Прим. № __

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стандартизація криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам

СТД-03-002-2026-В

ЗАХИСТ ІНФОРМАЦІЇ. ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. ЗАГАЛЬНІ ВИМОГИ

Київ
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
2026

СТД-03-002-2026-В

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: призначеним органом стандартизації у сфері криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам Державної служби спеціального зв’язку та захисту інформації України – Державним науково-дослідним інститутом технологій кібербезпеки та захисту інформації.

РОЗРОБНИКИ: **Д. Бондаренко**, керівник розробки; **О. Дирда**, канд. техн. наук; **Р. Цирень; О. Безсмертний**; **О. Юдін**, канд. техн. наук; **М. Терлецький**; **Н. Лисенко**; **Ф. Іванов**; **В. Жукович**; **Н. Заїка**; **Я. Стефанишин**; **І. Мартинюк**; **О. Пономарьов**.

2 ПОГОДЖЕНО: Адміністрацією Державної служби спеціального зв’язку та захисту інформації України (лист від 19.10.2026 № 04/03/02-28261/2026/ВН).

3 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: наказом Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації від 23.10.2026 р. № 134, з 30.10.2026 р.

4 Цей стандарт застосовується на добровільній основі, крім випадків, якщо обов’язковість його застосування встановлена нормативно-правовими актами.

5 Право власності на стандарти криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам належить державі в особі Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, який розповсюджує такі стандарти.

6 УВЕДЕНО ВПЕРШЕ.

ЗМІСТ

1 СФЕРА ЗАСТОСУВАННЯ 4
2 НОРМАТИВНІ ПОСИЛАННЯ 4
3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ 4
4 ПОЗНАКИ ТА СКОРОЧЕННЯ 8
5 ВИМОГИ ДО ЗАСОБУ КЗІ 9
5.1 Загальні положення 9
5.2 Загальні вимоги до засобів КЗІ 11
Додаток А (обов’язковий) Особливості застосування загальних вимог до засобів КЗІ 17
Бібліографія 19

1 СФЕРА ЗАСТОСУВАННЯ

1.1 Цей стандарт визначає загальні вимоги до засобів криптографічного захисту інформації (далі – засоби КЗІ).

1.2 Цей стандарт застосовний до суб'єктів, які беруть участь у розробленні, виробництві та експлуатації (використанні) засобів КЗІ.

1.3 Цей стандарт поширюється на всі засоби КЗІ, призначені для захисту відкритої інформації, вимога щодо захисту якої встановлена законом та інформації з обмеженим доступом.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті наведено посилання на такі нормативні документи:

ДСТУ ISO/IEC 15408-2:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки (ISO/IEC 15408-2:2022, IDT)

ISO/IEC 19790:2025 Information security, cybersecurity and privacy protection – Security requirements for cryptographic modules

Примітка. У разі заміни нормативного документа, на який наведено посилання, слід застосовувати новий нормативний документ. У разі скасування нормативного документа, на який наведено посилання, слід застосовувати останню чинну на момент застосування редакцію нормативного документа. Якщо до нормативного документа, на який наведено посилання, внесено зміни (поправки), застосовують цей нормативний документ з урахуванням усіх внесених до нього змін (поправок).

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті вжито терміни, наведені в ISO/IEC 19790:2025 [10].

Нижче подано терміни, додатково вжиті в цьому стандарті, та визначення позначених ними понять.

3.1 апаратний засіб

Засіб КЗІ, схвалені функції безпеки якого реалізовані в апаратних компонентах (програмованих логічних інтегральних схемах, контролерах,

процесорах тощо), а незмінне або обмежене операційне середовище (що охоплює апаратні компоненти та може охоплювати також вбудоване програмне забезпечення) є внутрішнім щодо криптографічної межі засобу

3.2 апаратно-програмний засіб

Засіб КЗІ, схвалені функції безпеки якого реалізовані в апаратних компонентах (програмованих логічних інтегральних схемах, контролерах, процесорах тощо) та в компонентах програмного забезпечення, водночас окремі компоненти програмного забезпечення засобу працюють в операційному середовищі, що є зовнішнім щодо криптографічної межі засобу

Примітка. В апаратно-програмних засобах КЗІ операційне середовище може бути змінним, незмінним або обмеженим. Апаратно-програмний засіб КЗІ може бути двох типів – гібридний програмний криптомодуль (hybrid software cryptomodule) та гібридний вбудований криптомодуль (hybrid firmware cryptomodule) [10].

3.3 життєвий цикл засобу КЗІ

Сукупність етапів існування засобу КЗІ, що описує послідовні зміни його стану (створення, впровадження, використання, виведення з експлуатації та утилізація), управління якими гарантує надійність виконання ним функцій захисту інформації

3.4 засіб КЗІ

Апаратний, програмний або апаратно-програмний засіб (криптомодуль), що реалізує у криптографічній межі схвалені функції безпеки

3.5 змінне операційне середовище *(modifiable operation environment*)

Операційне середовище, яке призначене для прийняття функціональних змін, що можуть містити неконтрольоване програмне забезпечення (може бути модифіковане, змінене або переконфігуроване)

3.6 клас безпеки засобу КЗІ

Визначений набір вимог до засобу КЗІ, що характеризує його здатність до реалізації функцій безпеки (зокрема, захищеність від атак, надійність реалізації криптографічних функцій тощо) для захисту відповідної категорії інформації

3.7 ключові дані (ключ)

Конкретний стан деяких параметрів криптографічного алгоритму, які забезпечують вибір одного криптографічного перетворення із сукупності усіх можливих для цього криптографічного алгоритму

3.8 криптоаналітично значущий квантовий комп'ютер (*cryptanalytically relevant quantum computer*)

Потужний квантовий комп'ютер з достатньо великою кількістю квантових бітів (кубітів), великим терміном перебування кубітів у стабільному стані та низькою ймовірністю помилки виконання квантових операцій, який може бути використаний на практиці для зламу реальних криптосистем

3.9 криптографічна межа

Чітко визначений периметр, який встановлює межу розташування всіх компонентів (апаратних та програмних) засобу КЗІ

3.10 криптографічна стійкість

Здатність криптографічного алгоритму протистояти спробам злому (криптоаналізу) та розшифрування інформації без доступу до ключа. Криптографічна стійкість визначається обчислювальною складністю найшвидшого на цей час алгоритму криптоаналізу

3.11 криптографічне перетворення інформації

Перетворення інформації за певним алгоритмом з метою приховування (відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства, дати створення тощо

3.12 криптографічний алгоритм

Математичний алгоритм, який визначає правила здійснення криптографічного перетворення інформації з використанням ключових даних або без них

3.13 критичний параметр безпеки (*critical security parameter, CSP*)

Інформація, пов’язана із безпекою, розкриття або модифікація якої може спричинити загрозу безпеці засобу КЗІ

3.14 незмінне операційне середовище *(non-modifiable operation environment*)

Операційне середовище, яке розроблено таким чином, щоб не приймати зміни вбудованого програмного забезпечення

3.15 обмежене операційне середовище (*limited operation environment*)

Операційне середовище, яке призначене для прийняття лише контрольованих змін вбудованого програмного забезпечення

3.16 операційне середовище (*operation environment*)

Операційна система (охоплюючи віртуальну(і) машину(и) та середовище, в якому виконується програмне забезпечення) та апаратне забезпечення, необхідні для роботи засобу КЗІ

Примітка. Операційне середовище може охоплювати інтегральні схеми, процесори, мікроконтролери, бібліотеки, керування пам’яттю, керування процесами, драйвери пристроїв для апаратного забезпечення, джерела живлення та корпуси

3.17 програмний засіб

Засіб КЗІ, схвалені функції безпеки якого реалізовані в програмному забезпеченні (яке функціонує в операційному середовищі), що є зовнішнім щодо криптографічної межі засобу

Примітка. У програмних засобах КЗІ операційне середовище може бути змінним, незмінним або обмеженим. Програмні засоби КЗІ можуть бути двох типів – програмний криптомодуль (software cryptomodule) та вбудований криптомодуль (firmware cryptomodule) [10].

3.18 публічний параметр безпеки (*public security parameter, PSP*)

Публічна інформація, пов’язана з безпекою, модифікація якої може скомпрометувати безпеку засобу КЗІ

3.19 схвалена функція безпеки

Криптографічні алгоритми та протоколи, методи захисту (генерації та встановлення SSP, автентифікації сутностей тощо), профілі захисту, технічні специфікації, що дозволені для реалізації у засобах КЗІ відповідно до законодавства

3.20 чутливий параметр безпеки (*sensitive security parameter, SSP*)

Критичні параметри безпеки та публічні параметри безпеки засобу КЗІ

4 ПОЗНАКИ ТА СКОРОЧЕННЯ

У цьому стандарті вжито такі познаки та скорочення:

ГВП – генератор випадкових послідовностей;

ГПВП – генератор псевдовипадкових послідовностей;

ДСТУ – державний стандарт України;

КЗІ – криптографічний захист інформації;

CSP – критичний параметр безпеки (*critical security parameter*);

IPsec – набір протоколів безпеки на мережевому рівні, який шифрує та автентифікує всі IP-пакети під час передачі даних (*internet protocol security*);

PSP – публічний параметр безпеки (*public security parameter*);

SSH – криптографічний мережевий протокол для безпечного віддаленого керування операційними системами та передачі файлів (*secure shell)*;

SSP – чутливий параметр безпеки (*sensitive security parameter*);

TLS – криптографічний протокол, який шифрує дані та забезпечує безпечний обмін інформацією між пристроями в мережі (наприклад, між браузером і веб-сайтом) (*transport layer security*).

5 ВИМОГИ ДО ЗАСОБУ КЗІ

5.1 Загальні положення

5.1.1 До засобів КЗІ належать засоби, які призначені для:

– шифрування інформації;

– виготовлення ключових даних або документів та управління ключовими даними, що використовуються засобами КЗІ;

– захисту від нав’язування неправдивої інформації або від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації (криптоалгоритми), зокрема засоби імітозахисту та цифрового підпису;

– розмежування доступу до інформації (засоби КЗІ, які здійснюють криптографічні перетворення для реалізації функцій автентифікації, розмежування доступу та/або контролю доступу до інформації).

5.1.2 Для захисту інформації, залежно від порядку доступу до неї, потрібно використовувати засоби КЗІ, які мають відповідний клас безпеки.

5.1.3 Залежно від порядку доступу до інформації, яка захищається, цей стандарт встановлює чотири класи безпеки засобу КЗІ:

– клас безпеки В – містить вимоги до захисту засобу КЗІ, який призначений для захисту відкритої інформації, вимога щодо захисту якої встановлена законодавством;

– клас безпеки К – містить вимоги до захисту засобу КЗІ, який призначений для захисту конфіденційної та/або таємної інформації, що не становить державної таємниці;

– клас безпеки С – містить вимоги до захисту засобу КЗІ, який призначений для захисту службової інформації;

– клас безпеки Т – містить вимоги до захисту засобу КЗІ, який призначений для захисту інформації, що становить державну таємницю.

Примітка. Клас безпеки наведено в порядку збільшення вимог таким чином, що рівень, наведений нижче, передбачає виконання вимог усіх наведених вище класів безпеки. Власник

інформації, яка захищається, обирає клас безпеки засобу КЗІ самостійно, але не нижче класу, визначеного для відповідного порядку доступу до інформації.

5.1.4 У засобах КЗІ можуть бути реалізовані такі компоненти безпеки:

1) специфікація/опис (характеристики) засобу КЗІ;

2) криптографічна стійкість криптографічних алгоритмів засобу КЗІ;

3) інтерфейси засобу КЗІ;

4) ролі, послуги та автентифікація;

5) безпека програмного забезпечення;

6) операційне середовище;

7) фізична безпека;

8) управління чутливими параметрами безпеки;

9) самотестування;

10) гарантії життєвого циклу.

5.1.5 Засоби КЗІ повинні бути розроблені таким чином, щоб забезпечити виконання таких функцій безпеки:

а) використання та реалізація схвалених функцій безпеки;

б) захист засобу КЗІ від несанкціонованого використання або експлуатації;

в) запобігання несанкціонованому розкриттю вмісту засобу КЗІ, у тому числі критичних параметрів безпеки;

г) запобігання несанкціонованій та непоміченій модифікації засобу КЗІ та криптографічних алгоритмів, у тому числі несанкціонованій модифікації, заміні, вставленню та видаленню чутливих параметрів безпеки;

д) інформування про робочий стан засобу КЗІ;

е) підтвердження, що засіб КЗІ коректно функціонує у схваленому режимі;

ж) виявлення помилок у роботі засобу КЗІ та запобігання компрометації SSP через помилки;

и) забезпечення належного проєктування, доставки, встановлення та підтримки засобу КЗІ.

5.1.6 У загальному випадку, у засобах КЗІ всіх чотирьох класів безпеки використовують однакові криптографічні методи та технології.

5.1.7 Засоби КЗІ повинні відповідати загальним вимогам безпеки у повному обсязі.

Примітка 1. Для засобів КЗІ класу безпеки В вимоги 5.2.2, 5.2.3 та 5.2.7 є необов'язковими [5].

Примітка 2. Для засобів КЗІ, які не використовуються (не експлуатуються) окремо, а є складовими частинами інших засобів, вимоги 5.2.3, 5.2.4, 5.2.5.1, 5.2.7, 5.2.8.2, 5.2.8.3, 5.2.8.4, 5.2.8.5 та 5.2.9 можуть не застосовуватися або застосовуватися обмежено, за умови реалізації цих вимог у засобах, в яких ці складові частини експлуатуються.

Примітка 3. Додаткові вимоги до засобів КЗІ, призначених для захисту службової інформації та інформації, що становить державну таємницю, встановлюються окремим стандартом.

5.1.8 За способом реалізації засіб КЗІ повинен належати до одного з таких типів:

– апаратний засіб;

– програмний засіб;

– апаратно-програмний засіб.

5.2 Загальні вимоги до засобів КЗІ

5.2.1 За компонентом безпеки «специфікація/опис (характеристики) засобу КЗІ»

5.2.1.1 Реалізація схвалених функцій безпеки повинна бути забезпечена виключно у визначеній криптографічній межі.

5.2.1.2 У засобі КЗІ повинні бути використані схвалені криптографічні алгоритми згідно із затвердженим переліком [6] або ті, на які за результатами експертних або тематичних досліджень Адміністрацією Держспецзв'язку видано позитивний експертний висновок.

5.2.2 За компонентом безпеки «криптографічна стійкість криптографічних алгоритмів засобу КЗІ» криптографічна стійкість криптографічного алгоритму, який використовується у засобі КЗІ для забезпечення конфіденційності

інформації, до класичних (неквантових) методів криптоаналізу має бути не менше ніж 10^{38}.

Примітка. У перехідний період до появи криптоаналітично значущого квантового комп'ютера нижня межа криптографічної стійкості відносно квантових методів криптоаналізу у цьому стандарті не визначена.

5.2.3 За компонентом безпеки «інтерфейси засобу КЗІ»

5.2.3.1 Повинно бути реалізовано розділення інтерфейсів засобу КЗІ для запобігання порушенню конфіденційності та цілісності чутливих параметрів безпеки.

Примітка 1. Всі логічні інформаційні потоки повинні передаватися лише через фізичні порти доступу та логічні інтерфейси, які визначені як точки входу та виходу через криптографічну межу засобу КЗІ.

Примітка 2. Логічні канали, через які засіб КЗІ приймає команди управління або чутливі параметри безпеки, мають бути повністю відокремлені від каналів, через які передаються зашифровані/розшифровані дані користувача.

5.2.3.2 Повинна бути забезпечена реалізація довіреного каналу для отримання інформації, яка підлягає захисту, у тому числі, публічних параметрів безпеки, зокрема, сертифікатів відкритих ключів асиметричних криптографічних алгоритмів.

Примітка. Довірений канал може бути реалізований криптографічними методами з використанням механізмів захисту SSP, зокрема, з використанням протоколів IPsec, TLS, SSH тощо, а також шляхом локального підключення до портів засобу КЗІ, які призначені для передавання даних.

5.2.4 За компонентом безпеки «ролі, послуги та автентифікація засобу КЗІ» повинна бути забезпечена реалізація механізмів розмежування доступу до функцій засобу КЗІ (послуг) та критичних параметрів безпеки.

Примітка 1. Застосовується розділення ролей на адміністратора (криптоофіцера) та оператора (користувача) засобу КЗІ. За необхідності, може бути застосована роль «технік з обслуговування засобу КЗІ» [7]. Надання повноважень для ролі стосовно доступу до засобу КЗІ повинно здійснюватися залежно від визначеної політики безпеки за результатами авторизації користувача.

Примітка 2. Доступ до функцій засобу КЗІ повинен надаватися тільки після успішної автентифікації користувача.

5.2.5 За компонентом безпеки «безпека програмного забезпечення засобу КЗІ»

5.2.5.1 Повинна бути забезпечена реалізація механізмів контролю цілісності програмного забезпечення засобу КЗІ (що реалізує функції, неправильне виконання яких може призвести до порушення конфіденційності, цілісності та автентичності інформації).

Примітка 1. Контроль цілісності програмного забезпечення реалізується з використанням схвалених:

– функцій гешування;

– кодів автентифікації повідомлень;

– алгоритмів цифрового підпису.

Примітка 2. Вимога не застосовується у разі апаратної реалізації засобу КЗІ без використання програмного забезпечення.

5.2.5.2 Повинна бути забезпечена реалізація механізмів захисту чутливих параметрів безпеки засобу КЗІ від недокументованих можливостей прикладного програмного забезпечення.

Примітка. Цей механізм захисту для програмних засобів КЗІ може здійснюватися шляхом виконання програмного забезпечення в ізольованих середовищах.

5.2.6 За компонентом безпеки «операційне середовище засобу КЗІ» повинна бути забезпечена реалізація механізмів інформування про стан засобу КЗІ, логування (протоколювання або запис) подій.

Примітка. Для журналів подій повинні бути запроваджені механізми, які перешкоджають несанкціонованим діям згідно з політикою безпеки, зокрема їх видалення, внесення змін, несанкціонованого перегляду тощо.

5.2.7 За компонентом безпеки «фізична безпека засобу КЗІ» повинна бути забезпечена реалізація механізмів фізичної безпеки засобу КЗІ (міцні корпуси, печатки (наприклад, у вигляді голографічних стрічок чи металевих пломб), апаратні механізми захисту мікрочипів тощо) з метою запобігання або виявлення несанкціонованих дій з SSP.

Примітка. Вимога не застосовується до програмних засобів КЗІ.

5.2.8 За компонентом безпеки «управління чутливими параметрами безпеки засобу КЗІ»

5.2.8.1 Генерацію критичних параметрів безпеки, зокрема ключових даних, необхідно виконувати, використовуючи один із запропонованих нижче типів генераторів:

– апаратний генератор випадкових послідовностей (ГВП) зі схемою вирівнювання статистичних характеристик. Вихідна випадкова послідовність, що генерується ГВП, повинна відповідати вимогам ДСТУ ISO/IEC 18031 [8];

– програмний генератор псевдовипадкових послідовностей (ГПВП), який для ініціалізації використовує фізичне (апаратне) джерело ентропії. При цьому криптографічна стійкість алгоритму генерації ПВП повинна бути не менше ніж 10^{38}.

Примітка. Методика генерації критичних параметрів безпеки повинна бути погоджена з Адміністрацію Держспецзв'язку.

5.2.8.2 У засобі КЗІ повинні бути реалізовані механізми захисту ключових даних від порушення конфіденційності та цілісності, у тому числі на носіях ключових даних.

Примітка. Для захисту ключових даних можуть бути використані [7]:
– захищені носії даних на базі криптопроцесора;
– захищені ділянки пам'яті мікропроцесорів або мікроконтролерів;
– файлові криптоконтейнери;
– механізми захисту оперативної пам'яті (де тимчасово перебувають ключові дані під час обчислень) від читання або модифікації іншими процесами;
– механізми розділення секрету тощо.

5.2.8.3 Повинна бути забезпечена реалізація механізмів захисту від порушення конфіденційності критичних параметрів безпеки або несанкціонованої та непоміченої модифікації засобу КЗІ і криптографічних алгоритмів, у тому числі несанкціонованої модифікації, заміни, встановлення та видалення схвалених функцій, внаслідок помилкових дій оператора або відхилень у роботі складових елементів засобу КЗІ.

Примітка 1. Механізм захисту може охоплювати:

– блокування команд (наприклад, вивантаження ключів у відкритому вигляді) на рівні програмного коду. Навіть якщо користувач помилково або навмисно виконає зазначену команду, повинна виникнути системна помилка із забороною операції експорту ключа;

– постійний контроль роботи складових елементів засобу КЗІ у процесі їх експлуатації;

– блокування сесії керування засобом КЗІ у разі бездіяльності користувача протягом певного часу.

Примітка 2. Повинно бути впроваджено автоматизований (без задіяння користувача) процес виконання критичних операцій щодо керування ключовими даними, виконання криптографічних операцій тощо.

5.2.8.4 Повинна бути забезпечена реалізація механізмів знищення ключових даних після закінчення строку їх дії.

Примітка 1. Повинен бути визначений строк дії ключових даних та вимоги щодо їх знищення. Наприклад, формат вимоги може бути викладений таким способом:

– «*знищення ключових даних в оперативній памяті відбувається відразу після завершення криптографічної операції*»;

– «*сеансовий ключ шифрування інформації повинен знищуватися в оперативній пам'яті, одразу після завершення сеансу захищеного обміну даними, шляхом перезапису відповідних ділянок нульовою або псевдовипадковою послідовністю*».

Примітка 2. Знищення ключових даних на електронних носіях і в оперативній пам'яті повинно здійснюватися шляхом запису у ділянки, де розміщувалися ключі, фіксованих або випадкових даних. Для магнітних носіїв повинен використовуватися багаторазовий (не менше ніж три) перезапис ділянок випадковими даними. Також носії ключових даних можуть знищуватись фізично шляхом руйнування, спалення тощо.

5.2.8.5 Повинна бути забезпечена реалізація механізмів знищення критичних параметрів безпеки у разі спроби несанкціонованого доступу до засобу КЗІ.

Примітка 1. Знищення критичних параметрів безпеки повинно відбуватися автоматично (без участі оператора) у разі несанкціонованого доступу до засобу КЗІ. В обґрунтованих випадках, може бути реалізовано режим знищення критичних параметрів безпеки за командою оператора.

Примітка 2. Для засобів КЗІ класу безпеки В та К під спробою несанкціонованого доступу можна вважати момент перевищення максимальної кількості спроб введення неправильних даних під час автентифікації оператора [7].

5.2.9 За компонентом безпеки «самотестування засобу КЗІ» повинна бути забезпечена реалізація механізмів самотестування засобу КЗІ на правильність роботи усіх функцій, неправильне виконання яких може призвести до порушення конфіденційності, цілісності та автентичності інформації, а також блокування роботи засобу КЗІ у разі виникнення помилки тестування.

Примітка. Самотестування засобу КЗІ може здійснюватися одним або кількома з таких методів:

– виконання тестів з відомою відповіддю для криптографічних алгоритмів та протоколів;

– статистичне тестування генераторів випадкових послідовностей;

– дублювання окремих функцій із порівнянням ідентичності результатів;

– перевірка цілісності та автентичності програмного забезпечення;

– перевірка криптографічних ключів (наприклад, відповідності відкритих та секретних ключів асиметричних криптоалгоритмів);

– перевірка працездатності систем контролю та блокування (наприклад, напруги джерел живлення системи захисту від несанкціонованого доступу).

5.2.10 За компонентом безпеки «гарантії життєвого циклу засобу КЗІ» вміст документації на засіб КЗІ повинен відповідати додатку A ISO/IEC 19790 [10].

5.2.11 Вміст політики безпеки засобу КЗІ повинен відповідати додатку B ISO/IEC 19790 [10].

Примітка. Вищевикладені особливості застосування вимог до засобів КЗІ за класами безпеки наведено у додатку А.

ДОДАТОК А
(обов'язковий)

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ЗАГАЛЬНИХ ВИМОГ ДО ЗАСОБІВ КЗІ

Особливості застосування вимог до засобів КЗІ за класами безпеки наведено у таблиці А.1.

Таблиця А.1 – Застосування вимог до засобів КЗІ за класами безпеки

Компоненти безпеки засобу КЗІ	**Склад вимог**	**Вимоги до засобів КЗІ за класами безпеки**			
		В	**К**	**С***	**Т***
1	2	3	4	5	6
Специфікація/опис (характеристики)	5.2.1	+	+	+	+
Криптографічна стійкість криптографічних алгоритмів	5.2.2	Вимоги не обов'язкові**	+	+	+
Інтерфейси	5.2.3	Вимоги не обов'язкові	+	+	+
		Вимоги можуть не застосовуватися повністю або обмежено для засобів КЗІ, які не використовуються (не експлуатуються) окремо, а є складовими частинами інших засобів за умови, що вимоги реалізовані у їх складових частинах			
Ролі, послуги та автентифікація	5.2.4	+	+	+	+
		Вимоги можуть не застосовуватися повністю або обмежено для засобів КЗІ, які не використовуються (не експлуатуються) окремо, а є складовими частинами інших засобів за умови, що вимоги реалізовані у їх складових частинах			
Безпека програмного забезпечення	5.2.5	+	+	+	+
		Вимоги 5.2.5.1 можуть не застосовуватися повністю або обмежено для засобів КЗІ, які не використовуються (не експлуатуються) окремо, а є складовими частинами інших засобів за умови, що вимоги реалізовані у їх складових частинах			
Операційне середовище	5.2.6	+	+	+	+

Продовження таблиці

1	2	3	4	5	6
Фізична безпека	5.2.7	Вимоги не обов’язкові	+	+	+
		Вимоги можуть не застосовуватися повністю або обмежено для засобів КЗІ, які не використовуються (не експлуатуються) окремо, а є складовими частинами інших засобів за умови, що вимоги реалізовані у їх складових частинах			
Управління чутливими параметрами безпеки	5.2.8	+	+	+	+
		Вимоги 5.2.8.2 – 5.2.8.5 можуть не застосовуватися повністю або обмежено для засобів КЗІ, які не використовуються (не експлуатуються) окремо, а є складовими частинами інших засобів за умови, що вимоги реалізовані у їх складових частинах			
Самотестування	5.2.9	+	+	+	+
		Вимоги можуть не застосовуватися повністю або обмежено для засобів КЗІ, які не використовуються (не експлуатуються) окремо, а є складовими частинами інших засобів за умови, що вимоги реалізовані у їх складових частинах			
Гарантії життєвого циклу	5.2.10	+	+	+	+
** додаткові вимоги до засобів КЗІ, призначених для захисту службової інформації та інформації, що становить державну таємницю, встановлюються окремим стандартом* *** вимоги не обов’язкові, якщо засіб не використовується для забезпечення конфіденційності інформації*					

БІБЛІОГРАФІЯ

1 Закон України «Про інформацію»;

2 Закон України «Про доступ до публічної інформації»;

3 Закон України «Про державну таємницю»;

4 Закон України «Про критичну інфраструктуру»;

5 Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»;

6 Перелік стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 27.10.2020 № 687, зареєстрований у Міністерстві юстиції України 21.12.2020 за № 1272/35555 (із змінами);

7 ДСТУ ISO/IEC 15408-2:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки (ISO/IEC 15408-2:2022, IDT);

8 ДСТУ ISO/IEC 18031:2015 Інформаційні технології. Методи захисту. Генерування випадкових бітів (ISO/IEC 18031:2011/Amd 1:2017, IDT);

9 ISO/IEC 15408-2:2026 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security. Part 2: Security functional components;

10 ISO/IEC 19790:2025 Information security, cybersecurity and privacy protection – Security requirements for cryptographic modules.

Коди згідно з КСД 001: 03.04;

НК 004: 35.030

Ключові слова: криптографічний захист інформації, засоби КЗІ, вимоги до засобів КЗІ, клас безпеки засобу КЗІ, схвалена функція безпеки, криптографічна межа, криптографічний алгоритм.