орган, що призначає, відповідні органи державного ринкового нагляду та інші 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, до закінчення строку дії такого сертифіката.

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 протягом 10 років після введення останнього зразка продукції в обіг.

стандартів, передбаченого пунктом Технічного регламенту, а також елементи, що були розроблені відповідно до інших технічних специфікацій;

проводить відповідні дослідження і випробування або доручає їх проведення з метою перевірки того, що у разі обрання виробником для застосування рішення відповідних стандартів з переліку національних стандартів, передбаченого пунктом 35 Технічного регламенту, вони були застосовані правильно;

проводить відповідні дослідження і випробування або доручає їх проведення з метою перевірки того, що у разі незастосування виробником рішень з відповідних стандартів з переліку національних стандартів, передбаченого пунктом 35 Технічного регламенту, прийняті виробником рішення про застосування інших відповідних технічних специфікацій відповідають відповідним суттєвим вимогам Технічного регламенту;

погоджує з виробником місце проведення досліджень і випробувань.

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 органом, що призначає.

Без шкоди для своїх обов'язків стосовно органу, що призначає, призначений орган оприлюднює (повністю або частково) зміст зазначеного звіту лише за згодою виробника.

6. У разі коли типовий зразок продукції відповідає вимогам Технічного регламенту, які застосовуються до певної продукції, 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 відповідна 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 відмовляє у видачі сертифіката

Продовження додатка 3

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 4
Технічного регламенту засобів криптографічного захисту інформації

## 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 категорії продукції, 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.

Призначений орган повинен припускати відповідність вимогам, наведеним у пункті 4 цього додатка, тих елементів системи управління якістю, що відповідають відповідним вимогам стандарту з переліку національних стандартів, передбаченого пунктом 35 Технічного регламенту.

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.

11. Крім періодичних аудитів, призначений орган може здійснювати відвідування виробника без попередження. Під час таких відвідувань призначений орган може у разі потреби проводити випробування продукції 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.

Продовження додатка 4

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 продукції (крім компонентів) та зберігає її для надання на запити органів державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка продукції цієї моделі. 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 складає в письмовій формі заяву про відповідність для кожної моделі компонента та зберігає її для надання на запити органів державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка компонента цієї моделі. У заяві про відповідність повинна бути ідентифікована модель компонента, для якої її було складено. Кожен компонент повинен супроводжуватися копією заяви про відповідність.

15. Виробник повинен протягом 10 років після введення останнього зразка продукції в обіг зберігати для надання органам ринкового нагляду:

документацію, зазначену в пункті 3 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.

16. Призначений орган повинен інформувати орган, що призначає, про системи управління якістю, які були схвалені або схвалення яких були скасовані, а також періодично чи на запит органу, що призначає, надавати йому список систем управління якістю, у схваленні яких відмовлено або дію яких зупинено чи іншим чином обмежено.

Призначений орган повинен інформувати інші призначені органи про системи управління якістю, у схваленні яких відмовлено або дію яких зупинено чи які скасовано або встановлено щодо них інші обмеження, а також на їх запит - про системи управління якістю, які були схвалені.

Уповноважений представник

17. Уповноважений представник виробника може подати заявку згідно з пунктом 3 цього додатка та виконувати обов'язки, визначені в пунктах 7 та 12-15 цього додатка, за умови визначення цих обов'язків у дорученні.

Додаток 5
Технічного регламенту засобів криптографічного захисту інформації

## МОДУЛЬ F
## Відповідність типу на основі перевірки продукції

1. Відповідність типу на основі перевірки продукції є частиною процедури оцінки відповідності, за допомогою якої виробник виконує обов'язки, встановлені в пунктах 2, 6 – 8 цього додатка, та гарантує і декларує під свою виключну відповідальність, що певна продукція, до якої було застосовано вимоги пункту 3 цього додатка, відповідає типу, описаному в сертифікаті експертизи типу, і вимогам Технічного регламенту засобів криптографічного захисту інформації (далі – Технічний регламент), які застосовуються до зазначеної продукції.

Виробництво

2. Виробник вживає всіх заходів, необхідних для того, щоб виробничий процес та контроль за ним забезпечували відповідність виготовленої продукції затвердженому типу, описаному в сертифікаті експертизи типу, і вимогам Технічного регламенту, які застосовуються до зазначеної продукції.

Дослідження і випробування

3. Призначений орган з оцінки відповідності (далі – призначений орган), обраний виробником, проводить належні дослідження і випробування з метою перевірки відповідності продукції затвердженому типу, описаному в сертифікаті експертизи типу, та відповідним вимогам Технічного регламенту.

Дослідження і випробування для перевірки відповідності продукції відповідним вимогам проводяться шляхом дослідження та випробування кожної одиниці продукції, як зазначено в пунктах 4 і 5 цього додатка.

Перевірка відповідності шляхом дослідження та випробування кожної одиниці продукції

4. Кожна одиниця продукції повинна бути окремо досліджена та підлягає належним випробуванням, які визначені у відповідному стандарті(ах) з переліку національних стандартів, зазначеного у пункті 35 Технічного регламенту, та/або рівноцінним випробуванням, встановленим у відповідних технічних специфікаціях, з метою перевірки їх відповідності затвердженому

типу, описаному в сертифікаті експертизи типу, та відповідним вимогам Технічного регламенту.

У разі відсутності таких стандартів відповідний призначений орган повинен прийняти рішення про те, які відповідні випробування мають бути проведені.

5. Призначений орган повинен видати сертифікат відповідності на підставі проведених досліджень та випробувань та нанести свій ідентифікаційний номер на кожну затверджену одиницю продукції або доручити його нанесення під свою відповідальність.

Виробник повинен зберігати сертифікати відповідності для надання на запити органів державного ринкового нагляду для інспекційних цілей протягом 10 років після введення в обіг останнього зразка продукції цієї моделі.

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

6. Виробник наносить знак відповідності технічним регламентам та під відповідальність призначеного органу, зазначеного в пункті 3 цього додатка, його ідентифікаційний номер на кожну одиницю продукції (за винятком компонентів), що відповідає затвердженому типу, описаному в сертифікаті експертизи типу, та застосовним вимогам Технічного регламенту.

7. Виробник складає письмову декларацію про відповідність для кожної моделі продукції (крім компонентів) та зберігає її для надання на запити органів державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка продукції цієї моделі (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.

У разі надання призначеним органом, зазначеним у пункті 3 цього додатка, згоди та під його відповідальність виробник також може наносити ідентифікаційний номер цього призначеного органу на продукцію (крім компонентів).

8. Виробник складає письмову заяву про відповідність для кожної моделі компонента та зберігає її для надання на запити органів державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка компонента цієї моделі. У заяві про відповідність повинна бути ідентифікована модель

компонента, для якої її було складено. Кожен компонент повинен супроводжуватися копією заяви про відповідність.

9. За згодою призначеного органу та під його відповідальність виробник може наносити ідентифікаційний номер цього призначеного органу на продукцію в процесі виробництва.

Уповноважений представник

10. Обов'язки виробника від його імені та під його відповідальність можуть бути виконані його уповноваженим представником за умови визначення цих обов'язків у дорученні.

Уповноважений представник не може виконувати обов'язки виробника, визначені в пункті 2 цього додатка.

Додаток 6
Технічного регламенту засобів криптографічного захисту інформації

## МОДУЛЬ С
## Відповідність типу на основі внутрішнього контролю виробництва з випробуваннями продукції під наглядом

1. Відповідність типу на основі внутрішнього контролю виробництва з випробуваннями продукції під наглядом є частиною процедури оцінки відповідності, за допомогою якої виробник виконує обов'язки, встановлені в пунктах 2-4 цього додатка, та гарантує і декларує під свою виключну відповідальність, що певна продукція відповідає типу, описаному в сертифікаті експертизи типу, та Технічного регламенту засобів криптографічного захисту інформації (далі - Технічний регламент), які застосовуються до зазначеної продукції.

Виробництво

2. Виробник вживає всіх заходів, необхідних для того, щоб виробничий процес і контроль за ним забезпечували відповідність виготовленої продукції типу, описаному в сертифікаті експертизи типу, та вимогам Технічного регламенту, які застосовуються до зазначеної продукції.

Контроль продукції

3. З метою перевірки відповідності продукції типу, описаному в сертифікаті експертизи типу, та відповідним вимогам Технічного регламенту виробник або особа, що діє від його імені, повинні для кожної виготовленої одиниці продукції провести одне чи кілька випробувань одного або кількох визначених показників продукції. Відповідальність за проведення зазначених випробувань несе призначений орган з оцінки відповідності, обраний виробником.

Виробник під відповідальність призначеного органу з оцінки відповідності наносить його ідентифікаційний номер у процесі виробництва.

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

4. Виробник наносить знак відповідності технічним регламентам на кожну одиницю продукції (крім компонентів), що відповідає типу, описаному в сертифікаті експертизи типу, та застосовним вимогам Технічного регламенту.

5. Виробник складає письмову декларацію про відповідність для моделі продукції (крім компонентів) та зберігає її для надання на запити органам державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка цієї моделі. У декларації про відповідність повинна бути ідентифікована модель продукції, для якої її було складено.

Кожен виріб (крім компонентів) повинен супроводжуватися копією декларації про відповідність.

6. Виробник складає письмову заяву про відповідність для кожної моделі компонента та зберігає її для надання на запити органам державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка компонента цієї моделі. В заяві про відповідність повинна бути ідентифікована модель компонента, для якої ця заява була складена. Кожен компонент повинен супроводжуватися копією заяви про відповідність.

Уповноважений представник

7. Обов'язки виробника, визначені в пунктах 4-6 цього додатка, від його імені та під його відповідальність можуть бути виконані його уповноваженим представником за умови визначення цих обов'язків у дорученні.

Додаток 7
Технічного регламенту засобів криптографічного захисту інформації

## МОДУЛЬ Е
## Відповідність типу на основі забезпечення якості продукції

1. Відповідність типу на основі забезпечення якості продукції є частиною процедури оцінки відповідності, за допомогою якої виробник виконує обов'язки, встановлені в пунктах 2 і 12-14 цього додатка, та гарантує і декларує під свою виключну відповідальність, що певна продукція відповідає типу, описаному в сертифікаті експертизи типу, та вимогам Технічного регламенту засобів криптографічного захисту інформації (далі – Технічний регламент), які застосовуються до зазначеної продукції.

Виробництво

2. Виробник застосовує схвалену систему управління якістю для контролю та випробувань готової продукції, яка зазначена в пунктах 3-7 цього додатка та підлягає нагляду згідно з пунктами 8-11 цього додатка.

Система управління якістю

3. Виробник подає обраному ним призначеному органу з оцінки відповідності (далі – призначений орган) заявку на оцінку своєї 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 щодо заявленої категорії продукції;

документація щодо системи управління якістю;

технічна документація стосовно затвердженого типу та копію 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, процедур та інструкцій, викладених у письмовій формі.

Документація стосовно системи управління якістю повинна давати можливість однозначного тлумачення програм, планів, настанов і записів щодо якості.

Ця документація повинна містити, зокрема, належний опис:

цілей у сфері якості та організаційної структури, обов'язків і повноважень керівництва стосовно якості продукції;

досліджень і випробувань, які будуть проводитися після виготовлення;

записів щодо якості виробничого процесу та/або продукції (протоколи контролю та результати випробувань, дані калібрувань, протоколи стосовно кваліфікації відповідного персоналу тощо);

засобів моніторингу, за допомогою яких досягається необхідний рівень 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.

Призначений орган повинен припускати відповідність вимогам, зазначеним у пункті 4 цього додатка, тих елементів системи управління якістю, що відповідають відповідним вимогам стандарту з переліку національних стандартів, зазначеного у пункті 35 Технічного регламенту.

Група з аудиту, крім членів, які мають досвід з оцінки систем управління якістю, повинна мати у своєму складі принаймні одного члена, який має досвід оцінювання відповідної продукції та технології її виготовлення, а також знання застосовних вимог Технічного регламенту. Проведення аудиту повинно включати відвідування підприємств виробника для здійснення оцінки. Група з аудиту повинна проаналізувати технічну документацію, зазначену в абзаці шостому пункту 3 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 обов'язки, пов'язані із забезпеченням функціонування схваленої 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 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, пов'язаних із забезпеченням функціонування схваленої системи управління якістю.

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

документацію системи управління якістю;

записи щодо якості виробничого процесу та/або продукції (протоколи контролю та результати випробувань, дані калібрувань, звіти стосовно кваліфікації відповідного персоналу та інше).

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

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

Продовження додатка 7

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

12. Виробник наносить знак відповідності технічним регламентам і 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.

13. Виробник складає письмову декларацію про відповідність для кожної моделі продукції (крім компонентів) та зберігає її для надання на запити органам державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка продукції цієї моделі. 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 складає письмову заяву про відповідність для кожної моделі компонента та зберігає її для надання на запити органам державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка компонента цієї моделі. В заяві про відповідність повинна бути ідентифікована модель компонента, для якої ця заява була складена. Кожен компонент повинен супроводжуватися копією заяви про відповідність.

15. Виробник повинен протягом 10 років після введення в обіг останнього зразка моделі продукції зберігати для надання на запити органів державного ринкового нагляду:

документацію, зазначену в пункті 3 цього додатка;

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

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

16. Призначений орган повинен інформувати орган, що призначає, про системи управління якістю, які були схвалені або схвалення яких були скасовані, а також періодично чи на запит органу, що призначає, надавати йому список систем управління якістю, у схваленні яких відмовлено або дію яких зупинено чи іншим чином обмежено.

Призначений орган повинен інформувати інші призначені органи про системи управління якістю, у схваленні яких відмовлено або дію яких зупинено чи які скасовано або встановлено щодо них інші обмеження, а також на їх запит про системи управління якістю, які були схвалені.

Уповноважений представник

17. Обов'язки виробника, визначені в пунктах 3, 7, 12-15 цього додатка, від його імені та під його відповідальність можуть бути виконані його уповноваженим представником за умови визначення цих обов'язків у дорученні.

Додаток 8
Технічного регламенту засобів криптографічного захисту інформації

## МОДУЛЬ А
## Внутрішній контроль виробництва

1. Внутрішній контроль виробництва є процедурою оцінки відповідності, за допомогою якої виробник виконує обов'язки, встановлені в пунктах 2-6 цього додатка, та гарантує і декларує під виключну відповідальність, що певна продукція відповідає вимогам Технічного регламенту засобів криптографічного захисту інформації (далі - Технічний регламент), які застосовуються до зазначеної продукції.

Технічна документація

2. Виробник розробляє технічну документацію, яка дає можливість оцінити відповідність продукції відповідним вимогам і включає належний аналіз та оцінку ризику (ризиків).

У технічній документації зазначаються застосовні вимоги та охоплені, наскільки це стосується такої оцінки, питання проектування, виробництва та функціонування продукції. Технічна документація має містити, зокрема такі елементи:

загальний опис продукції;

список застосованих повністю чи частково стандартів з переліку національних стандартів, передбаченого пунктом Технічного регламенту, а в разі, коли зазначені стандарти не були застосовані, описи рішень, прийнятих з метою забезпечення відповідності суттєвим вимогам Технічного регламенту, а також список інших відповідних технічних специфікацій, що були застосовані. У разі часткового застосування стандартів з переліку національних стандартів у технічній документації повинні бути зазначені ті частини, які були застосовані;

результати виконаних проектних розрахунків, проведених досліджень тощо;

протоколи випробувань.

Виробництво

3. Виробник вживає всіх заходів, необхідних для того, щоб виробничий процес і контроль за ним забезпечували відповідність виготовленої продукції

технічній документації, зазначеній в пункті 2 цього додатка, та вимогам Технічного регламенту, які застосовуються до зазначеної продукції.

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

4. Виробник наносить знак відповідності технічним регламентам на кожну одиницю продукції (крім компонентів), що відповідає застосовним вимогам Технічного регламенту.

5. Виробник складає письмову декларацію про відповідність для кожної моделі продукції (крім компонентів) та зберігає її разом із технічною документацією для надання на запити органів державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка продукції цієї моделі. У декларації про відповідність повинна бути ідентифікована модель продукції, для якої її було складено. Кожен виріб (крім компонентів) повинен супроводжуватися копією декларації про відповідність.

6. Виробник складає письмову заяву про відповідність для кожної моделі компонента та зберігає її разом із технічною документацією для надання на запити органів державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка компонента цієї моделі. В заяві про відповідність повинна бути ідентифікована модель компонента, для якої ця заява була складена. Кожен компонент повинен супроводжуватися копією заяви про відповідність.

Уповноважений представник

7. Обов'язки виробника, визначені в пунктах 4-6 цього додатка, від його імені та під його відповідальність можуть бути виконані його уповноваженим представником за умови визначення цих обов'язків у дорученні.

Додаток 9
Технічного регламенту засобів криптографічного захисту інформації

## МОДУЛЬ G

### Відповідність на основі перевірки одиниці продукції

1. Відповідність на основі перевірки одиниці продукції є процедурою оцінки відповідності, за допомогою якої виробник виконує обов'язки, встановлені в пунктах 2-4 і 6-8 цього додатка, та гарантує і декларує під свою виключну відповідальність, що відповідний виріб, до якого було застосовано положення пункту 5 цього додатка, відповідає вимогам Технічного регламенту засобів криптографічного захисту інформації (далі - Технічний регламент), які застосовуються до зазначеного виробу.

Технічна документація

2. Виробник розробляє технічну документацію та надає її призначеному органу з оцінки відповідності (далі - призначений орган), зазначеному в пункті 5 цього додатка. Технічна документація дає можливість оцінити відповідність продукції застосовним вимогам Технічного регламенту і включає належний аналіз та оцінку ризику (ризиків). У технічній документації визначаються застосовні вимоги та охоплені, наскільки це стосується такої оцінки, питання проектування, виробництва та функціонування продукції. Технічна документація має містити, зокрема, такі елементи:

загальний опис продукції;

ескізний проект, виробничі креслення та схеми компонентів, складальних вузлів, електричних кіл тощо;

описи та пояснення, необхідні для розуміння зазначених креслень і схем та функціонування продукції;

список застосованих повністю чи частково стандартів з переліку національних стандартів, передбаченого пунктом 35 Технічного регламенту, а в разі, коли зазначені стандарти не були застосовані, - описи рішень, прийнятих з метою забезпечення відповідності суттєвим вимогам Технічного регламенту, а також список інших відповідних технічних специфікацій, що були застосовані. У разі часткового застосування стандартів з переліку національних стандартів у технічній документації повинні бути зазначені ті частини, які були застосовані;

результати виконаних проектних розрахунків, проведених досліджень тощо;

протоколи випробувань.

3. Виробник повинен зберігати технічну документацію для надання її у разі потреби відповідним органам державного ринкового нагляду протягом 10 років після введення останнього зразка продукції в обіг.

Виробництво

4. Виробник вживає всіх заходів, необхідних для того, щоб виробничий процес і контроль за ним забезпечували відповідність виготовленого виробу застосовним вимогам Технічного регламенту.

Перевірка

5. Обраний виробником призначений орган проводить чи доручає проведення належних досліджень і випробувань, установлених у відповідних стандартах з переліку національних стандартів, відповідність яким надає презумпцію відповідності продукції суттєвим вимогам щодо охорони здоров'я та безпечності, або рівноцінних випробувань, визначених у відповідних технічних специфікаціях, з метою оцінки відповідності виробу застосовним вимогам Технічного регламенту. У разі відсутності такого стандарту відповідний призначений орган повинен прийняти рішення щодо відповідних випробувань, які будуть проводитися.

Призначений орган повинен видати сертифікат відповідності стосовно проведених досліджень і випробувань та нанести свій ідентифікаційний номер на затверджений виріб або доручити його нанесення під свою відповідальність.

Виробник зобов'язаний зберігати сертифікати відповідності для надання на запити органів державного ринкового нагляду протягом 10 років після введення виробу в обіг.

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

6. Виробник наносить знак відповідності технічним регламентам та під відповідальність призначеного органу, зазначеного в пункті 5 цього додатка, його ідентифікаційний номер на кожен виріб (за винятком компонентів), що відповідає застосовним вимогам Технічного регламенту.

7. Виробник складає письмову декларацію про відповідність та зберігає її для надання на запити органів державного ринкового нагляду протягом 10 років після введення виробу в обіг. У декларації про відповідність повинен бути ідентифікований виріб, для якого її було складено. Кожен виріб (за винятком компонентів) повинен супроводжуватися копією декларації про відповідність.

Продовження додатка 9

8. Виробник складає письмову заяву про відповідність і зберігає її для надання на запити органів державного ринкового нагляду протягом 10 років після введення в обіг останнього зразка цього компонента. В заяві про відповідність повинна бути ідентифікована модель компонента, для якої ця заява була складена. Кожен компонент повинен супроводжуватися копією заяви про відповідність.

Уповноважений представник

9. Обов'язки виробника, визначені в пунктах 3, 6-8 цього додатка, від його імені і під його відповідальність можуть бути виконані його уповноваженим представником за умови визначення цих обов'язків у дорученні.

Додаток 10
Технічного регламенту засобів криптографічного захисту інформації

**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

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 2018 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 45 такого змісту:

| | | |
|---|---|---|
| 45. Засоби криптографічного захисту інформації | постанова Кабінету Міністрів України від ___ _____ 2018 р. № _____ «Про затвердження Технічного регламенту засобів криптографічного захисту інформації» | Адміністрація Держспецзв'язку |

3. Доповнити 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), підпунктом 7-1 такого змісту:

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

# 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 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;

Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстроване в Мін'юсті 16.07.2007 № 820/14087.

У зв'язку з втратою 01 січня 2018 року чинності Декрету Кабінету Міністрів України від 10.05.1993 «Про стандартизацію та сертифікацію» скасовано Правила проведення робіт із сертифікації засобів захисту інформації,

затверджені спільним наказом Адміністрації Держспецзв'язку та Держспоживстандарту від 25.04.2007 № 75/91, зареєстровані в Мін'юсті 14.05.2007 за № 498/13765.

Зазначеними вище нормативно-правовими актами у сфері КЗІ не передбачені обов'язкові до виконання вимоги до криптографічних модулів, що є кращими європейськими практиками, та процедури оцінки відповідності відповідно до вимог Закону України «Про технічні регламенти та процедури оцінки відповідності».

Технічний регламент засобів криптографічного захисту інформації (далі – Технічний регламент) засновано на національному стандарті України ДСТУ ISO/IEC 19790:2015 «Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів», затвердженому наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, та має посилання на переліки нормативних документів, які визначають суттєві вимоги до криптографічних модулів та оцінки їх відповідності та додаткові (опціональні) вимоги до криптографічних модулів.

Низка нормативних документів з означених переліків потребує прийняття в якості національних стандартів України. Відповідні пропозиції Адміністрації Держспецзв'язку надіслано до технічного комітету стандартизації № 20 «Інформаційні технології».

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, 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 реалізацію у засобах КЗІ, що є засобами КЕП, вимог 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:

впровадження гармонізованих з міжнародними та європейськими національних стандартів України, застосування яких є доказом відповідності засобів КЗІ вимогам Технічного регламенту;

приведення у відповідність вимог України щодо засобів КЗІ, що є засобами КЕП, до Регламенту ЄС 910.

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* | Відсутні, оскільки дана ситуація призведе до відставання | Не виконання вимог законодавства у сфері кіберзахисту та |

| | | |
|---|---|---|
| *регулювання* | технологій з розроблення та оцінки засобів КЗІ від кращих міжнародних практик | зобов'язань в рамках Угоди про асоціацію |

***Оцінка впливу на сферу інтересів громадян***

| Вид альтернативи | Вигоди | Витрати |
|---|---|---|
| ***Альтернатива 1.*** *Прийняття проекту постанови* | Високі, запобігання наданню на ринку не відповідної встановленим вимогам продукції. (захист інтересів громадян шляхом отримання безпечної продукції з відповідним рівнем гарантій) | Додаткових витрат не потребує |
| ***Альтернатива 2.*** *Збереження чинного регулювання* | Відсутні | Застосування засобів КЗІ без підтвердження їх відповідності кращим вимогам з безпеки несе додаткові ризики компрометації даних, що може призвести до несанкціонованого їх розголошення, підробки електронного підпису та, як наслідок завдати 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<br>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 засобів КЗІ та органами з оцінки відповідності, отримати додаткові прибутки. | Додаткових витрат не потребує |
| ***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:

суттєві вимоги до засобів КЗІ;

обов'язки суб'єктів господарювання (виробників, уповноважених представників виробника, імпортерів, розповсюджувачів);

положення щодо презумпції відповідності засобів КЗІ;

питання, пов'язані зі складанням декларації про відповідність, нанесенням знака відповідності технічним регламентам та іншого маркування;

положення щодо призначення органів з оцінки відповідності та спеціальні вимоги до них;

положення щодо здійснення державного ринкового нагляду;

процедури оцінки відповідності засобів КЗІ:

модуль А (внутрішній контроль виробництва);

модуль В (експертиза типу);

модуль С (відповідність типу на основі внутрішнього контролю виробництва з випробуванням продукції під наглядом);

модуль D (відповідність типу на основі забезпечення якості виробничого процесу);

модуль Е (відповідність типу на основі забезпечення якості продукції);

модуль F (відповідність типу на основі перевірки продукції);

модуль G (відповідність на основі перевірки одиниці продукції).

**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»;

визначити строк набрання чинності проекту постанови, а саме, через шість місяців з дня її офіційного опублікування.

**Заходи, що пропонуються для розв'язання проблеми:**

погодити проект постанови з Мінекономрозвитку та Держпідприємництвом;

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 шляхом проведення семінарів.

**Реалізація положень проекту постанови:**

забезпечить вирішення визначених проблем; сприятиме розвитку галузі промисловості; стимулюватиме ділову активність на ринку засобів КЗІ; встановлюватиме гармонізовані з європейськими вимоги безпеки засобів КЗІ, при проектуванні, виготовленні, проведенні оцінки відповідності, маркуванні та введенні в обіг, та обов'язки суб'єктів господарювання щодо їх дотримання.

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

## 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

Впровадження положень проекту постанови забезпечить:

запровадження проведення оцінки відповідності засобів КЗІ відповідно до процедур визначених Законом України «Про технічні регламенти та оцінку відповідності»;

впровадження кращих європейських практик з вимог безпеки до засобів КЗІ та оцінки їх відповідності шляхом застосування гармонізованих з міжнародними та європейськими національних стандартів України, застосування яких є доказом відповідності засобів КЗІ вимогам Технічного регламенту;

приведення у відповідність вимог України щодо засобів КЗІ, що є засобами КЕП, до Регламенту ЄС 910

забезпечення населення безпечними засобами КЗІ, у тому числі засобів КЕП;

створення умов для міжнародного співробітництва у сфері електронних довірчих послуг та електронної ідентифікації.

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.

Строк набрання чинності регуляторного акта встановлено згідно з Законом – через шість місяців з дня його опублікування.

## 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

«___»_____ 2018 року

04/02/03-1292
23.04.18

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 | Витрати | Разом за рік | Витрати за |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| | проходження відповідних процедур (витрати часу, витрати на експертизи, тощо) | безпосередньо на дозволи, ліцензії, сертифікати, страхові поліси (за рік - стартовий) | (стартовий) | 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 інформації» (далі – проект постанови) розроблено Адміністрацією Держспецзв'язку на виконання пункту 2 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» щодо забезпечення функціонування національної системи кібербезпеки у сфері криптографічного захисту інформації, термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері кібербезпеки та кіберзахисту інформації відповідно до міжнародних стандартів, інформаційної безпеки Європейського Союзу та НАТО, пункту 43 Плану зокрема стандартів Європейського Союзу та НАТО, затвердженого наказо розроблення технічних регламентів на 2018-2019 роки, затвердженого Мінекономрозвитку від 15.02.2018 № 196.

Технічний регламент засобів криптографічного захисту інформації (дал Технічний регламент), що затверджується проектом постанови, розробле Інститутом проблем математичних машин та систем НАН України замовлення Адміністрації Держспецзв'язку.

Технічний регламент засобів криптографічного захисту інформації - зас вимога щодо захисту якої встановлює вимоги до продукції - засобів КЗІ), оцін відповідності та обігу на ринку України державних інформаційних ресурсів та інфор «Про технічні регламенти та процедури оцінки відповідності» (далі – засоби Закону У, Технічний регламент встановлена законом до вимог Закону У, ДСТУ ISO/IEC 19790:2015 «Інформаційні технології. Методи захист безпеки до криптографічного модуля», затвердженому наказом підприємства «Український науково дослідний і навчальний це стандартизації, сертифікації та якості» від 18 грудня 2015 року посилання на перелік нормативних документів, які визначают до криптографічних модулів та оцінки їх відповідно (опціональні) вимоги до криптографічних модулів.

Метою проекту по встановлення вимог безпеки до засобів КЗІ від європейських практик з урахуванням національних особл запровадження процедур виготовлення, обігу, засобів КЗІ відповідно до вимог Закону України «Пр процедури оцінки відповідності»; запровадження критеріїв та методології оці відповідно до міжнародних стандартів; створення термінологічної бази у сфері КЗІ;

**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 інформації» (далі – проект постанови) розроблено Адміністрацією Держспецзв'язку на виконання пункту 2 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» щодо забезпечення функціонування національної системи кібербезпеки 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, пункту 43 Плану розроблення технічних регламентів на 2018-2019 роки, затвердженого наказом Мінекономрозвитку від 15.02.2018 № 196.

Технічний регламент засобів криптографічного захисту інформації (далі – Технічний регламент), що затверджується проектом постанови, розроблено Інститутом проблем математичних машин та систем НАН України на замовлення Адміністрації Держспецзв'язку.

Технічний регламент установлює вимоги до продукції - засобів криптографічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом (далі – засоби КЗІ), оцінки їх відповідності та обігу на ринку України відповідно до вимог Закону України «Про технічні регламенти та процедури оцінки відповідності».

Технічний регламент засновано на національному стандарті України ДСТУ ISO/IEC 19790:2015 «Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів», затвердженому наказом державного підприємства «Український науково дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, та має посилання на переліки нормативних документів, які визначають суттєві вимоги до криптографічних модулів та оцінки їх відповідності та додаткові (опціональні) вимоги до криптографічних модулів.

Метою проекту постанови є:

встановлення вимог безпеки до засобів КЗІ відповідно до кращих європейських практик з урахуванням національних особливостей;

запровадження процедур виготовлення, обігу, оцінки відповідності засобів КЗІ відповідно до вимог Закону України «Про технічні регламенти та процедури оцінки відповідності»;

запровадження критеріїв та методології оцінки безпеки засобів КЗІ відповідно до міжнародних стандартів;

створення термінологічної бази у сфері КЗІ;

забезпечення відповідності засобів КЗІ, що є засобами кваліфікованого електронного підпису, вимогам Регламенту ЄС 910 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.

В процедурах оцінки відповідності засобів КЗІ застосовуються Модулі оцінки відповідності, які використовуються для розроблення процедур оцінки відповідності, затверджені постановою Кабінету Міністрів України від 13 січня 2016 року № 95.

**2. Адреси для зауважень та пропозицій до проекту акта**

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

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

поштова: вул. Солом'янська, 13, м. Київ, 03680; тел. (044) 281-90-10, (044) 281-94-83, факс (044) 226-26-83;

електронна: info@dsszzi.gov.ua;

- Державної регуляторної служби України:

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

електронна: inform@dkrp.gov.ua

**3. Обраний спосіб оприлюднення проекту акта**

Проект акта оприлюднюється в мережі Інтернет: проект постанови та аналіз регуляторного впливу.

**4. Строк, протягом якого приймаються зауваження та пропозиції**

Зауваження та пропозиції до проекту акта приймаються протягом 60 календарних днів з дня його оприлюднення.

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

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

«___» квітня 2018 р.

04/02/03-1290
23.04.18

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

| Зміст положення (норми) чинного законодавства | Зміст відповідного положення (норми) проекту акта |
|---|---|
| **Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 лютого 2006 року № 373** | |
| 22. Порядок проведення державної експертизи системи захисту, державної експертизи **та сертифікації** засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією. | 22. Порядок проведення державної експертизи системи захисту, державної експертизи засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією. |
| **Перелік видів продукції, щодо яких органи державного ринкового нагляду здійснюють державний ринковий нагляд, затверджений постановою Кабінету Міністрів України від 28 грудня 2016 р. № 1069** | |
| … | … … … |
| **Норма відсутня** | **45. Засоби криптографічного захисту інформації** \| **постанова Кабінету Міністрів України від _____ 2018 р. № _____ «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»** \| **Адміністрація Держспецзв'язку** |
| … | |

| 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:<br>…<br>**Норма відсутня**<br>… | 4. Адміністрація Держспецзв'язку відповідно до покладених на неї завдань:<br>…<br>**$7^{1}$) здійснює державний ринковий нагляд у межах сфери своєї відповідальності;**<br>… |

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

04/02/03- 128