ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

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

СТД-02.03-001-2026-В

ЗАХИСТ ІНФОРМАЦІЇ. ЗАСОБИ КРИПТОГРАФІЧНОГО ТА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. ПОРЯДОК ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ

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

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: Робоча група із стандартизації РГ02 «ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ», робоча група із стандартизації РГ03 «КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

2 ПОГОДЖЕНО: Адміністрацією Державної служби спеціального зв'язку та захисту інформації України «___» _____ 2026 р. № _____.

3 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ наказом Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації від «____» _____ 2026 р. № _____, з «____» _____ 2026 р.

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

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

5 УВЕДЕНО ВПЕРШЕ.

ЗМІСТ

1 СФЕРА ЗАСТОСУВАННЯ

1.1 Стандарт Державної служби спеціального зв’язку та захисту інформації «Захист інформації. Засоби криптографічного та технічного захисту інформації. Порядок експертних досліджень» (далі – Стандарт) визначає порядок експертних досліджень засобів криптографічного та технічного захисту інформації (далі – засоби) з урахуванням критеріїв та методологій оцінювання безпеки інформаційних технологій (далі – ІТ), визначених національними стандартами України ДСТУ ISO/IEC 15408:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ» (Частини 1-5) та ДСТУ ISO/IEC 18045:2023 (ISO/IEC 18045:2022, IDT). «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ».

1.2 Стандарт застосовний до суб’єктів експертних досліджень у сфері криптографічного захисту інформації (далі – КЗІ) та/або технічного захисту інформації (далі – ТЗІ).

1.3 Стандарт поширюється на засоби КЗІ (крім тих, що призначені для захисту службової інформації і інформації, що становить державну таємницю) та засоби ТЗІ (крім експертних досліджень їх властивостей захисту інформації від витоку технічними каналами та від спеціального впливу на засоби обробки інформації).

2 НОРМАТИВНІ ПОСИЛАННЯ

У Стандарті наведено посилання на такі нормативні документи:

ДСТУ ISO/IEC 15408-1:2023 (ISO/IEC 15408-1:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель;

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

ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення;

ДСТУ ISO/IEC 15408-4:2023 (ISO/IEC 15408-4:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності;

ДСТУ ISO/IEC 15408-5:2023 (ISO/IEC 15408-5:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки;

ДСТУ ISO/IEC 18045:2023 (ISO/IEC 18045:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ.

Примітки:

1. У разі заміни нормативного документу, на який наведено посилання, слід застосовувати новий нормативний документ. У разі скасування нормативного документу, на який наведено посилання, слід застосовувати останню чинну на момент застосування редакцію нормативного документу. Якщо до нормативного документу, на який є посилання, внесено зміни/поправки, треба застосовувати новий нормативний документ, охоплюючи всі внесені зміни/поправки до нього.

2. Специфікації та документи, що застосовують положення цього Стандарту, можуть мати посилання на загальнодоступні стандарти (Common Criteria for Information Technology Security Evaluation (CC) та Common Methodology for Information Technology Security Evaluation (CEM))3, які відображені у положеннях державних стандартів України, наведених у цьому розділі.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У Стандарті вжито терміни, наведені в ДСТУ ISO/IEC 15408-1 [2].

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

3.1 **Визначення проблеми безпеки** (*Security Problem Definition, SPD*) – твердження, яке формальним чином визначає характер та обсяг безпеки, яку має охопити об’єкт експертних досліджень;

3.2 **Вимога гарантії безпеки** (*Security Assurance Requirement, SAR*) – вимога безпеки, що стосується умов та процесів розроблення та реалізації об’єкта експертних досліджень, а також дій, що вимагаються від експертної організації щодо доказів, отриманих за цих умов та процесів;

3.3 **Об’єкт експертних досліджень** (*Target Of Evaluation, TOE*) – набір програмного забезпечення, вбудованого програмного забезпечення (прошивки) та/або апаратного забезпечення, що є засобами, а також документації щодо процесів їх розробки, проєктування, виробництва, постачання та експлуатації;

3.4 **Профіль захисту** (*Protection Profile, PP*) – це опис загальних вимог до певного типу TOE, який можна використовувати як шаблон для різних ST, які будуть застосовуватися в різних експертних дослідженнях;

3.5 **Рівень гарантії оцінювання** (*Evaluation Assurance Level, EAL*) – пакет SAR, що визначає обсяг та глибину експертних досліджень відповідно до рівня, визначеного за шкалою з ДСТУ ISO/IEC 15408-5 [6];

3.6 **Технічний протокол експертних досліджень** (*Evaluation Technical Report, ETR*) – документація щодо результатів експертних досліджень (загальний вердикт) та їх обґрунтування, підготовлена експертною організацією та подана до експертного органу;

3.7 **Технічні вимоги** (*Security Target, ST*) – документ замовника, що описує конкретний TOE та вимоги, реалізація яких має бути підтверджена за результатами експертних досліджень;

3.8 **Функціональна вимога безпеки** (*Security Functional Requirement, SFR*) – вимога безпеки TOE, яка спрямована на вирішення проблеми безпеки відповідно до ST або PP TOE.

4 ПОЗНАКИ ТА СКОРОЧЕННЯ

У Стандарті вжито такі познаки та скорочення:

ДСТУ – державний стандарт України;

КЗІ – криптографічний захист інформації;

ТЗІ – технічний захист інформації;

ALC – клас гарантії: підтримка життєвого циклу (*Assurance Class: Life-cycle Support*);

ATE – клас гарантії: тести (*Assurance Class: Tests*);

CC – загальні критерії (*Common Criteria*);

EAL – рівень гарантії оцінювання (*Evaluation Assurance Level*);

ETR – технічний протокол експертних досліджень (*Evaluation Technical Report*);

IEC – міжнародна електротехнічна комісія (*International Electrotechnical Commission*);

ISO – міжнародна організація зі стандартизації (*International Organization for Standardization*);

IT – інформаційні технології (*Information Technology*);

PP – профіль захисту (*Protection Profile*);

SAR – вимога гарантії безпеки (*Security Assurance Requirement*);

SFR – функціональна вимога безпеки (*Security Functional Requirement*);

SPD – визначення проблеми безпеки (*Security Problem Definition*);

ST – технічні вимоги (*Security Target*);

TOE – об’єкт експертних досліджень (*Target of Evaluation*);

TSF – функції безпеки об’єкта експертних досліджень (*TOE Security Functions*)

5 ПОРЯДОК ПРОВЕДЕННЯ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ ЗАСОБІВ

5.1 Загальна модель

Загальна модель проведення експертних досліджень, яка забезпечує конкретизацію способів застосування положень серії стандартів ДСТУ ISO/IEC 15408 [2-6] та ДСТУ ISO/IEC 18045 [7] під час проведення експертних

досліджень засобів, описує ролі суб’єктів експертних досліджень та вимоги до них.

5.2 Суб’єкти

Перелік суб’єктів експертних досліджень включає:

а) замовника (виробник/спонсор);

б) експертну організацію;

в) експертний орган.

5.3 Замовник

5.3.1 Замовник здійснює збір усіх елементів об’єкта експертних досліджень (TOE), підготовку технічних вимог (ST), обирає експертну організацію, взаємодіє з експертною організацією з метою визначення обсягу експертних досліджень та вирішення інших питань щодо їх проведення.

5.3.2 Обов’язки замовника, з урахуванням положень Стандарту, визначаються вимогами чинного законодавства.

5.4 Експертна організація

5.4.1 Експертна організація проводить експертні дослідження засобів.

5.4.2 Експертна організація повинна бути незалежною та не мати будь-якого конфлікту інтересів. Експертна організація не повинна бути залучена до процесів проєктування, виробництва, постачання, складання, використання або технічного обслуговування засобів, відносно яких проводяться експертні дослідження.

5.4.3 Експертна організація повинна мати технічну компетенцію у проведенні експертних досліджень засобів та бути здатною виконати всі завдання з експертних досліджень засобу відповідно до Стандарту, незалежно від того, чи виконує такі завдання самостійно, чи їх виконання здійснюється від її імені або під її відповідальність.

5.4.4 До початку експертних досліджень засобу, експертна організація повинна щонайменше мати:

а) персонал з технічними знаннями та достатнім відповідним досвідом для виконання експертних досліджень;

б) опис процедур, на підставі яких проводяться експертні дослідження, задокументований із рівнем деталізації достатнім для забезпеченням можливості їх розуміння та відтворення;

в) обладнання, необхідне для проведення експертних досліджень.

5.4.5 Співробітники експертної організації повинні бути вільними від тиску і стимулів, які могли б вплинути на їхнє рішення або результати їхньої експертної діяльності, зокрема, тиску або стимулів фінансового характеру.

5.4.6 Обов’язки експертної організації та підтвердження її спроможностей, з урахуванням положень Стандарту, визначаються вимогами чинного законодавства.

5.5 Експертний орган

5.5.1 Експертний орган розглядає матеріали з питань експертних досліджень засобів, які надходять від замовників та експертних організацій.

5.5.2 За результатами розгляду матеріалів з питань експертних досліджень, у разі їх повноти та відповідності встановленим вимогам, експертний орган видає експертний висновок [1] на засіб.

5.5.3 Співробітники експертного органу повинні бути вільними від тиску і стимулів, які могли б вплинути на їхнє рішення або результати їхньої експертної діяльності, зокрема, тиску або стимулів фінансового характеру.

5.5.4 Співробітники експертного органу повинні мати досвід роботи, пов'язаний з виробництвом/проектуванням/випробуванням засобів, не менше 1 року.

5.5.5 Співробітники експертного органу повинні мати підтверджуючі документи щодо проходження навчань/підвищення кваліфікацій відповідно до напрямку діяльності експертного органу.

5.6 Об’єкт експертних досліджень (TOE)

5.6.1 Технічні вимоги (ST) об’єкта експертних досліджень (TOE) базуються на типових наборах рівнів гарантій оцінювання (EAL) або профілів захисту (PP), які описують проблеми та вимоги безпеки для певного типу засобу.

5.6.2 Мінімальний обсяг експертних досліджень визначається вимогами ДСТУ ISO/IEC 15408-5 [6] до рівня гарантії оцінювання EAL1.

5.6.3 За необхідності, замовник може, до визначеного рівня EAL обрати додаткові вимоги до гарантій безпеки (SAR), вищий EAL або PP, який базується на типовому наборі EAL.

5.6.4 Вимоги щодо обсягу експертних досліджень визначаються у ST.

5.7 Процедура експертних досліджень

Процедура експертних досліджень складається з наступних етапів.

5.7.1 Підготовчий етап:

а) збір замовником усіх елементів TOE та підготовка ST;

б) обрання замовником експертної організації, встановлення з нею взаємовідносин та обговорення умов проведення експертних досліджень.

5.7.2 Основний етап:

а) проведення експертною організацією експертних досліджень за методологією ДСТУ ISO/IEC 18045 [7];

б) підготовка експертною організацією технічного протоколу експертних досліджень та звіту про експертні дослідження та їх подання до експертного органу.

5.7.3 Підсумковий етап:

а) опрацювання експертним органом наданих експертною організацією матеріалів експертних досліджень і прийняття рішення щодо можливості видачі експертного висновку та визначення терміну його дії;

б) видача експертним органом експертного висновку, його публікація разом з ST та звітом про експертні дослідження, отриманим від експертної організації.

5.8 Технічні вимоги (ST)

5.8.1 Загальні структура та зміст ST до об’єкта експертних досліджень наведені у додатку А до Стандарту, а деталізовані положення щодо його написання та наповнення визначені у розділі 12 та додатку D ДСТУ ISO/IEC 15408-1 [2].

5.8.2 Експертним дослідженням повинні підлягати всі функції, які зазначені в ST.

5.8.3 У разі наявності в ST будь-якої інформації з обмеженим доступом (захищена авторським правом пропрієтарна, конфіденційна, службова чи секретна інформація), замовник готує окрему редакцію ST, з якої повинна бути виключена така інформація шляхом видалення або перефразування, та подає її до експертної організації разом з оригінальним ST, для забезпечення можливості подальшого її опублікування експертним органом.

5.9 Технічний протокол експертних досліджень (ETR)

ETR є документом, який готує експертна організація за результатами виконання експертних досліджень за методологією ДСТУ ISO/IEC 18045 [7]. Цей документ повинен містити детальні результати перевірки ТОЕ на відповідність критеріям ДСТУ ISO/IEC 15408 [2-6] у межах, визначених ST.

Загальні структура та зміст ETR наведені у додатку Б до Стандарту, а деталізовані положення щодо написання ETR та його наповнення визначені ДСТУ ISO/IEC 18045 [7].

5.10 Звіт про експертні дослідження

5.10.1 Звіт про експертні дослідження є для заінтересованих споживачів джерелом детальної практичної інформації про безпеку засобу.

5.10.2 Звіт про експертні дослідження не повинен містити інформацію з обмеженим доступом (захищену авторським правом пропрієтарну, конфіденційну, службову чи секретну інформацію), оскільки, як і ST, він містить інформацію для споживача, необхідну для безпечного застосування засобу.

5.10.3 Якщо експертний орган визначив додаткову інформацію, що повинна бути доступною споживачеві (наприклад, пов’язаний PP [11] або інші підтверджуючі документи), вона повинна міститися або бути легкодоступною через точне посилання у звіті про експертні дослідження.

5.10.4 Структура та зміст звіту про експертні дослідження наведені у додатку В до Стандарту.

5.11 Експертний висновок

5.11.1 Експертний висновок [1] за результатами експертних досліджень видається експертним органом, з урахуванням характеристик досліджуваного засобу, на строк, що не перевищує 5 років.

5.11.2 У експертному висновку повинні бути вказані, щонайменше:

а) унікальний номер експертного висновку та дата видачі;

б) повна назва власника експертного висновка (замовника);

в) найменування та версія засобу, який пройшов процедуру експертних досліджень;

г) посилання на ST та звіт про експертні дослідження засобу, який пройшов процедуру експертних досліджень;

д) набір гарантій (EAL) та додаткові вимоги до гарантій безпеки, включно з рівнем AVA_VAN [8] (якщо вони відрізняються від заявленого типового набору EAL), що застосовувалися під час експертних досліджень, або PP, якому відповідає засіб;

е) назва експертної організації, яка проводила експертні дослідження;

ж) термін дії експертного висновку.

5.12 Процедура внесення змін/оновлень до ТОЕ

5.12.1 Для забезпечення можливості усунення вразливостей/оновлення ТОЕ упродовж терміну життєвого циклу, у складі його ST повинен бути визначений відповідний функціонал, який підлягатиме оцінюванню.

За наявності функціоналу усунення вразливостей/оновлення ТОЕ, усі зміни повинні контролюватися таким чином, щоб забезпечити збереження довіри до вже оцінених елементів ТОЕ.

5.12.2 Наслідком внесення будь-яких змін до ТОЕ, без дотримання визначеного у ST алгоритму усунення вразливостей/оновлення, є втрата попередніх результатів оцінювання.

5.12.3 Можливі зміни ТОЕ (усунення вразливостей або оновлення) поділяються на:

а) суттєві зміни (*Major Changes*) (зміни архітектури, нові механізми автентифікації/авторизації, контролю доступу, зміни криптографічних функцій, зміна поведінки функціональних вимог безпеки (SFR), зміни або інтеграція нового ядра, тощо) потребують окремих експертних досліджень відповідно до визначеної процедури, при цьому експертним органом видається експертний висновок на нову версію засобу (наприклад, v2.0).

У разі суттєвих змін ТОЕ експертний висновок на попередню версію засобу оголошується недійсним або чинним до певної дати;

б) несуттєві зміни (*Minor Changes*) (патчі без зміни TSF, оновлення драйверів без впливу на політики безпеки, оновлення документації тощо) потребують проходження визначених процедур ALC та ATE, документування та повідомлення експертного органу, без необхідності повторних експертних досліджень у повному обсязі.

У разі несуттєвих змін ТОЕ та з урахуванням його складу та архітектури засобу розробник повинен:

а) визначити та ідентифікувати у ST усі елементи, будь-яка зміна яких вважатиметься суттєвою зміною ТОЕ;

б) визначити подальший порядок ідентифікації та маркування (елементів) ТОЕ після несуттєвих змін.

5.12.4 Процедура внесення змін до ТОЕ передбачає, що розробник повинен:

а) провести відповідний аналіз та визначити обсяг змін;

б) у разі суттєвих змін провести окремі експертні дослідження за визначеною процедурою;

в) у разі несуттєвих змін:

1) довести, що вони не створюють нових загроз та не порушують перевірені SFR;

2) провести тестування та задокументувати його результати із застосуванням оцінених процесів усунення вразливостей/оновлення;

3) за необхідності оновити експлуатаційну документацію;

г) надати експертному органу аналіз змін, результати окремих експертних досліджень або тестування та відповідну документацію.

5.12.5 У разі несуттєвих змін, за рішенням експертного органу оновлена версія ТОЕ вважається такою, що відповідає оригінальному експертному висновку (для цього експертний орган готує звіт про зміни «Maintenance Report» згідно з вимогами [10] та викладає його як доповнення до звіту про експертні дослідження), або видається нова версія експертного висновку (без нової оцінки) із зазначенням «Застосовано дії щодо змін (Maintenance action applied)».

5.12.6 Для реалізації процедур змін «Maintenance» доцільно керуватися «Assurance Continuity: CCRA REQUIREMENTS» [10].

5.12.7 Алгоритм усунення вразливостей/оновлення має бути формально описаний в ST як компонент гарантій (SAR), а саме клас рівня гарантії ALC_FLR з компонентом виправлення недоліків/вразливостей «Flaw Remediation» та детально викладений у технічній документації ТОЕ.

5.12.8 За замовчуванням ALC_FLR не входить у типові набори EAL, тому для можливості внесення оновлень/патчів ТОЕ оцінюють на рівень EAL+

доповнений з ALC_FLR «augmented with ALC_FLR», що передбачає перевірку процесу виробника щодо виправлення помилок та внесення оновлень.

5.12.9 Включення ALC_FLR в ST та підтвердження його реалізації за результатами експертних досліджень означає, що:

а) оцінено політики та існують процедури виробника щодо відстеження та виправлення недоліків;

б) виробник зобов’язаний дотримуватися процедур та відстежувати всі повідомлені недоліки безпеки (вразливості);

в) для кожного недоліку (вразливості) мають бути визначені коригувальні дії – виправлення (патчі);

г) процедури повинні гарантувати, що самі виправлення не вносять нових вразливостей (регресійне тестування);

д) розробник повинен мати методи інформування користувачів про помилки/вразливості та надання виправлень.

5.12.10 Можливе використання розширених вимог безпеки (extended security requirements), які не базуються на компонентах ДСТУ ISO/IEC 15408-3 [4], але визначені PP, або окремим стандартом, наприклад, ISO/IEC TS 9569:2023 [9], який вводить поняття керування виправленнями «patch-management» як компонент забезпечення безпеки ALC_PAM (Patch Management).

ДОДАТОК А

(обов’язковий)

ФОРМА ТЕХНІЧНИХ ВИМОГ ДО ОБ’ЄКТА ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ

ПОГОДЖЕНО

_____
(посада, підпис, власне ім’я, прізвище керівника експертної організації)

“___” _____ 20 __ року

ЗАТВЕРДЖУЮ

_____
(посада, підпис, власне ім’я, прізвище керівника експертного органу)

“___” _____ 20 __ року

ТЕХНІЧНІ ВИМОГИ
ДО ОБ’ЄКТА ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ (ST)

_____
_____
Версія (унікальний ідентифікатор ST)

на ___ арк.

ПОГОДЖЕНО

_____
(посада, підпис, власне ім’я, прізвище керівника організації Замовника)

“___” _____ 20 __ року

1 Загальні характеристики об’єкта експертних досліджень

1.1 Ідентифікаційні дані про об’єкт експертних досліджень

1.1.1 Назва засобу _____

1.1.2 Тип _____

1.1.3 Ідентифікатор _____
(версія, модель, модифікація тощо)

1.1.4 Унікальні ідентифікатори складових частин засобів _____
(номер, версія тощо)

1.1.5 Реквізити виробника засобу _____

1.1.6 Реквізити замовника експертних досліджень _____

1.2 Огляд об’єкта експертних досліджень

1.2.1 Умови експлуатації засобу _____

1.2.2 Основні функції безпеки _____

1.2.3 Ідентифікаційні дані допоміжних засобів _____
(номер, версія тощо допоміжного апаратно-

_____
програмного забезпечення, яке не є частиною засобу, але необхідне для забезпечення його роботи)

1.3 Опис об’єкта експертних досліджень

1.3.1 Перелік складових частин засобу _____
(апаратне, програмне забезпечення, прошивки)

1.3.2 Перелік та ідентифікатори усіх складових ТОЕ, будь-яка зміна яких вважатиметься суттєвою зміною ТОЕ _____

1.3.3 Основні функції _____

1.3.4 Функції безпеки _____

Примітка. Функції об’єкта експертних досліджень наводяться таким чином, щоб не залишалося жодних сумнівів щодо того, чи певна функція входить до його складу, чи вона знаходиться поза його межами.

1.3.5 Перелік керівних документів _____

1.3.6 Порядок ідентифікації та маркування (елементів) ТОЕ після внесення несуттєвих змін _____

2 Заяви про відповідність

2.1 Застосовані стандарти _____
(версії ДСТУ ISO/IEC 15408, ДСТУ ISO/IEC 18045 інші)

2.2 Відповідність профілям захисту _____
(при застосуванні – найменування, номер, коли і ким затверджено)

2.3 Відповідність пакетам вимог _____
(пакети SFR та SAR, які мають реалізовуватися засобом)

3 Визначення проблеми безпеки

3.1 Загрози _____
опис моделі порушника (ресурси, можливості, мотивація тощо) та можливі (несприятливі) його дії

3.2 Політика безпеки організації _____

_____
(набір правил безпеки, процедур або інструкцій, встановлених організацією (запланованих до встановлення гіпотетичною організацією) або законодавством для роботи засобу в середовищі функціонування)

3.3 Припущення _____
(щодо середовища функціонування ТОЕ для забезпечення реалізації SFR)

Примітка. Припущення можуть бути пов’язані з аспектами фізичного середовища, персоналом, зовнішніми зв’язками середовища функціонування та ТОЕ.

4 Цілі (завдання) безпеки

4.1 Шляхи вирішення проблеми безпеки _____
(для проблеми, визначеної у розділі 3)

4.2 Цілі безпеки _____
(для ТОЕ та середовища його функціонування)

Примітка. Кожна ціль безпеки повинна стосуватися принаймні однієї загрози або політики організаційної безпеки.

4.3 Обґрунтування ефективності цілей безпеки _____

Примітка. Обґрунтування має доводити комплексне вирішення проблеми та відповідати таким критеріям:

1) відсутність надлишкових цілей – кожна ціль безпеки співвідноситься, принаймні, з однією загрозою, вимогою політики організаційної безпеки або припущенням;

2) повнота визначення проблеми безпеки – для кожної загрози, вимоги політики організаційної безпеки та припущення існує, принаймні, одна мета безпеки, співвіднесена з ними;

3) коректність співвіднесення – сукупність логічних обґрунтувань, які показують, що всі загрози, політики організаційної безпеки та припущення щодо середовища функціонування засобу належним чином враховані у цілях безпеки.

5 Визначення розширених компонентів безпеки

_____
(наводяться за наявності, нові компоненти, яких немає у ДСТУ ISO/IEC 15408-2 або ДСТУ ISO/IEC 15408-3)

6 Вимоги з безпеки

6.1 Функціональні вимоги безпеки _____
(SFR згідно з ДСТУ ISO/IEC 15408-2)

6.2 Вимоги гарантії безпеки _____
(SAR згідно з ДСТУ ISO/IEC 15408-3)

6.3 Обґрунтування _____
(обґрунтування цілей безпеки щодо їх достатності та необхідності)

Примітки:

1. Кожна функціональна вимога безпеки повинна співвідноситись, принаймні, з однією ціллю безпеки та для кожної цілі безпеки повинна бути, принаймні, одна функціональна вимога безпеки, співвіднесена з нею;

2. Декілька функціональних вимог безпеки можуть бути співвіднесені з однією й тією ж ціллю безпеки, із вказанням, що поєднання цих вимог безпеки задовольняє означену ціль безпеки.

7 Загальна специфікація об’єкта експертних досліджень

7.1 Загальна інформація про реалізацію функції безпеки _____

Примітка. Загальна інформація про реалізацію засобом функції безпеки повинна відображати відповідність кожній SFR певних технічних механізмів та яким чином виконується кожна SAR.

ДОДАТОК Б

(обов’язковий)

ФОРМА ТЕХНІЧНОГО ПРОТОКОЛУ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ

ПОГОДЖЕНО

_____
(посада, підпис, власне ім’я, прізвище керівника експертної організації)

“___” _____ 20 __ року

ЗАТВЕРДЖУЮ

_____
(посада, підпис, власне ім’я, прізвище керівника експертного органу)

“___” _____ 20 __ року

ТЕХНІЧНИЙ ПРОТОКОЛ
ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ (ETR)
засобу

_____

№ _____

на ___ арк.

1 Ідентифікаційна інформація

1.1 Визначення ТОЕ _____
(назви моделей, версії засобів, документація тощо)

1.2 Технічні вимоги_____
(посилання на конкретну версію ST, за якою проводяться експертні дослідження)

1.3 Замовник _____
(назва замовника експертного дослідження)

1.4 Виробник _____
(назва виробника засобу)

1.5 Експертна організація _____
(яка проводила експертні дослідження)

1.6 Стандарти, за якими проводилися експертні дослідження _____
(конкретні редакції)

1.7 Пакет гарантій безпеки, на відповідність яким проводилися експертні дослідження _____
(набір EAL та додаткові елементи (за наявності), PP)

2 Опис об’єкта експертних досліджень (TOE Description)

2.1 Тип продукту _____
(наприклад, міжмережевий екран, операційна система, смарт-карта тощо)

2.2 Фізичні та логічні межі об’єкта експертних досліджень _____
(що входить в оцінювання)

2.3 Архітектурний огляд та опис реалізованих функцій безпеки (TSF) _____

3 Методологія та інструментарій (Evaluation Methodology)

3.1 Використані методи експертних досліджень _____
(відповідно до ДСТУ ISO/IEC 18045)

3.2 Інструменти (засоби) тестування _____
(особливо актуально для класів ATE та AVA)

3.3 Опис лабораторних умов та конфігурації середовища _____
_____
(у яких проводилося тестування функцій безпеки та аналіз вразливостей)

4 Результати експертних досліджень за класами гарантій (Evaluation Results)

_____
(результати структуровані за класами гарантій відповідно до ДСТУ ISO/IEC 15408)

Примітки:

1. Для кожного класу гарантій, відповідно до методології ДСТУ ISO/IEC 18045, вказуються вердикти (ПОЗИТИВНИЙ / НЕГАТИВНИЙ / НЕ ДОВЕДЕНО).

2. Усі класи мають вердикт НЕ ДОВЕДЕНО до винесення вердикту ПОЗИТИВНИЙ або НЕГАТИВНИЙ.

3. Загальний вердикт ПОЗИТИВНИЙ виноситься тільки після винесення вердиктів ПОЗИТИВНИЙ для всіх класів.

4.1 Оцінювання завдання з безпеки (Class ASE)

4.2.1 Аналіз повноти та несуперечливості ST _____

4.2.2 Результати перевірки опису цілей безпеки, загроз та функціональних вимог (SFR) _____

4.2 Розробка (Class ADV)

4.2.1 Аналіз специфікації функцій безпеки, архітектури безпеки та проєкту (design) об’єкта експертних досліджень _____

4.2.2 Результати перевірки відповідності між різними рівнями представлення продукту _____
(наприклад, від SFR до проєктної документації)

4.3 Керівництва (Class AGD)

4.3.1 Оцінювання документації для користувачів та адміністраторів _____

4.3.2 Перевірка того, чи дозволяють керівництва безпечно встановити та експлуатувати продукт _____

4.4 Підтримка життєвого циклу (Class ALC)

_____
(аналіз процесів розробки, інструментів конфігураційного управління, безпеки процедур доставки продукту замовнику, усунення вразливостей/оновлення)

4.5 Тестування (Class ATE)

4.5.1 Перевірка повноти охоплення тестами розробника функцій безпеки _____

4.5.2 Опис тестів, проведених експертною організацією _____

4.5.3 Результати вибіркової перевірки тестів розробника _____

4.6 Оцінювання вразливостей (Class AVA)

4.6.1 Пошук вразливостей _____
(аналіз загальнодоступних джерел на наявність відомих проблем та/або використання спеціалізованих інструментів)

4.6.2 Результати тестування на проникнення (Penetration Testing) _____
(опис спроб експлуатації потенційних вразливостей з урахуванням можливостей порушника, наприклад, для рівня EAL4 – посилений базовий рівень нападу).

5 Спостереження та результати (Observations)

5.1 Питання та запити на роз’яснення до розробника _____
(зафіксовані при експертних дослідженнях)

5.2 Виправлення, внесені розробником _____
(при експертних дослідженнях для усунення невідповідностей)

6 Висновки та рекомендації (Conclusions and Recommendations)

6.1 Загальний висновок _____
(відповідність ТОЕ вимогам ДСТУ ISO/IEC 15408 на заявленому рівні)

6.2 Умови використання _____
_____
(специфічні налаштування або обмеження середовища, за яких гарантується безпека продукту)

6.3 Рекомендації та пропозиції для експертного органу _____
(щодо видачі експертного висновку)

7 Додатки (Appendices)

7.1 Список використаної документації розробника _____

7.2 Детальні протоколи технічних тестів _____
(які не включені в основну частину)

7.3 Глосарій термінів та абревіатур _____

ДОДАТОК В

(обов’язковий)

ФОРМА ЗВІТУ ПРО ЕКСПЕРТНІ ДОСЛІДЖЕННЯ

ПОГОДЖЕНО

_____
(посада, підпис, власне ім’я, прізвище керівника експертної організації0

“___” _____ 20 __ року

ЗАТВЕРДЖУЮ

_____
(посада, підпис, власне ім’я, прізвище керівника експертного органу)

“___” _____ 20 __ року

ЗВІТ ПРО ЕКСПЕРТНІ ДОСЛІДЖЕННЯ

_____

_____

на ___ арк.

1 Загальні висновки

1.1 Найменування засобу_____

1.2 Перелік компонентів засобу_____
(що підлягають експертним дослідженням)

1.3 Назва виробника _____

1.4 Версія засобу_____
(версія, модель, модифікація засобу , представленого на експертні дослідження)

1.5 Дата завершення експертних досліджень _____

1.6 Звіт про експертні дослідження _____
(посилання на звіт, складений експертною організацією)

1.7 Короткий опис результатів звіту про експертні дослідження засобу:

а) Набір гарантій Загальних критеріїв

_____
(EAL та додаткові/або компоненти гарантій безпеки, включно з рівнем AVA_VAN, що застосовувався під час експертних досліджень, або профіль захисту, якому відповідає засіб захисту інформації)

б) Перелік функцій безпеки _____
(які реалізуються засобом)

в) Короткий виклад загроз та політики безпеки організації _____
(що враховуються засобом)

г) Спеціальні вимоги до конфігурації засобу _____

д) Припущення щодо середовища функціонування_____

2 Ідентифікація засобу

2.1 Назва засобу _____

2.2 Перелік компонентів_____
(на момент проходження засобом експертних досліджень)

2.3 Номери, версії компонентів засобу_____

_____
(специфікації програмних компонентів, які входять до складу інсталяційного пакета, та за наявності апаратних компонентів засобу)

2.4 Додаткові вимоги_____
(до середовища функціонування засобу)

2.5 Контактна інформація_____
(назва та контактна інформація замовника (виробника/спонсора)

2.6 Процедура управління виправленнями вразливостей_____
(за наявності)

Примітка. Належна ідентифікація засобу повинна забезпечувати повне та точне його представлення, яке можна повторно використовувати у майбутніх експертних дослідженнях.

3 Політика безпеки

_____
(опис політики або правил, яким засіб повинен відповідати та/або застосовувати їх)

Примітка. За наявності вказуються також умови, пов'язані з використанням процедури управління виправленнями, зокрема можливість внесення виправлень до елементів ТОЕ, які не визначені у пункті 1.3.2 ST, в рамках процедури внесення несуттєвих змін.

4 Припущення щодо умов та сфери використання об'єкта експертних досліджень

4.1 Припущення щодо використання та розгортання засобу_____
_____
(мінімальні вимоги, такі як належне встановлення та налаштування, для програмного засобу, вимоги до апаратного забезпечення)

4.2 Припущення щодо середовища функціонування _____

4.3 Обмеження_____
(які гарантують доступність послуг безпеки лише через інтерфейс засобу і контроль засобом всіх запитів на доступ до захищених об'єктів)

4.4 Аспекти безпеки середовища/конфігурації_____
(за яких очікується використання засобу)

4.5 Припущення щодо зовнішнього середовища_____
_____
(уточнення обсягу експертних досліджень стосовно загроз, відносно яких не вжито заходів з протидії)

Примітка. Інформація має бути якомога зрозумілішою, щоб дозволити користувачам засобу приймати обґрунтовані рішення щодо ризиків, пов'язаних з його використанням.

5 Інформація про архітектуру

5.1 Наведення характеристики архітектурної відокремленості основних компонентів _____
(опис засобу на високому рівні та його основних компонентів на основі результатів, описаних у відповідному сімействі SAR, щодо проєктування ТОЕ (ADV_TDS))

6 Документація

_____
(повний перелік документації на засіб , яка постачається виробником споживачеві)

Примітки:

1. Важливо, щоб вся відповідна документація позначалася номерами версій.

2. Документація повинна містити інструкції користувача, з адміністрування та встановлення (допускається об’єднання інструкції з адміністрування та встановлення в одному документі).

7 Тестування засобу

7.1 Спосіб тестування_____
(спосіб тестування, конфігурація, глибина та результати тестування)

7.2 Ідентифікація використаних компонентів гарантування_____
(зі стандартів ДСТУ ISO/IEC 15408)

7.3 Повні та точні налаштування та конфігурацію_____
(включно з операційними нотатками та зауваженнями)

7.4 Профіль захисту _____
(у разі використання)

а) Автор профілю захисту_____

б) Ідентифікатор профілю захисту_____
(назва та ідентифікатор профілю захисту та його сертифікат)

в) Пакет гарантій_____
(пакет(и) гарантій, необхідний(і) для засобу, що відповідає профілю захисту)

8 Конфігурація

8.1 Опис конфігурації засобу_____
(конфігурація під час експертних досліджень)

8.2 Параметри та деталі конфігурації_____

_____
(точні параметри та деталі конфігурації із супровідним обґрунтуванням обраних варіантів)

8.3 Додаткові інструкції_____
(будь-які додаткові інструкції з експлуатації та спостереження)

Примітка. Як правило, інструкції з адміністрування та встановлення надають необхідні дані для правильної конфігурації засобу, зважаючи на те, що засіб може мати можливість різних налаштувань (залежно від середовища, в якому він функціонує, або політики безпеки, яку він реалізує).

9 Результати експертних досліджень

9.1 Вимоги щодо гарантій_____
(детальний опис вимог та відповідності засобу кожній з них)

9.2 Можливий термін дії експертного висновку на засіб_____

(інформація щодо дати завершення експертних досліджень та думка експертної організації
щодо можливого терміну дії експертного висновку на засіб (загалом не довше 5 років),
з урахуванням можливих процедур управління виправленнями вразливостей)

10 Технічні вимоги

(редакція ST для опублікування, яка не містить інформації з обмеженим доступом)

11 Бібліографія

11.1 Критерії, методологія, програмна та схемо-технічна документація _____

(документація, на яку є посилання, що використовується як вихідний матеріал при складанні звіту про експертні дослідження)

11.2 Технічно-довідкова документація _____

(документація, на яку є посилання, що використовується як вихідний матеріал при складанні звіту про експертні дослідження)

11.3 Документація виробника _____
(що використовується при експертних дослідженнях)

Примітка. З метою гарантування відтворюваності експертних досліджень, вся документація, на яку є посилання, повинна бути однозначно ідентифікована з правильними датою випуску та номерами версій.

12 Коментарі/рекомендації експертної організації, додатки (опціонально)

12.1 Коментарі/рекомендації_____
(які використовуються для надання додаткової інформації
про результати експертних досліджень)

12.2 Додатки _____
(які використовуються для викладення будь-якої додаткової інформації,
що може бути корисною аудиторії звіту про експертні дослідження,
але логічно не вписується у передбачені рамки звіту)

БІБЛІОГРАФІЯ

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

2 ДСТУ ISO/IEC 15408-1:2023 (ISO/IEC 15408-1:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель;

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

4 ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення;

5 ДСТУ ISO/IEC 15408-4:2023 (ISO/IEC 15408-4:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності;

6 ДСТУ ISO/IEC 15408-5:2023 (ISO/IEC 15408-5:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки;

7 ДСТУ ISO/IEC 18045:2023 (ISO/IEC 18045:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ;

8 Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC);

9 ISO/IEC TS 9569:2023 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045;

10 Assurance Continuity: CCRA Requirements від 29.02.2024;

11 Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security від 02.07.2014.

Коди КСД 02.05, 03.05, 06.

Код УКНД 35.030.

Ключові слова: криптографічний захист інформації, технічний захист інформації, засоби КЗІ, засоби ТЗІ, експертні дослідження, оцінювання безпеки.