**НОРМАТИВНИЙ ДОКУМЕНТ**

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

# Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

Департамент спеціальних телекомунікаційних систем та захисту інформації
Служби безпеки України

Київ 2016

## Передмова

РОЗРОБЛЕНО Товариством з обмеженою відповідальністю "Інститут комп'ютерних технологій".

ВНЕСЕНО Департаментом технічного захисту інформації Адміністрації Держспецзв’язку.

ВВЕДЕНО ВПЕРШЕ.

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказом Департаменту спеціальних
телекомунікаційних систем та захисту інформації
Служби безпеки України

від “ 27 ” квітня 2016 року № 294

# Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

НД ТЗІ 2.6-003-2015

ДСТСЗІ СБ України

Київ

Зміст

# ПОРЯДОК ЗІСТАВЛЕННЯ КОМПОНЕНТІВ ДОЛВІРИ ДО БЕЗПЕКИ, ВИЗНАЧЕНИХ ISO/IEC 15408, З ВИМОГАМИ НД ТЗІ 2.5-004-99

Чинний від 2016-24-07

## 1 Галузь використання

Цей нормативний документ визначає відповідність між вимогами, встановленими стандартом ISO/IEC 15408 щодо компонентів довіри до безпеки, та вимогами, встановленими НД ТЗІ 2.5-004-99 щодо гарантій коректності реалізації функціональних послуг безпеки (ФПБ), а також містить опис загальних положень та порядку проведення робіт із зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, які виконуються в процесі створення засобів технічного захисту інформації (ЗТЗІ) від несанкціонованого доступу (НСД), захищених від НСД компонентів обчислювальної системи та захищених інформаційно-телекомунікаційних систем (ІТС) або в процесі проведення державної експертизи в сфері технічного захисту інформації (ТЗІ).

Нормативний документ (НД) призначено для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, а також юридичних та фізичних осіб усіх форм власності, які виконують роботи зі створення ЗТЗІ від НСД, захищених від НСД компонентів обчислювальної системи та комплексних систем захисту інформації (КСЗІ) в ІТС, а також проведення їх державної експертизи на відповідність вимогам НД системи ТЗІ в Україні.

## 2 Нормативні посилання

У цьому НД наведено посилання на такі нормативні документи:

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни і визначення.

Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93. Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087.

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model (Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 1. Вступ і загальна модель).

ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components (Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 2. Функціональні компоненти безпеки).

ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components (Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 3. Компоненти довіри до безпеки).

## 3 Визначення

У цьому НД ТЗІ застосовуються терміни та визначення, встановлені ДСТУ 3396.2-97 та НД ТЗІ 1.1-003-99.

Крім цього, використано такі терміни та визначення.

*Завдання з безпеки* – сукупність вимог безпеки та специфікацій, призначена для використання як основи для оцінювання конкретного об'єкта оцінювання.

*Засіб технічного захисту інформації від несанкціонованого доступу* – програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт виробництва, має необхідну проектну та/або експлуатаційну документацію і забезпечує самостійно або в комплексі з іншими засобами захист від загроз несанкціонованого доступу для інформації, оброблюваної в інформаційно-телекомунікаційній системі.

*Захищений від несанкціонованого доступу компонент обчислювальної системи* – програмний, апаратний або програмно-апаратний засіб, в якому додатково до основного призначення передбачено функції захисту інформації від загроз несанкціонованого доступу.

*Інформаційна система* – організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів.

*Інформаційно-телекомунікаційна система* – сукупність інформаційних та телекомунікаційних систем, які в процесі оброблення інформації діють як єдине ціле.

*Об'єкт експертизи* – засіб технічного захисту інформації від несанкціонованого доступу або захищений від несанкціонованого доступу компонент обчислювальної системи, стосовно якого проводиться експертиза в сфері технічного захисту інформації.

*Об'єкт оцінювання* – продукт інформаційних технологій або система із настановами адміністратора та користувача, що підлягають оцінюванню (сертифікації) на відповідність ISO/IEC 15408.

*Оцінювання* – визначення міри відповідності характеристик об'єкта заданим критеріям та вимогам.

*Політика безпеки об'єкта оцінювання* – сукупність правил, що регулюють керування активами, їх захист та розподіл у межах об'єкта оцінювання.

*Політика функції безпеки* – політика безпеки, що реалізується функцією безпеки.

*Телекомунікаційна система* – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

*Функція безпеки* – функціональні можливості частини або частин об'єкта оцінювання, які забезпечують виконання підмножини взаємозв'язаних правил політики безпеки об'єкта оцінювання.

*Функції безпеки об'єкта оцінювання* – сукупність усіх функцій об'єкта оцінювання, спрямованих на реалізацію політики безпеки об'єкта оцінювання.

*Функціональна послуга безпеки* – сукупність функцій, що визначені відповідно до вимог НД ТЗІ 2.5-004-99 та забезпечують захист інформації від певної загрози або від множини загроз.

*Функціональна специфікація об'єкта експертизи* – упорядкований перелік реалізованих в об'єкті експертизи функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 разом з описом їх політики або іншим чином визначений перелік функцій захисту з описом їх політик згідно з вимогами міжнародних стандартів.

## 4 Позначення та скорочення

У цьому НД ТЗІ використано такі позначення та скорочення:

ЗБ – завдання з безпеки;

ЗТЗІ – засіб технічного захисту інформації;

ІТ – інформаційна технологія;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОВЗ – особа, що виконує зіставлення;
ОЕ – об'єкт експертизи;
ОО – об'єкт оцінювання;
ОРД – оціночний рівень довіри;
ПБО – політика безпеки об'єкта оцінювання;
ПЗП – постійний запам'ятовуючий пристрій;
ТЗІ – технічний захист інформації;
ФБО – функції безпеки об'єкта оцінювання;
ФПБ – функціональна послуга безпеки.

## 5 Загальні положення щодо зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

5.1 Відповідно до положень НД ТЗІ 1.1-002-99 у проблемі захисту від НСД інформації, оброблюваної в ІТС, виокремлюються два напрями:

- забезпечення захищеності інформації у функціонуючих та/або створюваних ІТС;
- створення ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи поза конкретним середовищем експлуатації.

При цьому як у першому, так і в другому випадку доцільним, а якщо в ІТС планується оброблення інформації, порядок захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформації, яка становить державну таємницю або віднесена до державних інформаційних ресурсів), то обов'язковим є незалежне підтвердження (оцінювання) відповідності реалізованих засобів і заходів захисту встановленим вимогам і нормам. Результатами проведеного оцінювання має бути відповідний висновок, на підставі якого власники ІТС та оброблюваних у них інформаційних ресурсів можуть приймати рішення щодо прийнятності та достатності вжитих заходів і реалізованих засобів.

5.2 Згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації, на підставі якого в Україні функціонує система оцінювання відповідності реалізованих засобів і заходів захисту встановленим вимогам і нормам, об'єктами експертизи (ОЕ) можуть бути як КСЗІ, які є невід'ємною складовою частиною ІТС, так і окремі ЗТЗІ від НСД, у тому числі захищені від НСД компоненти обчислювальної системи.

5.3 Відповідно до положень НД ТЗІ 2.6-001-11 обсяг і тривалість експертних робіт із державної експертизи КСЗІ в ІТС суттєво скорочуються у випадку, якщо у складі комплексу засобів захисту (КЗЗ) КСЗІ використовуються ЗТЗІ від НСД або захищені від НСД компоненти обчислюваної системи, стосовно яких уже було проведено державну експертизу в сфері ТЗІ та наявні чинні експертні висновки, що містять її результати та відображають відповідність цих засобів вимогам НД ТЗІ. Наявність і можливість використання таких ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) дозволяють також суттєво скоротити тривалість робіт зі створення КСЗІ.

5.4 На цей час поширеною у світі є практика оцінювання (сертифікації) ЗТЗІ від НСД та захищених від НСД компонентів обчислюваної системи на відповідність вимогам Єдиних критеріїв оцінки безпеки інформаційних технологій, встановлених міжнародним стандартом ISO/IEC 15408. Такі засоби та компоненти обчислювальної системи широко використовуються в Україні при побудові ІТС різного призначення. З метою спрощення процедури експертних робіт при проведенні експертизи цих засобів та компонентів (у вигляді як окремих ОЕ, так і складових КЗЗ КСЗІ) експерти повинні мати можливість визначення рівня гарантій коректності реалізації ФПБ відповідним засобом (компонентом) не тільки шляхом дослідження ОЕ у порядку, визначеному НД ТЗІ 2.7-010-09, а і шляхом зіставлення наявних результатів оцінювання компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. Розробники ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) та захищених ІТС (КСЗІ в ІТС) повинні мати можливість визначення відповідності (у частині, що стосується гарантій коректності реалізації ФПБ) між вимогами НД ТЗІ 2.5-004-99 та вимогами ISO/IEC 15408, що дозволить суттєво спростити та прискорити процес підготовки створюваних ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) до оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408 або процес аналізу та прийняття рішення щодо можливого використання певного засобу (компонента обчислювальної системи) у складі захищеної ІТС (у складі КЗЗ КСЗІ).

5.5 Зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 може проводитися під час виконання робіт:

- з оцінювання рівня гарантій коректності реалізації ФПБ, які виконуються в процесі проведення державної експертизи в сфері ТЗІ, з метою визначення та підтвердження факту реалізації в ОЕ ФПБ з рівнем гарантій, який однозначно відповідає переліку компонентів довіри до безпеки, реалізацію яких для відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи, компонента КЗЗ КСЗІ) підтверджено за результатами оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408;
- зі створення ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою підготовки відповідних матеріалів (завдання з безпеки (ЗБ), опис об'єкта оцінювання (ОО) тощо), необхідних для оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408;
- зі створення захищених ІТС (КСЗІ в ІТС) під час проведення аналізу можливості включення до складу відповідних ІТС (КЗЗ створюваних КСЗІ) певних ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи, для яких наявні результати оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408, але немає (на момент проведення аналізу) результатів державної експертизи в сфері ТЗІ, з метою попереднього визначення рівня гарантій коректності реалізації ФПБ, який може бути призначений КЗЗ створюваної КСЗІ за результатами експертизи;
- в інших можливих випадках.

5.6 Зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, яке виконується під час робіт з оцінювання рівня гарантій коректності реалізації ФПБ, проводиться особами, що виконують зіставлення (ОВЗ) – експертами на етапі ознайомлення з оцінюваним ОЕ, збирання та аналізу матеріалів (документів), що характеризують організацію процесу його розроблення, виробництва та постачання.

5.6.1 З урахуванням загальних вимог щодо порядку проведення робіт на етапі ознайомлення з оцінюваним ОЕ, збирання та аналізу матеріалів (документів), встановлених НД ТЗІ 2.6-001-11, зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 під час оцінювання рівня гарантій коректності реалізації ФПБ передбачає виконання на підставі вмісту наданих замовником експертизи вхідних матеріалів, у складі яких мають бути надані результати оцінювання ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи) на відповідність вимогам ISO/IEC 15408, зіставлення реалізованих для ОЕ компонентів довіри до безпеки з вимогами НД ТЗІ 2.5-004-99 щодо гарантій та документування отриманих результатів.

5.6.2 Метою виконання такого зіставлення є:

- попереднє визначення рівня гарантій коректності реалізації ФПБ згідно з НД ТЗІ 2.5-004-99, що може бути призначений оцінюваному ОЕ за результатами експертизи;

- документування отриманих результатів та прийняття рішення щодо проведення подальших етапів експертних робіт або щодо їх припинення.

5.6.3 Визначення рівня гарантій коректності реалізації ФПБ згідно з НД ТЗІ 2.5-004-99 здійснюється ОВЗ шляхом виконання прямого зіставлення реалізованих для ОЕ компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 щодо критеріїв гарантій у порядку, наведеному у розділі 6.

**Примітка.** Наявність можливості визначення рівня гарантій коректності реалізації ФПБ згідно з НД ТЗІ 2.5-004-99 шляхом зіставлення реалізованих для ОЕ компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 щодо критеріїв гарантій не означає, що роботи з попереднього визначення рівня гарантій не можуть бути виконані шляхом аналізу результатів ознайомлення з оцінюваним ОЕ та аналізу матеріалів (документів), що характеризують організацію процесу його розроблення, виробництва та постачання у порядку, визначеному НД ТЗІ 2.7-010-09.

5.6.4 Результати зіставлення, виконаного під час робіт із оцінювання рівня гарантій коректності реалізації ФПБ, документуються у порядку, визначеному у розділі 11.

5.7 Зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, яке виконується під час робіт зі створення ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою підготовки матеріалів, необхідних для оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408, проводиться ОВЗ – розробниками цих засобів на відповідному етапі робіт.

5.7.1 Зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 під час робіт зі створення ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) передбачає виконання попереднього аналізу матеріалів (документів), що містять опис порядку задоволення вимог до визначеного розробниками у проектній документації рівня гарантій коректності реалізації ФПБ, з подальшим виконанням зіставлення вимог до складових відповідного рівня гарантій із вимогами ISO/IEC 15408 щодо компонентів довіри до безпеки та документування отриманих результатів.

5.7.2 Метою попереднього аналізу матеріалів (документів), що містять опис порядку задоволення вимог до визначеного рівня гарантій, є чітке визначення ОВЗ того, яким саме чином, за допомогою яких саме засобів, заходів та процедур забезпечено задоволення тих вимог до різних складових відповідного рівня гарантій, встановлених НД ТЗІ 2.5-004-99, які у подальшому мають бути зіставлені з вимогами ISO/IEC 15408.

5.7.3 Зіставлення вимог до різних складових відповідного рівня гарантій, встановлених НД ТЗІ 2.5-004-99, задоволення яких було забезпечено під час створення відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи), з вимогами ISO/IEC 15408 щодо компонентів довіри до безпеки здійснюється ОВЗ шляхом виконання зворотного зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 щодо критеріїв гарантій у порядку, наведеному у розділі 6.

5.7.4 Результатом виконаного зіставлення мають бути документовані у довільній формі відомості щодо компонентів довіри до безпеки згідно з ISO/IEC 15408, які за результатами зіставлення визнані такими, що реалізовані для створюваного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи), та визначений на підставі цих відомостей оціночний рівень довіри (ОРД). Обсяг зазначених відомостей має бути достатнім для підготовки відповідних матеріалів (ЗБ, опис ОО тощо), необхідних для оцінювання (сертифікації) створюваного ЗТЗІ від НСД на відповідність вимогам ISO/IEC 15408.

5.8 Зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, яке виконується в ході робіт зі створення захищених ІТС (КСЗІ в ІТС) під час проведення аналізу можливості включення до складу відповідних ІТС (КЗЗ створюваних КСЗІ) певних ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи, проводиться ОВЗ – розробниками відповідних систем. Метою відповідного зіставлення є попереднє визначення рівня гарантій коректності реалізації ФПБ згідно з НД ТЗІ 2.5-004-99, що може бути призначений КЗЗ створюваної КСЗІ у випадку використання у складі відповідної захищеної ІТС (КЗЗ створюваної КСЗІ) певного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи). Зіставлення має проводитись аналогічно до того, як це виконується в ході робіт із оцінювання рівня гарантій коректності реалізації ФПБ, шляхом виконання дій, зазначених у п. 5.6.3.

Після аналізу результатів зіставлення, отриманих для різних ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи), ОВЗ – розробником системи може бути прийнято рішення (з урахуванням вимог НД ТЗІ 3.6-001-2000 щодо рівня гарантій коректності реалізації ФПБ окремими ЗТЗІ від НСД, які використовуються у складі КЗЗ) щодо можливості дотримання у випадку використання певного засобу у складі створюваної ІТС (КСЗІ в ІТС) визначених вимог щодо рівня гарантій коректності реалізації ФПБ, та щодо доцільності або недоцільності включення відповідного засобу до складу створюваної ІТС (КСЗІ в ІТС) з метою виконання певних функцій із захисту інформації.

5.9 В інших випадках зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 може проводитись шляхом виконання прямого або зворотного зіставлення в порядку, наведеному у розділі 6.

## 6 Порядок виконання зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

6.1 Пряме зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 проводиться під час виконання робіт:

- з оцінювання рівня гарантій коректності реалізації ФПБ, які виконуються в процесі проведення державної експертизи в сфері ТЗІ, з метою визначення та підтвердження факту реалізації в ОЕ ФПБ з рівнем гарантій, який однозначно відповідає переліку компонентів довіри до безпеки, реалізацію яких для відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи, компонента КЗЗ КСЗІ) підтверджено за результатами оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408;
- зі створення захищених ІТС (КСЗІ в ІТС) під час проведення аналізу можливості включення до складу відповідних ІТС (КЗЗ створюваних КСЗІ) певних ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи, для яких наявні результати оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408, але немає (на момент проведення аналізу) результатів державної експертизи в сфері ТЗІ, з метою попереднього визначення рівня гарантій коректності реалізації ФПБ, що може бути призначений КЗЗ створюваної КСЗІ за результатами експертизи;
- в інших аналогічних випадках.

6.2 Пряме зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 передбачає виконання зіставлення компонентів довіри до безпеки згідно з ISO/IEC 15408, реалізованих для відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи), з вимогами критеріїв гарантій, встановленими НД ТЗІ 2.5-004-99, з метою визначення груп елементів певних компонентів довіри до безпеки, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99 щодо різних складових критеріїв гарантій (архітектури, середовища розробки, послідовності розробки, середовища функціонування, документації та випробувань) для певних рівнів гарантій.

6.3 Зіставлення компонентів довіри до безпеки згідно з ISO/IEC 15408, реалізованих для певного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи), з вимогами критеріїв гарантій, встановленими НД ТЗІ 2.5-004-99, з метою визначення груп елементів певних компонентів довіри до безпеки, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99 щодо різних складових критеріїв гарантій для певних рівнів гарантій, виконується у такому порядку.

6.3.1 На підставі вмісту матеріалів щодо результатів оцінювання (сертифікації) відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи) на відповідність вимогам ISO/IEC 15408 (ЗБ, опис ОО, звіт за результатами оцінювання тощо) визначається перелік усіх компонентів довіри до безпеки та усіх їх елементів, які мають бути зіставлені з вимогами НД ТЗІ 2.5-004-99.

6.3.2 У визначеному за результатами виконання пп. 6.3.1 переліку елементів компонентів довіри до безпеки на підставі відомостей, наведених у колонках 3 таблиць 7.1 -12.1, визначається наявність певних груп елементів відповідних компонентів довіри до безпеки, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99, наведені у колонках 2 відповідних таблиць, щодо певних складових критеріїв гарантій для певних рівнів гарантій.

**Примітка.** З метою спрощення визначення груп елементів довіри, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99 щодо певних складових критеріїв гарантій для певних рівнів гарантій, рекомендується користуватися таблицями А.1 - А.11 Додатка А.

6.3.3 Для кожної групи елементів довіри, визначеної за результатами виконання пп. 6.3.2, перевіряється факт дотримання умов задоволення елементами довіри, що входять у відповідну групу, вимог НД ТЗІ 2.5-004-99 щодо певної складової критеріїв гарантій для певного рівня гарантій, наведених у колонках 4 відповідних таблиць.

6.3.4 У випадку встановлення факту дотримання умов задоволення елементами довіри, що входять у певну групу, вимог НД ТЗІ 2.5-004-99 щодо певної складової критеріїв гарантій для певного рівня гарантій, характеристики відповідних елементів довіри, зокрема перелік матеріалів і документів, посилання на які містяться в описах відповідних елементів довіри, документуються, а відповідний рівень гарантій фіксується як такий, для якого задовольняються вимоги відповідної складової критеріїв гарантій.

6.3.5 У випадку встановлення за результатами виконання пп. 6.3.1-6.3.4, факту задоволення всіх вимог до всіх визначених НД ТЗІ 2.5-004-99 складових критеріїв гарантій як визначений за результатами зіставлення рівень гарантій обирається мінімальний із рівнів гарантій, зафіксованих при виконанні пп. 6.3.4 для кожної зі складових критеріїв гарантій.

6.4 Зворотне зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 проводиться:

- під час виконання робіт зі створення ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою підготовки відповідних матеріалів (ЗБ, опис ОО тощо), необхідних для оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408;
- в інших аналогічних випадках.

6.5 Зворотне зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 передбачає виконання зіставлення вимог до різних складових відповідного рівня гарантій, встановлених НД ТЗІ 2.5-004-99, задоволення яких було забезпечено під час створення певного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи), з вимогами до компонентів довіри до безпеки згідно з ISO/IEC 15408, з метою визначення переліку компонентів довіри до безпеки та їх елементів, які відповідають цьому рівню гарантій.

6.6 Зіставлення вимог до різних складових відповідного рівня гарантій, встановлених НД ТЗІ 2.5-004-99, задоволення яких було забезпечено під час створення певного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи), з вимогами до компонентів довіри до безпеки згідно з ISO/IEC 15408 виконується у такому порядку.

6.6.1 На підставі матеріалів (документів), що містять опис порядку задоволення вимог до визначеного розробниками у проектній документації рівня гарантій коректності реалізації ФПБ, фіксується відповідний рівень гарантій.

6.6.2 Для кожної складової відповідного рівня гарантій, зафіксованого за результатами виконання пп. 6.6.1, на підставі відомостей, наведених у колонках 1 - 2 таблиць 7.1 - 12.1, визначаються вимоги щодо груп елементів компонентів довіри до безпеки згідно з ISO/IEC 15408, наведені у колонках 3 відповідних таблиць, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99 щодо відповідної складової відповідного рівня гарантій.

6.6.3 Для елементів довіри, що входять до складу кожної визначеної за результатами виконання пп. 6.6.2 групи елементів довіри, на підставі вмісту матеріалів (документів), що містять опис порядку задоволення вимог до визначеного розробниками у проектній документації рівня гарантій коректності реалізації ФПБ, зазначених у пп. 6.6.1, та з урахуванням умов задоволення елементами довіри, що входять у відповідні групи, вимог НД ТЗІ 2.5-004-99 щодо певних складових певних рівнів гарантій, наведених у колонках 4 відповідних таблиць, визначаються їхні характеристики (переліки та назви документів тощо).

6.6.4 З урахуванням положень ISO/IEC 15408 формулюються вимоги та визначаються характеристики решти елементів довіри, які разом із визначеними при виконанні пп. 6.6.2 входять до складу відповідних компонентів довіри до безпеки.

6.6.5 Для всіх елементів, які входять до складу визначених при виконанні пп. 6.6.2 - 6.6.4 компонентів довіри до безпеки, перевіряється дотримання умов ISO/IEC 15408 щодо їх залежності від інших елементів довіри. Компоненти довіри до безпеки, для елементів яких дотримання умов ISO/IEC 15408 щодо їх залежності від інших елементів довіри не забезпечено, вилучаються із переліку, визначеного при виконанні пп. 6.6.2 - 6.6.4.

6.6.6 Характеристики компонентів довіри до безпеки згідно з ISO/IEC 15408, які складаються із характеристик усіх їх елементів, визначених при виконанні пп. 6.6.2 - 6.6.5 та задовольняють вимоги НД ТЗІ 2.5-004-99 щодо всіх складових відповідного рівня гарантій, та визначений на підставі їх сукупності ОРД документуються.

## 7 Відомості щодо відповідності компонентів довіри до безпеки згідно з ISO/IEC 15408 вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо архітектури

*У цьому розділі у таблиці 7.1 викладено відомості щодо відповідності елементів відповідних компонентів довіри, встановлених стандартом ISO/IEC 15408, вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо архітектури. Відомості викладено у табличному вигляді із зазначенням: рівня (рівнів) гарантій; вимог НД ТЗІ 2.5-004-99 щодо відповідного рівня гарантій; вимог стандарту ISO/IEC 15408-3 щодо елементів відповідних компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких для певного засобу технічного захисту інформації від НСД у процесі виконання зіставлення компонентів довіри, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 можна приймати рішення про те, що певна сукупність елементів компонентів довіри задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.*

Таблиця 7.1 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо архітектури

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1, Г-2 | КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені | ADV_INT.1.1D: Розробник повинен проектувати та структурувати функції безпеки об'єкта (ФБО) у модульному вигляді, уникаючи необов'язкових зв'язків між модулями проекту.<br>ADV_INT.1.2D: Розробник повинен надати опис архітектури.<br>ADV_INT.1.1C: Опис архітектури має ідентифікувати модулі ФБО.<br>ADV_INT.1.2C: Опис архітектури має містити опис призначення, інтерфейсів, параметрів і результатів застосування кожного модуля ФБО | У складі модулів ФБО, ідентифікованих у описі архітектури, зазначеному в елементі довіри ADV_INT.1.1C, наявні модулі, які відповідають усім компонентам КЗЗ |

| | | | |
|---|---|---|---|
| Г-3 | КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені<br>КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень | ADV_INT.1.1D: Розробник повинен проектувати та структурувати ФБО у модульному вигляді, уникаючи необов'язкових зв'язків між модулями проекту.<br>ADV_INT.1.2D: Розробник повинен надати опис архітектури.<br>ADV_INT.1.1C: Опис архітектури має ідентифікувати модулі ФБО.<br>ADV_INT.1.2C: Опис архітектури має містити опис призначення, інтерфейсів, параметрів і результатів застосування кожного модуля ФБО.<br>ADV_INT.1.3C: Опис архітектури має містити опис того, яким чином проект ФБО забезпечує більшу незалежність модулів, щоб уникнути непотрібної взаємодії. | У складі модулів ФБО, ідентифікованих у описі архітектури, зазначеному в елементі довіри ADV_INT.1.1C, наявні модулі, які відповідають усім компонентам КЗЗ |
| Г-4 | КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені<br>КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень<br>Критичні для безпеки компоненти КЗЗ повинні бути захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно- | ADV_INT.2.1D: Розробник повинен проектувати та структурувати ФБО у модульному вигляді, уникаючи необов'язкових зв'язків між модулями проекту.<br>ADV_INT.2.2D: Розробник повинен надати опис архітектури.<br>ADV_INT.2.3D: Розробник повинен проектувати та структурувати ФБО по рівнях з мінімізацією взаємних зв'язків між рівнями проекту.<br>ADV_INT.2.4D: Розробник повинен проектувати та структурувати ФБО у спосіб, що мінімізує складність тих частин ФБО, які реалізують будь-які політики керування доступом та/або інформаційними потоками.<br>ADV_INT.2.1C: Опис архітектури має ідентифікувати модулі ФБО та специфікувати, які частини ФБО реалізують політики керування доступом та/або | У складі модулів ФБО, ідентифікованих у описі архітектури, зазначеному в елементі довіри ADV_INT.2.1C, наявні модулі, які відповідають усім компонентам КЗЗ.<br>Поділ архітектури на рівні, наведений у описі архітектури, зазначеному в елементі довіри ADV_INT.2.4C, забезпечує можливість захисту критичних для безпеки модулів ФБО від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня |

| | | | |
|---|---|---|---|
| | апаратними засобами більш низького рівня | інформаційними потоками..<br>ADV_INT.2.2C: Опис архітектури має містити опис призначення, інтерфейсів, параметрів і результатів застосування кожного модуля ФБО.<br>ADV_INT.2.3C: Опис архітектури має містити опис того, яким чином проект ФБО забезпечує більшу незалежність модулів, щоб уникнути непотрібної взаємодії.<br>ADV_INT.2.4C: Опис архітектури має показати її поділ на рівні.<br>ADV_INT.2.5C: Опис архітектури має показати, що взаємні зв'язки були мінімізовані, та містити логічне обґрунтування зв'язків, що залишились.<br>ADV_INT.2.6C: Опис архітектури має містити опис того, яким чином частини ФБО, що реалізують будь-які політики керування доступом та/або інформаційними потоками, структуровані з метою мінімізації складності | |
| Г-5 - Г-7 | КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені<br>КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень<br>Критичні для безпеки компоненти КЗЗ повинні бути захищені від не | ADV_INT.3.1D: Розробник повинен проектувати та структурувати ФБО у модульному вигляді, уникаючи необов'язкових зв'язків між модулями проекту.<br>ADV_INT.3.2D: Розробник повинен надати опис архітектури.<br>ADV_INT.3.3D: Розробник повинен проектувати та структурувати ФБО по рівнях з мінімізацією взаємних зв'язків між рівнями проекту.<br>ADV_INT.3.4D: Розробник повинен проектувати та структурувати ФБО у спосіб, що мінімізує складність ФБО в цілому.<br>ADV_INT.3.5D: Розробник повинен проектувати та структурувати частини ФБО, | У складі модулів ФБО, ідентифікованих у описі архітектури, зазначеному в елементі довіри ADV_INT.3.1C, наявні модулі, які відповідають усім компонентам КЗЗ.<br>Поділ архітектури на рівні, наведений у описі архітектури, зазначеному в елементі довіри ADV_INT.3.4C, забезпечує можливість захисту критичних для безпеки модулів ФБО від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня |

| | | | |
|---|---|---|---|
| 14 | критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня<br><br>З боку Розробника мають бути вжиті зусилля, спрямовані на виключення з КЗЗ компонентів, що не є критичними для безпеки. Мають бути наведені підстави для включення до КЗЗ будь-якого елемента, який не має відношення до захисту<br><br>Розробка програмного забезпечення переважно має бути спрямована на мінімізацію складності КЗЗ. КЗЗ має бути спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою. Цей механізм повинен відігравати центральну роль в реалізації внутрішньої структури КЗЗ. Під час розробки КЗЗ значною мірою повинні бути задіяні такі підходи як модульність побудови і приховання (локалізація) даних | які реалізують будь-які політики керування доступом та/або інформаційними потоками, таким чином, щоб вони були достатньо простими для аналізу.<br>ADV_INT.3.6D: Розробник повинен забезпечити, щоб функції, цілі яких не мають відношення до безпеки, не включались до модулів ФБО.<br>ADV_INT.3.1C: Опис архітектури має ідентифікувати модулі ФБО та специфікувати, які частини ФБО реалізують політики керування доступом та/або інформаційними потоками.<br>ADV_INT.3.2C: Опис архітектури має містити опис призначення, інтерфейсів, параметрів і результатів застосування кожного модуля ФБО.<br>ADV_INT.3.3C: Опис архітектури має містити опис того, яким чином проект ФБО забезпечує більшу незалежність модулів, щоб уникнути непотрібної взаємодії.<br>ADV_INT.3.4C: Опис архітектури має показати її поділ на рівні.<br>ADV_INT.3.5C: Опис архітектури має показати, що взаємні зв'язки були мінімізовані, та містити логічне обґрунтування зв'язків, що залишились.<br>ADV_INT.3.6C: Опис архітектури має містити опис того, яким чином усі ФБО структуровані з метою мінімізації складності.<br>ADV_INT.3.7C: Опис архітектури має містити логічне обґрунтування включення до ФБО кожного модуля, який не задіяний у реалізації політики безпеки об'єкта (ПБО) | |

## 8 Відомості щодо відповідності компонентів довіри до безпеки згідно з ISO/IEC 15408 вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо середовища розробки

*У цьому розділі у таблицях 8.1, 8.2 викладено відомості щодо відповідності елементів відповідних компонентів довіри, встановлених стандартом ISO/IEC 15408, вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо середовища розробки. Відомості викладено у табличному вигляді із зазначенням у кожній таблиці: рівня (рівнів) гарантій; вимог НД ТЗІ 2.5-004-99 щодо відповідного рівня гарантій; вимог стандарту ISO/IEC 15408-3 щодо елементів відповідних компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких для певного засобу технічного захисту інформації від НСД у процесі виконання зіставлення компонентів довіри, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 можна приймати рішення про те, що певна сукупність елементів компонентів довіри задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.*

Таблиця 8.1 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо середовища розробки у частині, що стосується процесу розробки

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1, Г-2 | Розробник повинен визначити всі стадії життєвого циклу ОЕ, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги | ALC_LCD.1.1D, ALC_LCD.2.1D, ALC_LCD.3.1D: Розробник повинен визначити модель життєвого циклу, що використовується при розробці та супроводженні ОО.<br>ALC_LCD.1.2D, ALC_LCD.2.2D, ALC_LCD.3.2D: Розробник повинен надати документацію з визначення життєвого циклу.<br>ALC_LCD.1.1C, ALC_LCD.2.1C: Документація з визначення життєвого циклу має містити опис моделі, що використовується при розробці та супроводженні ОО.<br>ALC_LCD.1.2C, ALC_LCD.2.2C: Модель життєвого циклу має забезпечити необхідний | У моделі життєвого циклу, яка наведена у документації з визначення життєвого циклу, зазначеній в елементах довіри ALC_LCD.1.1C, ALC_LCD.2.1C чи ALC_LCD.3.1C, документовані всі етапи кожної стадії життєвого циклу ОО і їх граничні вимоги |

| | | | |
|---|---|---|---|
| | | контроль за розробкою та супроводженням ОО.<br>ALC_LCD.3.1C: Документація з визначення життєвого циклу має містити опис моделі, що використовується при розробці та супроводженні ОО, у тому числі деталізацію її кількісних параметрів та/або метрик, що використовуються для оцінки відповідності процесу розроблення ОО прийнятій моделі.<br>ALC_LCD.3.2C: Модель життєвого циклу має забезпечити необхідний контроль за розробкою та супроводженням ОО | |
| Г-3 | Розробник повинен визначити всі стадії життєвого циклу ОЕ, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги | ALC_LCD.1.1D, ALC_LCD.2.1D, ALC_LCD.3.1D: Розробник повинен визначити модель життєвого циклу, що використовується при розробці та супроводженні ОО.<br>ALC_LCD.1.2D, ALC_LCD.2.2D, ALC_LCD.3.2D: Розробник повинен надати документацію з визначення життєвого циклу.<br>ALC_LCD.1.1C, ALC_LCD.2.1C: Документація з визначення життєвого циклу має містити опис моделі, що використовується при розробці та супроводженні ОО.<br>ALC_LCD.1.2C, ALC_LCD.2.2C: Модель життєвого циклу має забезпечити необхідний контроль за розробкою та супроводженням ОО.<br>ALC_LCD.3.1C: Документація з визначення життєвого циклу має містити опис моделі, що використовується при розробці та супроводженні ОО, у тому числі деталізацію її кількісних параметрів та/або метрик, що використовуються для оцінки відповідності процесу розроблення ОО прийнятій моделі.<br>ALC_LCD.3.2C: Модель | У моделі життєвого циклу, яка наведена у документації з визначення життєвого циклу, зазначеній в елементах довіри ALC_LCD.1.1C, ALC_LCD.2.1C чи ALC_LCD.3.1C, документовані всі етапи кожної стадії життєвого циклу ОО і їх граничні вимоги |

| | | | |
|---|---|---|---|
| | | життєвого циклу має забезпечити необхідний контроль за розробкою та супроводженням ОО | |
| | Розробник повинен описати стандарти кодування, яких необхідно додержуватися в процесі реалізації, і повинен гарантувати, що всі вхідні коди компілюються відповідно до цих стандартів. Будь-яка з використовуваних під час реалізації мов програмування має бути добре визначена. Всі залежні від реалізації параметри мов програмування або компіляторів повинні бути документовані | ALC_TAT.2.1D: Розробник повинен ідентифікувати інструментальні засоби розробки ОО.<br>ALC_TAT.2.2D: Розробник повинен задокументувати обрані опції інструментальних засобів розробки, що обумовлені реалізацією.<br>ALC_TAT.2.3D: Розробник повинен навести опис використовуваних стандартів реалізації.<br>ALC_TAT.2.1C: Усі інструментальні засоби розробки, що використовуються для реалізації, мають бути повністю визначені.<br>ALC_TAT.2.2C: Документація інструментальних засобів розробки має однозначно визначати значення всіх мовних конструкції, що використовуються в реалізації.<br>ALC_TAT.2.3C: Документація інструментальних засобів розробки має однозначно визначати значення всіх опцій, що обумовлені реалізацією | Інструментальні засоби розробки, зазначені в елементах довіри ALC_TAT.2.1C, ALC_TAT.2.2C, ALC_TAT.2.3C, використовуються для компіляції усіх вхідних кодів ОО |
| Г-4 - Г-6 | Розробник повинен визначити всі стадії життєвого циклу ОЕ, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги | ALC_LCD.1.1D, ALC_LCD.2.1D, ALC_LCD.3.1D: Розробник повинен визначити модель життєвого циклу, що використовується при розробці та супроводженні ОО.<br>ALC_LCD.1.2D, ALC_LCD.2.2D, ALC_LCD.3.2D: Розробник повинен надати документацію з визначення життєвого циклу.<br>ALC_LCD.1.1C, ALC_LCD.2.1C: Документація з визначення життєвого циклу має містити опис моделі, що використовується при розробці та супроводженні | У моделі життєвого циклу, яка наведена у документації з визначення життєвого циклу, зазначеній в елементах довіри ALC_LCD.1.1C, ALC_LCD.2.1C чи ALC_LCD.3.1C, документовані всі етапи кожної стадії життєвого циклу ОО і їх граничні вимоги |

| | | | |
|---|---|---|---|
| | | ОО.<br>ALC_LCD.1.2C,<br>ALC_LCD.2.2C: Модель життєвого циклу має забезпечити необхідний контроль за розробкою та супроводженням ОО.<br>ALC_LCD.3.1C: Документація з визначення життєвого циклу має містити опис моделі, що використовується при розробці та супроводженні ОО, у тому числі деталізацію її кількісних параметрів та/або метрик, що використовуються для оцінки відповідності процесу розроблення ОО прийнятій моделі.<br>ALC_LCD.3.2C: Модель життєвого циклу має забезпечити необхідний контроль за розробкою та супроводженням ОО | |
| | Розробник повинен описати стандарти кодування, яких необхідно додержуватися в процесі реалізації, і повинен гарантувати, що всі вхідні коди компілюються відповідно до цих стандартів. Будь-яка з використовуваних під час реалізації мов програмування має бути добре визначена. Всі залежні від реалізації параметри мов програмування або компіляторів повинні бути документовані | ALC_TAT.2.1D: Розробник повинен ідентифікувати інструментальні засоби розробки ОО.<br>ALC_TAT.2.2D: Розробник повинен задокументувати обрані опції інструментальних засобів розробки, що обумовлені реалізацією.<br>ALC_TAT.2.3D: Розробник повинен навести опис використовуваних стандартів реалізації.<br>ALC_TAT.2.1C: Усі інструментальні засоби розробки, що використовуються для реалізації, мають бути повністю визначені.<br>ALC_TAT.2.2C: Документація інструментальних засобів розробки має однозначно визначати значення всіх мовних конструкції, що використовуються в реалізації.<br>ALC_TAT.2.3C: Документація інструментальних засобів розробки має однозначно визначати значення всіх опцій, що обумовлені реалізацією | Інструментальні засоби розробки, зазначені в елементах довіри ALC_TAT.2.1C, ALC_TAT.2.2C, ALC_TAT.2.3C, використовуються для компіляції усіх вхідних кодів ОО |

| | | | |
|---|---|---|---|
| | Розробник повинен розробити, запровадити і підтримувати в робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної і кадрової безпеки | ALC_DVS.1.1D, ALC_DVS.2.1D: Розробник повинен розробити документацію з безпеки розробки.<br>ALC_DVS.1.1C, ALC_DVS.2.1C: Документація з безпеки розробки має містити опис усіх фізичних, процедурних, що мають відношення до персоналу та інших заходів безпеки, які необхідні для захисту конфіденційності та цілісності проекту ОО та його реалізації у середовищі розробки.<br>ALC_DVS.1.2C, ALC_DVS.2.2C: Документація з безпеки розробки має надавати свідоцтво того, що необхідних заходів безпеки дотримуються під час розробки та супроводження ОО | Немає |
| Г-7 | Розробник повинен визначити всі стадії життєвого циклу ОЕ, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги | ALC_LCD.1.1D, ALC_LCD.2.1D, ALC_LCD.3.1D: Розробник повинен визначити модель життєвого циклу, що використовується при розробці та супроводженні ОО.<br>ALC_LCD.1.2D, ALC_LCD.2.2D, ALC_LCD.3.2D: Розробник повинен надати документацію з визначення життєвого циклу.<br>ALC_LCD.1.1C, ALC_LCD.2.1C: Документація з визначення життєвого циклу має містити опис моделі, що використовується при розробці та супроводженні ОО.<br>ALC_LCD.1.2C, ALC_LCD.2.2C: Модель життєвого циклу має забезпечити необхідний контроль за розробкою та супроводженням ОО.<br>ALC_LCD.3.1C: Документація з визначення життєвого циклу має містити опис моделі, що використовується при розробці та супроводженні ОО, у тому чмслі деталізацію | У моделі життєвого циклу, яка наведена у документації з визначення життєвого циклу, зазначеній в елементах довіри ALC_LCD.1.1C, ALC_LCD.2.1C чи ALC_LCD.3.1C, документовані всі етапи кожної стадії життєвого циклу ОО і їх граничні вимоги |

| | | | |
|---|---|---|---|
| | | її кількісних параметрів та/або метрик, що використовуються для оцінки відповідності процесу розроблення ОО прийнятій моделі.<br>ALC_LCD.3.2C: Модель життєвого циклу має забезпечити необхідний контроль за розробкою та супроводженням ОО | |
| | Розробник повинен описати стандарти кодування, яких необхідно додержуватися в процесі реалізації, і повинен гарантувати, що всі вхідні коди компілюються відповідно до цих стандартів. Будь-яка з використовуваних під час реалізації мов програмування має бути добре визначена. Всі залежні від реалізації параметри мов програмування або компіляторів повинні бути документовані | ALC_TAT.3.1D: Розробник повинен ідентифікувати інструментальні засоби розробки ОО.<br>ALC_TAT.3.2D: Розробник повинен задокументувати обрані опції інструментальних засобів розробки, що обумовлені реалізацією.<br>ALC_TAT.3.3D: Розробник повинен навести опис стандартів реалізації для всіх частин ОО.<br>ALC_TAT.3.1C: Усі інструментальні засоби розробки, що використовуються для реалізації, мають бути повністю визначені.<br>ALC_TAT.3.2C: Документація інструментальних засобів розробки має однозначно визначати значення всіх мовних конструкції, що використовуються в реалізації.<br>ALC_TAT.3.3C: Документація інструментальних засобів розробки має однозначно визначати значення всіх опцій, що обумовлені реалізацією | Інструментальні засоби розробки, зазначені в елементах довіри ALC_TAT.3.1C, ALC_TAT.3.2C, ALC_TAT.3.3C, використовуються для компіляції усіх вхідних кодів ОО |
| | Розробник повинен розробити, запровадити і підтримувати в робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної і кадрової безпеки | ALC_DVS.1.1D, ALC_DVS.2.1D: Розробник повинен розробити документацію з безпеки розробки.<br>ALC_DVS.1.1C, ALC_DVS.2.1C: Документація з безпеки розробки має містити опис усіх фізичних, процедурних, маючих відношення до персоналу та інших заходів безпеки, які необхідні для захисту | Немає |

| | | | |
|---|---|---|---|
| | | конфіденційності та цілісності проекту ОО та його реалізації у середовищі розробки.<br>ALC_DVS.1.2C, ALC_DVS.2.2C: Документація з безпеки розробки має надавати свідоцтво того, що необхідних заходів безпеки дотримуються під час розробки та супроводження ОО | |

Таблиця 8.2 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо середовища розробки у частині, що стосується керування конфігурацією

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1 - Г-3 | Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією ОЕ на всіх стадіях її життєвого циклу.<br>Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми постійних запам'ятовуючих пристроїв (ПЗП), вхідні тексти, об'єктні коди, тестове покриття і документацію.<br>Система керування | ACM_SCP.1.1D, ACM_SCP.2.1D: Розробник повинен надати список елементів конфігурації для ОО.<br>ACM_SCP.1.1C: Список елементів конфігурації має містити: представлення реалізації та свідоцтва оцінювання, що вимагаються компонентами довіри згідно із завданням з безпеки.<br>ACM_SCP.2.1C: Список елементів конфігурації має містити: представлення реалізації, недоліки безпеки та свідоцтва оцінювання, що вимагаються компонентами довіри згідно із завданням з безпеки.<br>ACM_CAP.3.1D: Розробник повинен надати маркування для ОО.<br>ACM_CAP.3.2D: Розробник повинен використовувати систему керування конфігурацією.<br>ACM_CAP.3.3D: Розробник повинен надати документацію з керування конфігурацією.<br>ACM_CAP.3.1C: Маркування | У свідоцтвах оцінювання, зазначених в елементах довіри ACM_SCP.1.1C чи ACM_SCP.2.1C, наявні матеріали щодо керування внесенням змін в тестове покриття і документацію |

| | | | |
|---|---|---|---|
| 22 | конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ | ОО має бути унікальним для кожної версії ОО.<br>ACM_CAP.3.2C: ОО має бути помічений маркуванням.<br>ACM_CAP.3.3C: Документація з керування конфігурацією має містити список елементів конфігурації та план керування конфігурацією.<br>ACM_CAP.3.4C: Список елементів конфігурації має унікально ідентифікувати всі елементи конфігурації, що входять до складу ОО.<br>ACM_CAP.3.5C: Список елементів конфігурації має містити опис елементів конфігурації, що входять до складу ОО.<br>ACM_CAP.3.6C: Документація з керування конфігурацією має містити опис методу, який використовується для унікальної ідентифікації елементів конфігурації, що входять до складу ОО.<br>ACM_CAP.3.7C: Система керування конфігурацією має унікально ідентифікувати всі елементи конфігурації, що входять до складу ОО.<br>ACM_CAP.3.8C: План керування конфігурацією має містити опис того, як використовується система керування конфігурацією.<br>ACM_CAP.3.9C: Свідоцтво має демонструвати, що система керування конфігурацією діє згідно з планом керування конфігурацією.<br>ACM_CAP.3.10C: Документація з керування конфігурацією має містити свідоцтво того, що система керування конфігурацією супроводжувала та продовжує ефективно супроводжувати всі елементи конфігурації.<br>ACM_CAP.3.11C: Система керування конфігурацією має передбачати заходи, при реалізації яких у елементах конфігурації можуть бути здійснені лише санкціоновані зміни | |

| | | | |
|---|---|---|---|
| Г-4, Г-5 | Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією ОЕ на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вхідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ. Система керування конфігурацією повинна базуватися на автоматизованих засобах | ACM_SCP.3.1D: Розробник повинен надати список елементів конфігурації для ОО.<br>ACM_SCP.3.1C: Список елементів конфігурації має містити: представлення реалізації, недоліки безпеки, інструментальні засоби розробки і пов'язану з ними інформацію, а також свідоцтва оцінювання, що вимагаються компонентами довіри згідно із завданням з безпеки.<br>ACM_CAP.4.1D: Розробник повинен надати маркування для ОО.<br>ACM_CAP.4.2D: Розробник повинен використовувати систему керування конфігурацією.<br>ACM_CAP.4.3D: Розробник повинен надати документацію з керування конфігурацією.<br>ACM_CAP.4.1C: Маркування ОО має бути унікальним для кожної версії ОО.<br>ACM_CAP.4.2C: ОО має бути помічений маркуванням.<br>ACM_CAP.4.3C: Документація з керування конфігурацією має містити список елементів конфігурації, план керування конфігурацією та план приймання під керування конфігурацією.<br>ACM_CAP.4.4C: Список елементів конфігурації має унікально ідентифікувати всі елементи конфігурації, що входять до складу ОО.<br>ACM_CAP.4.5C: Список елементів конфігурації має містити опис елементів конфігурації, що входять до складу ОО.<br>ACM_CAP.4.6C: Документація з керування конфігурацією має містити опис методу, який використовується для унікальної ідентифікації елементів конфігурації, що входять до складу ОО.<br>ACM_CAP.4.7C: Система | У свідоцтвах оцінювання, зазначених в елементі довіри ACM_SCP.3.1C, наявні матеріали щодо керування внесенням змін в тестове покриття і документацію |
| | Система керування конфігурацією також повинна використовуватися для генерації КЗЗ з вхідного коду і обліку всіх змін з появою нових версій | | |

| | | | |
|---|---|---|---|
| 24 | Система керування конфігурацією повинна бути здатна видавати звіти про стан елементів конфігурації | керування конфігурацією має унікально ідентифікувати всі елементи конфігурації, що входять до складу ОО.<br>ACM_CAP.4.8C: План керування конфігурацією має містити опис того, як використовується система керування конфігурацією.<br>ACM_CAP.4.9C: Свідоцтво має демонструвати, що система керування конфігурацією діє згідно з планом керування конфігурацією.<br>ACM_CAP.4.10C: Документація з керування конфігурацією має містити свідоцтво того, що система керування конфігурацією супроводжувала та продовжує ефективно супроводжувати всі елементи конфігурації.<br>ACM_CAP.4.11C: Система керування конфігурацією має передбачати заходи, при реалізації яких у елементах конфігурації можуть бути здійснені лише санкціоновані зміни.<br>ACM_CAP.4.12C: Система керування конфігурацією має підтримувати генерацію ОО.<br>ACM_CAP.4.13C: План приймання має містити опис процедур, що використовуються для приймання модифікованих або новостворених елементів конфігурації як частини ОО.<br>ACM_AUT.1.1D: Розробник повинен використовувати систему керування конфігурацією.<br>ACM_AUT.1.2D: Розробник повинен надати план керування конфігурацією.<br>ACM_AUT.1.1C: Система керування конфігурацією має надавати автоматизовані засоби, з використанням яких у представленні реалізації ОО здійснюються лише санкціоновані зміни.<br>ACM AUT.1.2C: Система керування конфігурацією має | |

| | | | |
|---|---|---|---|
| | | надавати автоматизовані засоби для підтримки генерації ОО.<br>ACM_AUT.1.3C: План керування конфігурацією має містити опис автоматизованих інструментальних засобів, що використовуються в системі керування конфігурацією.<br>ACM_AUT.1.4C: План керування конфігурацією має містити опис того, як автоматизовані інструментальні засоби використовуються в системі керування конфігурацією | |
| Г-6, Г-7 | Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією ОЕ на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вхідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ. Система керування конфігурацією | ACM_SCP.3.1D: Розробник повинен надати список елементів конфігурації для ОО.<br>ACM_SCP.3.1C: Список елементів конфігурації має містити: представлення реалізації, недоліки безпеки, інструментальні засоби розробки і пов'язану з ними інформацію, а також свідоцтва оцінювання, що вимагаються компонентами довіри згідно із завданням з безпеки.<br>ACM_CAP.5.1D: Розробник повинен надати маркування для ОО.<br>ACM_CAP.5.2D: Розробник повинен використовувати систему керування конфігурацією.<br>ACM_CAP.5.3D: Розробник повинен надати документацію з керування конфігурацією.<br>ACM_CAP.5.1C: Маркування ОО має бути унікальним для кожної версії ОО.<br>ACM_CAP.5.2C: ОО має бути помічений маркуванням.<br>ACM_CAP.5.3C: Документація з керування конфігурацією має містити список елементів конфігурації, план керування конфігурацією, план приймання під керування конфігурацією та процедури компоновки.<br>ACM_CAP.5.4C: Список елементів конфігурації має | У свідоцтвах оцінювання, зазначених в елементі довіри ACM_SCP.3.1C, наявні матеріали щодо керування внесенням змін в тестове покриття і документацію. |

| | | | |
|---|---|---|---|
| | повинна базуватися на автоматизованих засобах | унікально ідентифікувати всі елементи конфігурації, що входять до складу ОО.<br>ACM_CAP.5.5C: Список елементів конфігурації має містити опис елементів конфігурації, що входять до складу ОО.<br>ACM_CAP.5.6C: Документація з керування конфігурацією має містити опис методу, який використовується для унікальної ідентифікації елементів конфігурації, що входять до складу ОО.<br>ACM_CAP.5.7C: Система керування конфігурацією має унікально ідентифікувати всі елементи конфігурації, що входять до складу ОО.<br>ACM_CAP.5.8C: План керування конфігурацією має містити опис того, як використовується система керування конфігурацією.<br>ACM_CAP.5.9C: Свідоцтво має демонструвати, що система керування конфігурацією діє згідно з планом керування конфігурацією.<br>ACM_CAP.5.10C: Документація з керування конфігурацією має містити свідоцтво того, що система керування конфігурацією супроводжувала та продовжує ефективно супроводжувати всі елементи конфігурації.<br>ACM_CAP.5.11C: Система керування конфігурацією має передбачати заходи, при реалізації яких у елементах конфігурації можуть бути здійснені лише санкціоновані зміни.<br>ACM_CAP.5.12C: Система керування конфігурацією має підтримувати генерацію ОО.<br>ACM_CAP.5.13C: План приймання має містити опис процедур, що використовуються для приймання модифікованих або новостворених елементів конфігурації як частини ОО.<br>ACM_CAP.5.14C: Процедури | |
| | Система керування конфігурацією також повинна використовуватися для генерації КЗЗ з вхідного коду і обліку всіх змін з появою нових версій | | |
| | Система керування конфігурацією повинна бути здатна видавати звіти про стан елементів конфігурації | | |
| | Повинна використовуватися система заходів технічної, фізичної, організаційної і кадрової безпеки, спрямованих на захист усіх засобів і матеріалів, використовуваних для генерації КЗЗ, від несанкціонованої модифікації або руйнування | | |

| | | | |
|---|---|---|---|
| | | компоновки мають описувати, як система керування конфігурацією використовується в процесі виготовлення ОО.<br>ACM CAP.5.15C: Система керування конфігурацією має задовольняти вимоги, щоб особа, відповідальна за включення елемента конфігурації під керування конфігурацією, не була його розробником.<br>ACM_CAP.5.16C: Система керування конфігурацією має чітко ідентифікувати елементи конфігурації, які складають ФБО.<br>ACM_CAP.5.17C: Система керування конфігурацією має підтримувати аудит усіх модифікацій ОО з реєстрацією, як мінімум ініціатора, дати і часу модифікації в журналі аудита.<br>ACM_CAP.5.18C: Система керування конфігурацією має бути здатна ідентифікувати оригінали всіх матеріалів, що використовуються для генерації ОО.<br>ACM_CAP.5.19C: Документація з керування конфігурацією має демонструвати, що використання системи керування конфігурацією спільно із заходами безпеки розробки зробить можливими лише санкціоновані зміни в ОО.<br>ACM_CAP.5.20C: Документація з керування конфігурацією має демонструвати, що використання процедур компоновки забезпечує виконання генерації ОО правильно та у санкціонований спосіб.<br>ACM_CAP.5.21C: Документація з керування конфігурацією має демонструвати, що система керування конфігурації здатна забезпечити, щоб особа, відповідальна за включення елемента конфігурації під керування конфігурацією, не була його розробником. | |

| | | | |
|---|---|---|---|
| 28 | | ACM_CAP.5.22C: Документація з керування конфігурацією має містити логічне обґрунтування того, що процедури приймання забезпечують адекватний і зручний перегляд змін усіх елементів конфігурації.<br>ACM_AUT.2.1D: Розробник повинен використовувати систему керування конфігурацією.<br>ACM_AUT.2.2D: Розробник повинен надати план керування конфігурацією.<br>ACM_AUT.2.1C: Система керування конфігурацією має надавати автоматизовані засоби, з використанням яких у представленні реалізації ОО та у всіх інших елементах конфігурації здійснюються лише санкціоновані зміни.<br>ACM AUT.2.2C: Система керування конфігурацією має надавати автоматизовані засоби для підтримки генерації ОО.<br>ACM_AUT.2.3C: План керування конфігурацією має містити опис автоматизованих інструментальних засобів, що використовуються в системі керування конфігурацією.<br>ACM_AUT.2.4C: План керування конфігурацією має містити опис того, як автоматизовані інструментальні засоби використовуються в системі керування конфігурацією.<br>ACM AUT.2.5C: Система керування конфігурацією має надавати автоматизовані засоби для виявлення відмінностей між ОО та його попередньою версією.<br>ACM AUT.2.6C: Система керування конфігурацією має надавати автоматизовані засоби для визначення всіх інших елементів конфігурації, на які впливає модифікація цього елемента конфігурації | |

## 9 Відомості щодо відповідності компонентів довіри до безпеки згідно з ISO/IEC 15408 вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо послідовності розробки

*У цьому розділі у таблицях 9.1 - 9.5 викладено відомості щодо відповідності елементів відповідних компонентів довіри, встановлених стандартом ISO/IEC 15408, вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо послідовності розробки. Відомості викладено у табличному вигляді із зазначенням у кожній таблиці: рівня (рівнів) гарантій; вимог НД ТЗІ 2.5-004-99 щодо відповідного рівня гарантій; вимог стандарту ISO/IEC 15408-3 щодо елементів відповідних компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких для певного засобу технічного захисту інформації від НСД у процесі виконання зіставлення компонентів довіри, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 можна приймати рішення про те, що певна сукупність елементів компонентів довіри задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.*

Таблиця 9.1 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується функціональних специфікацій (політики безпеки)

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1 - Г-7 | На стадії розробки технічного завдання Розробник повинен розробити функціональні специфікації ОЕ. Представлені функціональні специфікації повинні включати неформалізований опис політики безпеки, що реалізується КЗЗ. Політика безпеки повинна містити перелік і опис послуг безпеки, що надаються КЗЗ | ADV_FSP.1.1D, ADV_FSP.2.1D: Розробник повинен надати функціональну специфікацію. ADV_FSP.1.1C, ADV_FSP.2.1C: Функціональна специфікація має містити неформальний опис ФБО та їх зовнішніх інтерфейсів. ADV_FSP.1.2C, ADV_FSP.2.2C: Функціональна специфікація має бути внутрішньо несуперечливою. ADV_FSP.1.3C, ADV_FSP.2.3C: Функціональна специфікація має містити опис призначення та методів використання всіх зовнішніх інтерфейсів ФБО, забезпечуючи, де це необхідно, деталізацію результатів, нештатних ситуацій та повідомлень про помилки. ADV_FSP.1.4C, ADV_FSP.2.4C: Функціональна специфікація має повністю представляти ФБО | В описі ФБО, зазначеному в елементах довіри ADV_FSP.1.1C чи ADV_FSP.2.1C, міститься опис усіх функціональних компонентів безпеки згідно з ISO/IEC 15408-2, відповідних всім ФПБ, що надаються КЗЗ ОЕ |

Таблиця 9.2 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується функціональних специфікацій (моделі політики безпеки)

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-2 | Функціональні специфікації повинні включати модель політики безпеки<br>Стиль специфікації: неформалізована<br>Відповідність політиці безпеки: показ | ADV_SPM.1.1D: Розробник повинен надати модель ПБО.<br>ADV_SPM.1.2D: Розробник повинен продемонструвати відповідність між функціональною специфікацією та моделлю ПБО.<br>ADV_SPM.1.1C: Модель ПБО має бути неформальною.<br>ADV_SPM.1.2C: Модель ПБО має містити опис правил і характеристики всіх політик ПБО, які можуть бути промодельовані.<br>ADV_SPM.1.3C: Модель ПБО має містити обґрунтування, яке демонструє, що вона є узгодженою та повною відносно усіх політик ПБО, які можуть бути промодельовані.<br>ADV_SPM.1.4C: Демонстрація відповідності між моделлю ПБО та функціональною специфікацією має показати, що всі функції безпеки у функціональній специфікації є несуперечливими та повними відносно моделі ПБО | Немає |
| Г-3 | Функціональні специфікації повинні включати модель політики безпеки<br>Стиль специфікації: частково формалізована<br>Відповідність політиці безпеки: показ | ADV_SPM.2.1D: Розробник повинен надати модель ПБО.<br>ADV_SPM.2.2D: Розробник повинен продемонструвати відповідність між функціональною специфікацією та моделлю ПБО.<br>ADV_SPM.2.1C: Модель ПБО має бути напівформальною.<br>ADV_SPM.2.2C: Модель ПБО має містити опис правил і характеристики всіх політик ПБО, які можуть бути промодельовані.<br>ADV_SPM.2.3C: Модель ПБО має містити обґрунтування, яке демонструє, що вона є узгодженою та повною відносно усіх політик ПБО, які можуть бути промодельовані.<br>ADV_SPM.2.4C: Демонстрація відповідності між моделлю ПБО та | Немає |

| | | | |
|---|---|---|---|
| | | функціональною специфікацією має показати, що всі функції безпеки у функціональній специфікації є несуперечливими та повними відносно моделі ПБО.<br>ADV_SPM.2.5C: Там, де функціональна специфікація, як мінімум напівформальна, демонстрація відповідності між моделлю ПБО та функціональною специфікацією має бути напівформальною | |
| Г-4 - Г-7 | Функціональні специфікації повинні включати модель політики безпеки<br>Стиль специфікації: формалізована<br>Відповідність політиці безпеки: демонстрація | ADV_SPM.3.1D: Розробник повинен надати модель ПБО.<br>ADV_SPM.3.2D: Розробник повинен продемонструвати або довести, де це є необхідним, відповідність між функціональною специфікацією та моделлю ПБО.<br>ADV_SPM.3.1C: Модель ПБО має бути формальною.<br>ADV_SPM.3.2C: Модель ПБО має містити опис правил і характеристики всіх політик ПБО, які можуть бути промодельовані.<br>ADV_SPM.3.3C: Модель ПБО має містити обґрунтування, яке демонструє, що вона є узгодженою та повною відносно усіх політик ПБО, які можуть бути промодельовані.<br>ADV_SPM.3.4C: Демонстрація відповідності між моделлю ПБО та функціональною специфікацією має показати, що всі функції безпеки у функціональній специфікації є несуперечливими та повними відносно моделі ПБО.<br>ADV_SPM.3.5C: Там, де функціональна специфікація напівформальна, демонстрація відповідності між моделлю ПБО та функціональною специфікацією має бути напівформальною | Немає |

Таблиця 9.3 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується проекту архітектури

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1 | На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення<br>Стиль специфікації: неформалізована | ADV_HLD.2.1D: Розробник повинен надати проект верхнього рівня ФБО.<br>ADV_HLD.2.1C: Представлення проекту верхнього рівня має бути неформальним.<br>ADV_HLD.2.2C: Проект верхнього рівня має бути внутрішньо несуперечливим.<br>ADV_HLD.2.3C: Проект верхнього рівня має містити опис структури ФБО в термінах підсистем.<br>ADV_HLD.2.4C: Проект верхнього рівня має містити опис функціональних можливостей безпеки, що надаються кожною підсистемою ФБО.<br>ADV_HLD.2.5C: Проект верхнього рівня має ідентифікувати будь-які базові апаратні, програмно-апаратні та/або програмні засоби, потрібні ФБО, з представленням функцій, що забезпечуються підтримуючими механізмами захисту, які реалізовані у цих апаратних, програмно-апаратних та/або програмних засобах.<br>ADV_HLD.2.6C: Проект верхнього рівня має ідентифікувати всі інтерфейси для підсистем ФБО.<br>ADV_HLD.2.7C: Проект верхнього рівня має ідентифікувати, які з інтерфейсів підсистем ФБО є видимими ззовні.<br>ADV_HLD.2.8C: Проект верхнього рівня має містити опис призначення та методів використання всіх інтерфейсів підсистем ФБО, забезпечуючи, де це необхідно, деталізацію результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_HLD.2.9C: Проект верхнього рівня має містити опис розділення ОО на підсистеми, що реалізують ПБО, та інші | Немає |
| Г-2 | На стадії розробки ескізного проекту | ADV_HLD.2.1D: Розробник повинен надати проект верхнього рівня ФБО.<br>ADV_HLD.2.1C: Представлення | Немає |

| | | | |
|---|---|---|---|
| | Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення | проекту верхнього рівня має бути неформальним.<br>ADV_HLD.2.2C: Проект верхнього рівня має бути внутрішньо несуперечливим.<br>ADV_HLD.2.3C: Проект верхнього рівня має містити опис структури ФБО в термінах підсистем.<br>ADV_HLD.2.4C: Проект верхнього рівня має містити опис функціональних можливостей безпеки, що надаються кожною підсистемою ФБО.<br>ADV_HLD.2.5C: Проект верхнього рівня має ідентифікувати будь-які базові апаратні, програмно-апаратні та/або програмні засоби, потрібні ФБО, з представленням функцій, що забезпечуються підтримуючими механізмами захисту, які реалізовані у цих апаратних, програмно-апаратних та/або програмних засобах.<br>ADV_HLD.2.6C: Проект верхнього рівня має ідентифікувати всі інтерфейси для підсистем ФБО.<br>ADV_HLD.2.7C: Проект верхнього рівня має ідентифікувати, які з інтерфейсів підсистем ФБО є видимими ззовні.<br>ADV_HLD.2.8C: Проект верхнього рівня має містити опис призначення та методів використання всіх інтерфейсів підсистем ФБО, забезпечуючи, де це необхідно, деталізацію результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_HLD.2.9C: Проект верхнього рівня має містити опис розділення ОО на підсистеми, що реалізують ПБО, та інші | |
| | Стиль специфікації: неформалізована | | |
| | Відповідність моделі політики безпеки: показ | ADV_RCR.1.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.1.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають демонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.1.1C, наявні результати аналізу відповідності між проектом верхнього рівня ФБО та моделлю ПБО |
| Г-3, Г-4 | На стадії розробки ескізного проекту | ADV_HLD.3.1D: Розробник повинен надати проект верхнього рівня ФБО.<br>ADV_HLD.3.1C: Представлення | Немає |

| | | | |
|---|---|---|---|
| | Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення | проекту верхнього рівня має бути напівформальним.<br>ADV_HLD.3.2C: Проект верхнього рівня має бути внутрішньо несуперечливим.<br>ADV_HLD.3.3C: Проект верхнього рівня має містити опис структури ФБО в термінах підсистем.<br>ADV_HLD.3.4C: Проект верхнього рівня має містити опис функціональних можливостей безпеки, що надаються кожною підсистемою ФБО.<br>ADV_HLD.3.5C: Проект верхнього рівня має ідентифікувати будь-які базові апаратні, програмно-апаратні та/або програмні засоби, потрібні ФБО, з представленням функцій, що забезпечуються підтримуючими механізмами захисту, які реалізовані у цих апаратних, програмно-апаратних та/або програмних засобах.<br>ADV_HLD.3.6C: Проект верхнього рівня має ідентифікувати всі інтерфейси для підсистем ФБО.<br>ADV_HLD.3.7C: Проект верхнього рівня має ідентифікувати, які з інтерфейсів підсистем ФБО є видимими ззовні.<br>ADV_HLD.3.8C: Проект верхнього рівня має містити опис призначення та методів використання всіх інтерфейсів підсистем ФБО, забезпечуючи повну деталізацію всіх результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_HLD.3.9C: Проект верхнього рівня має містити опис розділення ОО на підсистеми, що реалізують ПБО, та інші | |
| | Стиль специфікації: частково формалізована | | |
| | Відповідність моделі політики безпеки: показ | ADV_RCR.1.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.1.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають демонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.1.1C, наявні результати аналізу відповідності між проектом верхнього рівня ФБО та моделлю ПБО |
| Г-5<br>34 | На стадії розробки ескізного проекту | ADV_HLD.4.1D: Розробник повинен надати проект верхнього рівня ФБО.<br>ADV_HLD.4.1C: Представлення | |

| | | | |
|---|---|---|---|
| | Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення<br><br>Стиль специфікації: частково формалізована | проекту верхнього рівня має бути напівформальним.<br>ADV_HLD.4.2C: Проект верхнього рівня має бути внутрішньо несуперечливим.<br>ADV_HLD.4.3C: Проект верхнього рівня має містити опис структури ФБО в термінах підсистем.<br>ADV_HLD.4.4C: Проект верхнього рівня має містити опис функціональних можливостей безпеки, що надаються кожною підсистемою ФБО.<br>ADV_HLD.4.5C: Проект верхнього рівня має ідентифікувати будь-які базові апаратні, програмно-апаратні та/або програмні засоби, потрібні ФБО, з представленням функцій, що забезпечуються підтримуючими механізмами захисту, які реалізовані у цих апаратних, програмно-апаратних та/або програмних засобах.<br>ADV_HLD.4.6C: Проект верхнього рівня має ідентифікувати всі інтерфейси для підсистем ФБО.<br>ADV_HLD.4.7C: Проект верхнього рівня має ідентифікувати, які з інтерфейсів підсистем ФБО є видимими ззовні.<br>ADV_HLD.4.8C: Проект верхнього рівня має містити опис призначення та методів використання всіх інтерфейсів підсистем ФБО, забезпечуючи повну деталізацію всіх результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_HLD.4.9C: Проект верхнього рівня має містити опис розділення ОО на підсистеми, що реалізують ПБО, та інші.<br>ADV_HLD.4.10C: Проект верхнього рівня має містити логічне обґрунтування того, що ідентифікований спосіб виконання розділення, у тому числі будь-яких механізмів захисту, є достатнім для забезпечення чіткого та ефективного відділення функцій, що реалізують ФБО, від функцій, що не беруть участь у реалізації ФБО.<br>ADV_HLD.4.11C: Проект верхнього рівня має містити логічне обґрунтування того, що механізми ФБО достатні для реалізації функцій безпеки, ідентифікованих у проекті верхнього рівня | |

| | | | |
|---|---|---|---|
| | Відповідність моделі політики безпеки: демонстрація | ADV_RCR.2.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.2.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають продемонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО.<br>ADV_RCR.2.2C: Для кожної суміжної пари наявних представлень ФБО, де частини обох представлень специфіковані, як мінімум напівформально, демонстрація відповідності між цими частинами представлень має бути напівформальною | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.2.1C, наявні результати аналізу відповідності між проектом верхнього рівня ФБО та моделлю ПБО |
| Г-6, Г-7 | На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення<br><br>Стиль специфікації: формалізована | ADV_HLD.5.1D: Розробник повинен надати проект верхнього рівня ФБО.<br>ADV_HLD.5.1C: Представлення проекту верхнього рівня має бути формальним.<br>ADV_HLD.5.2C: Проект верхнього рівня має бути внутрішньо несуперечливим.<br>ADV_HLD.5.3C: Проект верхнього рівня має містити опис структури ФБО в термінах підсистем.<br>ADV_HLD.5.4C: Проект верхнього рівня має містити опис функціональних можливостей безпеки, що надаються кожною підсистемою ФБО.<br>ADV_HLD.5.5C: Проект верхнього рівня має ідентифікувати будь-які базові апаратні, програмно-апаратні та/або програмні засоби, потрібні ФБО, з представленням функцій, що забезпечуються підтримуючими механізмами захисту, які реалізовані у цих апаратних, програмно-апаратних та/або програмних засобах.<br>ADV_HLD.5.6C: Проект верхнього рівня має ідентифікувати всі інтерфейси для підсистем ФБО.<br>ADV_HLD.5.7C: Проект верхнього рівня має ідентифікувати, які з інтерфейсів підсистем ФБО є видимими ззовні.<br>ADV_HLD.5.8C: Проект верхнього рівня має містити опис призначення та методів використання всіх інтерфейсів підсистем ФБО, забезпечуючи повну | |

| | | | |
|---|---|---|---|
| | | деталізацію всіх результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_HLD.5.9C: Проект верхнього рівня має містити опис розділення ОО на підсистеми, що реалізують ПБО, та інші.<br>ADV_HLD.5.10C: Проект верхнього рівня має містити логічне обґрунтування того, що ідентифікований спосіб виконання розділення, у тому числі будь-яких механізмів захисту, є достатнім для забезпечення чіткого та ефективного відділення функцій, що реалізують ФБО, від функцій, що не беруть участі у реалізації ФБО.<br>ADV_HLD.5.11C: Проект верхнього рівня має містити логічне обґрунтування того, що механізми ФБО достатні для реалізації функцій безпеки, ідентифікованих у проекті верхнього рівня | |
| | Відповідність моделі політики безпеки: доказ | ADV_RCR.3.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.3.2D: Для тих із відповідних частин представлень, які специфіковані формально, розробник повинен довести цю відповідність.<br>ADV_RCR.3.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають доказати або продемонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО.<br>ADV_RCR.3.2C: Для кожної суміжної пари наявних представлень ФБО, де частини одного представлення специфіковані напівформально, а іншого, як мінімум напівформально, демонстрація відповідності між цими частинами представлень має бути напівформальною.<br>ADV_RCR.3.3C: Для кожної суміжної пари наявних представлень ФБО, де частини обох представлень специфіковані формально, доказ відповідності між цими частинами представлень має бути формальним | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.3.1C, наявні результати аналізу відповідності між проектом верхнього рівня ФБО та моделлю ПБО |

Таблиця 9.4 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується детального проекту

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1 | На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект компонентів КЗЗ, що мають безпосереднє відношення до безпеки. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ<br>Стиль специфікації: неформалізована | ADV_LLD.1.1D: Розробник повинен надати проект нижнього рівня ФБО.<br>ADV_LLD.1.1C: Представлення проекту нижнього рівня має бути неформальним.<br>ADV_LLD.1.2C: Проект нижнього рівня має бути внутрішньо несуперечливим.<br>ADV_LLD.1.3C: Проект нижнього рівня має містити опис структури ФБО в термінах модулів.<br>ADV_LLD.1.4C: Проект нижнього рівня має містити опис призначення кожного модуля.<br>ADV_LLD.1.5C: Проект нижнього рівня має визначати взаємозв'язки між модулями в термінах функціональних можливостей безпеки, що надаються, та залежностей від інших модулів.<br>ADV_LLD.1.6C: Проект нижнього рівня має містити опис того, як надається кожна з функцій, що реалізують ПБО.<br>ADV_LLD.1.7C: Проект нижнього рівня має ідентифікувати всі інтерфейси модулів ФБО.<br>ADV_LLD.1.8C: Проект нижнього рівня має ідентифікувати, які з інтерфейсів модулів ФБО є видимими ззовні.<br>ADV_LLD.1.9C: Проект нижнього рівня має містити опис призначення та методів використання всіх інтерфейсів модулів ФБО, забезпечуючи, де це необхідно, деталізацію результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_LLD.1.10C: Проект нижнього рівня має містити опис розділення ОО на модулі, що реалізують ПБО, та інші | Немає |
| Г-2, Г-3 | На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений | ADV_LLD.1.1D: Розробник повинен надати проект нижнього рівня ФБО.<br>ADV_LLD.1.1C: Представлення проекту нижнього рівня має бути неформальним.<br>ADV_LLD.1.2C: Проект нижнього рівня має бути внутрішньо несуперечливим.<br>ADV_LLD.1.3C: Проект нижнього рівня має містити опис структури ФБО в термінах модулів.<br>ADV_LLD.1.4C: Проект нижнього рівня має містити опис призначення кожного | Немає |

| | | | |
|---|---|---|---|
| | детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ | модуля.<br>ADV_LLD.1.5C: Проект нижнього рівня має визначати взаємозв'язки між модулями в термінах функціональних можливостей безпеки, що надаються, та залежностей від інших модулів.<br>ADV_LLD.1.6C: Проект нижнього рівня має містити опис того, як надається кожна з функцій, що реалізують ПБО.<br>ADV_LLD.1.7C: Проект нижнього рівня має ідентифікувати всі інтерфейси модулів ФБО.<br>ADV_LLD.1.8C: Проект нижнього рівня має ідентифікувати, які з інтерфейсів модулів ФБО є видимими ззовні.<br>ADV_LLD.1.9C: Проект нижнього рівня має містити опис призначення та методів використання всіх інтерфейсів модулів ФБО, забезпечуючи, де це необхідно, деталізацію результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_LLD.1.10C: Проект нижнього рівня має містити опис розділення ОО на модулі, що реалізують ПБО, та інші | |
| | Стиль специфікації: неформалізована | | |
| | Відповідність проекту архітектури: показ | ADV_RCR.1.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.1.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають демонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.1.1C, наявні результати аналізу відповідності між проектом нижнього рівня ФБО та проектом верхнього рівня ФБО |
| Г-4 | На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. | ADV_LLD.2.1D: Розробник повинен надати проект нижнього рівня ФБО.<br>ADV_LLD.2.1C: Представлення проекту нижнього рівня має бути напівформальним.<br>ADV_LLD.2.2C: Проект нижнього рівня має бути внутрішньо несуперечливим.<br>ADV_LLD.2.3C: Проект нижнього рівня має містити опис структури ФБО в термінах модулів.<br>ADV_LLD.2.4C: Проект нижнього рівня має містити опис призначення кожного модуля.<br>ADV_LLD.2.5C: Проект нижнього рівня має визначати взаємозв'язки між модулями в термінах функціональних можливостей безпеки, що надаються, та залежностей від інших модулів.<br>ADV_LLD.2.6C: Проект нижнього рівня | Немає |

| | | | |
|---|---|---|---|
| | Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ | має містити опис того, як надається кожна з функцій, що реалізують ПБО.<br>ADV_LLD.2.7C: Проект нижнього рівня має ідентифікувати всі інтерфейси модулів ФБО.<br>ADV_LLD.2.8C: Проект нижнього рівня має ідентифікувати, які з інтерфейсів модулів ФБО є видимими ззовні.<br>ADV_LLD.2.9C: Проект нижнього рівня має містити опис призначення та методів використання всіх інтерфейсів модулів ФБО, надаючи повну деталізацію всіх результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_LLD.2.10C: Проект нижнього рівня має містити опис розділення ОО на модулі, що реалізують ПБО, та інші | |
| | Стиль специфікації: частково формалізована | | |
| | Відповідність проекту архітектури: показ | ADV_RCR.1.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.1.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають демонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.1.1C, наявні результати аналізу відповідності між проектом нижнього рівня ФБО та проектом верхнього рівня ФБО |
| Г-5 | На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ | ADV_LLD.2.1D: Розробник повинен надати проект нижнього рівня ФБО.<br>ADV_LLD.2.1C: Представлення проекту нижнього рівня має бути напівформальним.<br>ADV_LLD.2.2C: Проект нижнього рівня має бути внутрішньо несуперечливим.<br>ADV_LLD.2.3C: Проект нижнього рівня має містити опис структури ФБО в термінах модулів.<br>ADV_LLD.2.4C: Проект нижнього рівня має містити опис призначення кожного модуля.<br>ADV_LLD.2.5C: Проект нижнього рівня має визначати взаємозв'язки між модулями в термінах функціональних можливостей безпеки, що надаються, та залежностей від інших модулів.<br>ADV_LLD.2.6C: Проект нижнього рівня має містити опис того, як надається кожна з функцій, що реалізують ПБО.<br>ADV_LLD.2.7C: Проект нижнього рівня має ідентифікувати всі інтерфейси модулів ФБО.<br>ADV_LLD.2.8C: Проект нижнього рівня має ідентифікувати, які з інтерфейсів | Немає |
| | Стиль | | |

| | | | |
|---|---|---|---|
| | специфікації: частково формалізована | модулів ФБО є видимими ззовні.<br>ADV_LLD.2.9C: Проект нижнього рівня має містити опис призначення та методів використання всіх інтерфейсів модулів ФБО, надаючи повну деталізацію всіх результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_LLD.2.10C: Проект нижнього рівня має містити опис розділення ОО на модулі, що реалізують ПБО, та інші | |
| | Відповідність проекту архітектури: показ | ADV_RCR.2.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.2.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають продемонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО.<br>ADV_RCR.2.2C: Для кожної суміжної пари наявних представлень ФБО, де частини обох представлень специфіковані, як мінімум напівформально, демонстрація відповідності між цими частинами представлень має бути напівформальною | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.2.1C, наявні результати аналізу відповідності між проектом нижнього рівня ФБО та проектом верхнього рівня ФБО |
| Г-6 | На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ | ADV_LLD.2.1D: Розробник повинен надати проект нижнього рівня ФБО.<br>ADV_LLD.2.1C: Представлення проекту нижнього рівня має бути напівформальним.<br>ADV_LLD.2.2C: Проект нижнього рівня має бути внутрішньо несуперечливим.<br>ADV_LLD.2.3C: Проект нижнього рівня має містити опис структури ФБО в термінах модулів.<br>ADV_LLD.2.4C: Проект нижнього рівня має містити опис призначення кожного модуля.<br>ADV_LLD.2.5C: Проект нижнього рівня має визначати взаємозв'язки між модулями в термінах функціональних можливостей безпеки, що надаються, та залежностей від інших модулів.<br>ADV_LLD.2.6C: Проект нижнього рівня має містити опис того, як надається кожна з функцій, що реалізують ПБО.<br>ADV_LLD.2.7C: Проект нижнього рівня має ідентифікувати всі інтерфейси модулів ФБО.<br>ADV_LLD.2.8C: Проект нижнього рівня має ідентифікувати, які з інтерфейсів | Немає |
| | Стиль | | |

| | | | |
|---|---|---|---|
| | специфікації: частково формалізована | модулів ФБО є видимими ззовні.<br>ADV_LLD.2.9C: Проект нижнього рівня має містити опис призначення та методів використання всіх інтерфейсів модулів ФБО, надаючи повну деталізацію всіх результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_LLD.2.10C: Проект нижнього рівня має містити опис розділення ОО на модулі, що реалізують ПБО, та інші | |
| | Відповідність проекту архітектури: демонстрація | ADV_RCR.3.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.3.2D: Для тих із відповідних частин представлень, які специфіковані формально, розробник повинен довести цю відповідність.<br>ADV_RCR.3.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають доказати або продемонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО.<br>ADV_RCR.3.2C: Для кожної суміжної пари наявних представлень ФБО, де частини одного представлення специфіковані напівформально, а іншого, як мінімум напівформально, демонстрація відповідності між цими частинами представлень має бути напівформальною.<br>ADV_RCR.3.3C: Для кожної суміжної пари наявних представлень ФБО, де частини обох представлень специфіковані формально, доказ відповідності між цими частинами представлень має бути формальним | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.3.1C, наявні результати аналізу відповідності між проектом нижнього рівня ФБО та проектом верхнього рівня ФБО |
| Г-7 | На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх | ADV_LLD.3.1D: Розробник повинен надати проект нижнього рівня ФБО.<br>ADV_LLD.3.1C: Представлення проекту нижнього рівня має бути формальним.<br>ADV_LLD.3.2C: Проект нижнього рівня має бути внутрішньо несуперечливим.<br>ADV_LLD.3.3C: Проект нижнього рівня має містити опис структури ФБО в термінах модулів.<br>ADV_LLD.3.4C: Проект нижнього рівня має містити опис призначення кожного модуля.<br>ADV_LLD.3.5C: Проект нижнього рівня має визначати взаємозв'язки між | Немає |

| | | | |
|---|---|---|---|
| | компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ | модулями в термінах функціональних можливостей безпеки, що надаються, та залежностей від інших модулів.<br>ADV_LLD.3.6C: Проект нижнього рівня має містити опис того, як надається кожна з функцій, що реалізують ПБО.<br>ADV_LLD.3.7C: Проект нижнього рівня має ідентифікувати всі інтерфейси модулів ФБО.<br>ADV_LLD.3.8C: Проект нижнього рівня має ідентифікувати, які з інтерфейсів модулів ФБО є видимими ззовні.<br>ADV_LLD.3.9C: Проект нижнього рівня має містити опис призначення та методів використання всіх інтерфейсів модулів ФБО, надаючи повну деталізацію всіх результатів, нештатних ситуацій і повідомлень про помилки.<br>ADV_LLD.3.10C: Проект нижнього рівня має містити опис розділення ОО на модулі, що реалізують ПБО, та інші | |
| | Стиль специфікації: формалізована | | |
| | Відповідність проекту архітектури: доказ | ADV_RCR.3.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.3.2D: Для тих із відповідних частин представлень, які специфіковані формально, розробник повинен довести цю відповідність.<br>ADV_RCR.3.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають доказати або продемонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО.<br>ADV_RCR.3.2C: Для кожної суміжної пари наявних представлень ФБО, де частини одного представлення специфіковані напівформально, а іншого – як мінімум, напівформально, демонстрація відповідності між цими частинами представлень має бути напівформальною.<br>ADV_RCR.3.3C: Для кожної суміжної пари наявних представлень ФБО, де частини обох представлень специфіковані формально, доказ відповідності між цими частинами представлень має бути формальним | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.3.1C, наявні результати аналізу відповідності між проектом нижнього рівня ФБО та проектом верхнього рівня ФБО |

Таблиця 9.5 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується реалізації

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-3, Г-4 | Розробник повинен подати вхідний код частини КЗЗ | ADV_IMP.1.1D: Розробник має забезпечити представлення реалізації для обраної підмножини ФБО.<br>ADV_IMP.1.1C: Представлення реалізації має однозначно визначати ФБО на такому рівні деталізації, щоб ФБО могли бути створені без подальших проектних рішень.<br>ADV_IMP.1.2C: Представлення реалізації має бути внутрішньо несуперечливим | У представленні реалізації, зазначеному в елементі довіри ADV_IMP.1.1C, наявний вхідний код реалізації відповідної підмножини ФБО |
| | Відповідність детальному проекту: показ | ADV_RCR.1.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.1.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають демонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.1.1C, наявні результати аналізу відповідності між представленням реалізації та проектом нижнього рівня ФБО |
| Г-5, Г-6 | Розробник повинен подати вхідний код усього КЗЗ | ADV_IMP.2.1D: Розробник має забезпечити представлення реалізації для всіх ФБО.<br>ADV_IMP.2.1C: Представлення реалізації має однозначно визначати ФБО на такому рівні деталізації, щоб ФБО могли бути створені без подальших проектних рішень.<br>ADV_IMP.2.2C: Представлення реалізації має бути внутрішньо несуперечливим.<br>ADV_IMP.2.3C: Представлення реалізації має містити опис взаємозв'язків між усіма частинами реалізації | У представленні реалізації, зазначеному в елементі довіри ADV_IMP.2.1C, наявний вхідний код реалізації усіх ФБО |
| | Відповідність детальному проекту: показ | ADV_RCR.2.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.2.1C: Для кожної суміжної | У результатах аналізу відповідності, зазначених в елементі довіри |

| | | | |
|---|---|---|---|
| | | пари наявних представлень ФБО результати аналізу мають продемонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО.<br>ADV_RCR.2.2C: Для кожної суміжної пари наявних представлень ФБО, де частини обох представлень специфіковані, як мінімум напівформально, демонстрація відповідності між цими частинами представлень має бути напівформальною | ADV_RCR.2.1C, наявні результати аналізу відповідності між представленням реалізації та проектом нижнього рівня ФБО |
| Г-7 | Розробник повинен подати вхідний код усього КЗЗ та усіх бібліотек часу виконання | ADV_IMP.3.1D: Розробник має забезпечити представлення реалізації для всіх ФБО.<br>ADV_IMP.3.1C: Представлення реалізації має однозначно визначати ФБО на такому рівні деталізації, щоб ФБО могли бути створені без подальших проектних рішень.<br>ADV_IMP.3.2C: Представлення реалізації має бути внутрішньо несуперечливим.<br>ADV_IMP.3.3C: Представлення реалізації має містити опис взаємозв'язків між усіма частинами реалізації.<br>ADV_IMP.3.4C: Представлення реалізації має бути структурованим на невеликі та зрозумілі розділи | У представленні реалізації, зазначеному в елементі довіри ADV_IMP.3.1C, наявний вхідний код реалізації усіх ФБО та всіх бібліотек часу виконання, що входять до складу ОО |
| | Відповідність детальному проекту: демонстрація | ADV_RCR.3.1D: Розробник повинен надати результати аналізу відповідності між усіма суміжними парами наявних представлень ФБО.<br>ADV_RCR.3.2D: Для тих із відповідних частин представлень, які специфіковані формально, розробник повинен довести цю відповідність.<br>ADV_RCR.3.1C: Для кожної суміжної пари наявних представлень ФБО результати аналізу мають доказати або продемонструвати, що всі функціональні можливості більш абстрактного представлення ФБО, що мають відношення до безпеки, правильно і повністю уточнені у менш абстрактному представленні ФБО.<br>ADV_RCR.3.2C: Для кожної суміжної пари наявних представлень ФБО, де частини одного представлення | У результатах аналізу відповідності, зазначених в елементі довіри ADV_RCR.3.1C, наявні результати аналізу відповідності між представленням реалізації та проектом нижнього рівня ФБО |

| | | | |
|---|---|---|---|
| | | специфіковані напівформально, а іншого, як мінімум напівформально, демонстрація відповідності між цими частинами представлень має бути напівформальною.<br>ADV_RCR.3.3C: Для кожної суміжної пари наявних представлень ФБО, де частини обох представлень специфіковані формально, доказ відповідності між цими частинами представлень має бути формальним | |

## 10 Відомості щодо відповідності компонентів довіри до безпеки згідно з ISO/IEC 15408 вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо середовища функціонування

*У цьому розділі у таблиці 10.1 викладено відомості щодо відповідності елементів відповідних компонентів довіри, встановлених стандартом ISO/IEC 15408, вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99 щодо, середовища функціонування. Відомості викладено у табличному вигляді із зазначенням: рівня (рівнів) гарантій; вимог НД ТЗІ 2.5-004-99 щодо відповідного рівня гарантій; вимог стандарту ISO/IEC 15408-3 щодо елементів відповідних компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких для певного засобу технічного захисту інформації від НСД у процесі виконання зіставлення компонентів довіри, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 можна приймати рішення про те, що певна сукупність елементів компонентів довіри задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.*

Таблиця 10.1 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо середовища функціонування

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1, Г-2 | Розробник повинен представити засоби інсталяції, генерації і запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. Розробник повинен представити | ADO_IGS.1.1D, ADO_IGS.2.1D: Розробник повинен задокументувати процедури, необхідні для безпечного встановлення, генерації та запуску ОО.<br>ADO_IGS.1.1C, ADO_IGS.2.1C: Документація щодо встановлення, генерації та запуску має містити опис послідовності усіх дій, необхідних для безпечного встановлення, генерації та запуску ОО | У документації щодо встановлення, генерації та запуску, зазначеній в елементах довіри ADO_IGS.1.1C чи ADO_IGS.2.1C, наведено перелік усіх можливих параметрів конфігурації, які можуть |

| | | | |
|---|---|---|---|
| | перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску | | використовуватися в процесі встановлення, генерації та запуску ОО |
| Г-3 - Г-5 | Розробник повинен представити засоби інсталяції, генерації і запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану.<br>Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску | ADO_IGS.1.1D, ADO_IGS.2.1D: Розробник повинен задокументувати процедури, необхідні для безпечного встановлення, генерації та запуску ОО.<br>ADO_IGS.1.1C, ADO_IGS.2.1C: Документація щодо встановлення, генерації та запуску має містити опис послідовності усіх дій, необхідних для безпечного встановлення, генерації та запуску ОО | У документації щодо встановлення, генерації та запуску, зазначеній в елементах довіри ADO_IGS.1.1C чи ADO_IGS.2.1C, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі встановлення, генерації та запуску ОО |
| | Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, яке поставляється Замовнику, точно відповідає еталонній копії | ADO_DEL2.1D: Розробник повинен задокументувати процедури постачання ОО або його частин споживачу.<br>ADO_DEL.2.2D: Розробник повинен використовувати процедури постачання.<br>ADO_DEL.2.1C: Документація щодо постачання має містити опис усіх процедур, необхідних для підтримки безпеки при розповсюдженні версій ОО до місць використання.<br>ADO_DEL.2.2C: Документація щодо постачання має містити опис того, як різні процедури та технічні заходи забезпечують виявлення модифікацій або будь-яких розбіжностей між оригіналом розробника та версією, одержаною в місці використання.<br>ADO_DEL.2.3C: Документація щодо постачання має містити опис того, як різні процедури дозволяють виявити | Процедури, наведені у документації щодо постачання, зазначеній в елементах довіри ADO_DEL.2.1C, ADO_DEL.2.2C та ADO_DEL.2.3C, у сукупності складають систему технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення ОО, яке поставляється Замовнику, точно відповідає еталонній копії |

| | | | |
|---|---|---|---|
| | | спробу підміни від імені розробника, навіть у тих випадках, коли розробник нічого не відправляв до місця використання | |
| Г-6, Г-7 | Розробник повинен представити засоби інсталяції, генерації і запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску | ADO_IGS.1.1D, ADO_IGS.2.1D: Розробник повинен задокументувати процедури, необхідні для безпечного встановлення, генерації та запуску ОО.<br>ADO_IGS.1.1C, ADO_IGS.2.1C: Документація щодо встановлення, генерації та запуску має містити опис послідовності усіх дій, необхідних для безпечного встановлення, генерації та запуску ОО | У документації щодо встановлення, генерації та запуску, зазначеній в елементах довіри ADO_IGS.1.1C чи ADO_IGS.2.1C, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі встановлення, генерації та запуску ОО |
| | Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, яке поставляється Замовнику, точно відповідає еталонній копії | ADO_DEL.3.1D: Розробник повинен задокументувати процедури постачання ОО або його частин споживачу.<br>ADO_DEL.3.2D: Розробник повинен використовувати процедури постачання.<br>ADO_DEL.3.1C: Документація щодо постачання має містити опис усіх процедур, необхідних для підтримки безпеки при розповсюдженні версій ОО до місць використання.<br>ADO_DEL.3.2C: Документація щодо постачання має містити опис того, як різні процедури та технічні заходи забезпечують запобігання модифікаціям або будь-яким розбіжностям між оригіналом розробника та версією, одержаною в місці використання.<br>ADO_DEL.3.3C: Документація щодо постачання має містити опис того, як різні процедури дозволяють виявити спробу підміни від імені розробника, навіть у тих випадках, коли розробник нічого не відправляв до місця використання | Процедури, наведені у документації щодо постачання, зазначеній в елементах довіри ADO_DEL.3.1C, ADO_DEL.3.2C та ADO_DEL.3.3C, у сукупності складають систему технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення ОО, яке поставляється Замовнику, точно відповідає еталонній копії, а також систему керування розповсюдженням ОО |
| | Для підтримки відповідності між КЗЗ, що поставляється Замовнику, і еталонною копією повинна існувати система керування розповсюдженням захищеного ОЕ | | |

## 11 Відомості щодо відповідності компонентів довіри до безпеки згідно з ISO/IEC 15408 вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо документації

*У цьому розділі у таблиці 11.1 викладено відомості щодо відповідності елементів відповідних компонентів довіри, встановлених стандартом ISO/IEC 15408, вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо документації. Відомості викладено у табличному вигляді із зазначенням: рівня (рівнів) гарантій; вимог НД ТЗІ 2.5-004-99 щодо відповідного рівня гарантій; вимог стандарту ISO/IEC 15408-3 щодо елементів відповідних компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких для певного засобу технічного захисту інформації від НСД у процесі виконання зіставлення компонентів довіри, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 можна приймати рішення про те, що певна сукупність елементів компонентів довіри задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.*

Таблиця 11.1 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 1 5408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо документації

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1 - Г-7 | У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки | ADV_FSP.1.1D, ADV_FSP.2.1D: Розробник повинен надати функціональну специфікацію. ADV_FSP.1.1C, ADV_FSP.2.1C: Функціональна специфікація має містити неформальний опис ФБО та їх зовнішніх інтерфейсів | У неформальному описі ФБО та їх зовнішніх інтерфейсів, зазначеному в елементах довіри ADV_FSP.1.1C чи ADV_FSP.2.1C, містяться відомості щодо політики безпеки, що реалізується ОО |
| | В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики | | |

| | | | |
|---|---|---|---|
| | безпеки, що реалізується КЗЗ оцінюваної ОЕ, а також самі послуги. | | |
| | Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску ОЕ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску ОЕ, опис властивостей ОЕ, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує ОЕ | AGD_ADM.1.1D: Розробник повинен надати настанови адміністратору, призначені для персоналу системного адміністрування.<br>AGD_ADM.1.1C: Настанови адміністратору мають містити опис функцій адміністрування та інтерфейсів, доступних адміністратору ОО.<br>AGD_ADM.1.2C: Настанови адміністратору мають містити опис того, як керувати ОО безпечним чином.<br>AGD_ADM.1.3C: Настанови адміністратору мають містити попередження щодо функцій та привілеїв, які слід контролювати у безпечному середовищі оброблення інформації.<br>AGD_ADM.1.4C: Настанови адміністратору мають містити опис усіх припущень щодо поведінки користувача, які пов'язані з безпечною експлуатацією ОО.<br>AGD_ADM.1.5C: Настанови адміністратору мають містити опис усіх параметрів безпеки, що контролюються адміністратором, із зазначенням за необхідності їх безпечних значень.<br>AGD_ADM.1.6C: Настанови адміністратору мають містити опис кожного типу події, що мають відношення до безпеки, які пов'язані з виконанням обов'язкових функцій адміністрування, у тому числі зміну характеристик безпеки сутностей, контрольованих ФБО.<br>AGD_ADM.1.7C: Настанови адміністратору мають бути узгоджені з усієї іншою документацією, наданою для оцінювання.<br>AGD_ADM.1.8C: Настанови адміністратору мають містити опис усіх вимог безпеки до середовища інформаційної технології (ІТ), що мають відношення до адміністратора | Немає |

| | | | |
|---|---|---|---|
| | Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором) | AGD_USR.1.1D: Розробник повинен надати настанови користувачу.<br>AGD_USR.1.1C: Настанови користувачу мають містити опис функцій адміністрування та інтерфейсів, доступних користувачам ОО, не пов'язаним із адмініструванням.<br>AGD_USR.1.2C: Настанови користувачу мають містити опис використання доступних користувачам функцій безпеки, що надаються ОО.<br>AGD_USR.1.3C: Настанови користувачу мають містити попередження щодо доступних користувачу функцій та привілеїв, які слід контролювати у безпечному середовищі оброблення інформації.<br>AGD_USR.1.4C: Настанови користувачу має чітко визначати всі обов'язки користувача, необхідні для безпечної експлуатації ОО, у тому числі обов'язки, пов'язані з припущеннями стосовно дій користувача, які містяться у викладенні середовища безпеки ОО.<br>AGD_USR.1.5C: Настанови користувачу мають бути узгоджені з усієї іншою документацією, наданою для оцінювання.<br>AGD_USR.1.6C: Настанови користувачу мають містити опис усіх вимог безпеки до середовища ІТ, що мають відношення до користувача | Немає |

## 12 Відомості щодо відповідності компонентів довіри до безпеки згідно з ISO/IEC 15408 вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо випробувань

*У цьому розділі у таблиці 12.1 викладено відомості щодо відповідності елементів відповідних компонентів довіри, встановлених стандартом ISO/IEC 15408, вимогам критеріїв гарантій, встановленим НД ТЗІ 2.5-004-99, щодо випробувань. Відомості викладено у табличному вигляді із зазначенням: рівня (рівнів) гарантій; вимог НД ТЗІ 2.5-004-99 щодо відповідного рівня гарантій; вимог стандарту ISO/IEC 15408-3 щодо елементів відповідних компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких для певного засобу технічного захисту інформації від НСД у процесі виконання зіставлення компонентів довіри, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 можна приймати рішення про те, що певна сукупність елементів компонентів довіри задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.*

Таблиця 12.1 – відомості щодо відповідності елементів компонентів довіри згідно з ISO/IEC 15408 вимогам критеріїв гарантій НД ТЗІ 2.5-004-99 щодо випробувань

| **Рівень гарантій** | **Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99** | **Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99** | **Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99** |
|---|---|---|---|
| Г-1 | Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття | ATE_FUN.1.1D, ATE_FUN.2.1D: Розробник повинен протестувати ФБО та задокументувати результати.<br>ATE_FUN.1.2D, ATE_FUN.2.2D: Розробник повинен надати тестову документацію.<br>ATE_FUN.1.1C, ATE_FUN.2.1C: Тестова документація має містити плани та описи процедур тестування, а також очікуваних і фактичних результатів тестування.<br>ATE_FUN.1.2C, ATE_FUN.2.2C: Плани тестування мають ідентифікувати функції безпеки, що перевіряються, та містити викладення цілей виконуваних тестів.<br>ATE_FUN.1.3C, ATE_FUN.2.3C: Описи процедур тестування мають ідентифікувати тести, які необхідно виконати, та містити сценарії для тестування кожної функції безпеки. Ці сценарії мають ураховувати будь-який вплив послідовності виконання тестів на результати інших тестів.<br>ATE_FUN.1.4C, ATE_FUN.2.4C: Очікувані результати тестування мають показати прогнозовані вихідні дані у разі успішного виконання тестів.<br>ATE_FUN.1.5C, ATE_FUN.2.5C: Результати виконання тестів розробником мають демонструвати, що кожна перевірена функція безпеки виконувалась відповідно до специфікацій.<br>ATE_COV.1.1D: Розробник повинен надати свідоцтво покриття тестами.<br>ATE_COV.1.1C: Свідоцтво покриття тестами має показати відповідність між тестами, ідентифікованими у тестовій документації, та описом ФБО у функціональній специфікації.<br>ATE_DPT.1.1D: Розробник повинен | У планах тестування, зазначених в елементах довіри ATE_FUN.1.2C чи ATE_FUN.2.2C, передбачено тестування функцій безпеки, реалізованих усіма функціональними компонентами безпеки згідно з ISO/IEC 15408-2, які відповідають всім ФПБ, що надаються КЗЗ ОЕ |
| | Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування | | |

| | | | |
|---|---|---|---|
| | | надати аналіз глибини тестування.<br>ATE_DPT.1.1C: Аналіз глибини має показати достатність тестів, ідентифікованих у тестовій документації, для демонстрації того, що ФБО виконуються відповідно до проекту верхнього рівня | |
| Г-2, Г-3 | Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття | ATE_FUN.1.1D, ATE_FUN.2.1D: Розробник повинен протестувати ФБО та задокументувати результати.<br>ATE_FUN.1.2D, ATE_FUN.2.2D: Розробник повинен надати тестову документацію.<br>ATE_FUN.1.1C, ATE_FUN.2.1C: Тестова документація має містити плани та описи процедур тестування, а також очікуваних і фактичних результатів тестування.<br>ATE_FUN.1.2C, ATE_FUN.2.2C: Плани тестування мають ідентифікувати функції безпеки, що перевіряються, та містити викладення цілей виконуваних тестів.<br>ATE_FUN.1.3C, ATE_FUN.2.3C: Описи процедур тестування мають ідентифікувати тести, які необхідно виконати, та містити сценарії для тестування кожної функції безпеки. Ці сценарії мають ураховувати будь-який вплив послідовності виконання тестів на результати інших тестів.<br>ATE_FUN.1.4C, ATE_FUN.2.4C: Очікувані результати тестування мають показати прогнозовані вихідні дані у разі успішного виконання тестів.<br>ATE_FUN.1.5C, ATE_FUN.2.5C: Результати виконання тестів розробником мають демонструвати, що кожна перевірена функція безпеки виконувалась відповідно до специфікацій.<br>ATE_COV.2.1D: Розробник повинен надати аналіз покриття тестами.<br>ATE_COV.2.1C: Аналіз покриття тестами має продемонструвати відповідність між тестами, ідентифікованими у тестовій документації, та описом ФБО у функціональній специфікації.<br>ATE_COV.2.2C: Аналіз покриття тестами має продемонструвати повну відповідність між описом ФБО у функціональній специфікації та | У планах тестування, зазначених в елементах довіри ATE_FUN.1.2C чи ATE_FUN.2.2C, передбачено тестування функцій безпеки, реалізованих усіма функціональними компонентами безпеки згідно з ISO/IEC 15408-2, відповідними до всіх ФПБ, що надаються КЗЗ ОЕ |
| | Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування | | |
| | Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені | | |

| | | | |
|---|---|---|---|
| | недоліки були усунені і не з'явилися нові “слабкі місця ” | тестами, ідентифікованими у тестовій документації.<br>ATE_DPT.2.1D: Розробник повинен надати аналіз глибини тестування.<br>ATE_DPT.2.1C: Аналіз глибини має показати достатність тестів, ідентифікованих у тестовій документації, для демонстрації того, що ФБО виконуються відповідно до проекту верхнього рівня та проекту нижнього рівня | |
| Г-4, Г-5 | Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття | ATE_FUN.1.1D, ATE_FUN.2.1D: Розробник повинен протестувати ФБО та задокументувати результати.<br>ATE_FUN.1.2D, ATE_FUN.2.2D: Розробник повинен надати тестову документацію.<br>ATE_FUN.1.1C, ATE_FUN.2.1C: Тестова документація має містити плани та описи процедур тестування, а також очікуваних і фактичних результатів тестування.<br>ATE_FUN.1.2C, ATE_FUN.2.2C: Плани тестування мають ідентифікувати функції безпеки, що перевіряються, та містити викладення цілей виконуваних тестів.<br>ATE_FUN.1.3C, ATE_FUN.2.3C: Описи процедур тестування мають ідентифікувати тести, які необхідно виконати, та містити сценарії для тестування кожної функції безпеки. Ці сценарії мають ураховувати будь-який вплив послідовності виконання тестів на результати інших тестів.<br>ATE_FUN.1.4C, ATE_FUN.2.4C: Очікувані результати тестування мають показати прогнозовані вихідні дані у разі успішного виконання тестів.<br>ATE_FUN.1.5C, ATE_FUN.2.5C: Результати виконання тестів розробником мають демонструвати, що кожна перевірена функція безпеки виконувалась відповідно до специфікацій.<br>ATE_COV.3.1D: Розробник повинен надати аналіз покриття тестами.<br>ATE_COV.3.1C: Аналіз покриття тестами має продемонструвати відповідність між тестами, ідентифікованими у тестовій документації, та описом ФБО у функціональній специфікації. | У планах тестування, зазначених в елементах довіри ATE_FUN.1.2C чи ATE_FUN.2.2C, передбачено тестування функцій безпеки, реалізованих усіма компонентами безпеки згідно з ISO/IEC 15408-2, відповідними до всіх ФПБ, що надаються КЗЗ ОЕ |
| | Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування | | |
| | Розробник повинен усунути або нейтралізувати всі знайдені "слабкі місця" і виконати повторне | | |

| | | | |
|---|---|---|---|
| | тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові "слабкі місця" | ATE_COV.3.2C: Аналіз покриття тестами має продемонструвати повну відповідність між описом ФБО у функціональній специфікації та тестами, ідентифікованими у тестовій документації.<br>ATE_COV.3.3C: Аналіз покриття тестами має переконливо продемонструвати, що всі зовнішні інтерфейси ФБО, ідентифіковані у функціональній специфікації, повністю перевірені.<br>ATE_DPT.3.1D: Розробник повинен надати аналіз глибини тестування.<br>ATE_DPT.3.1C: Аналіз глибини має показати достатність тестів, ідентифікованих у тестовій документації, для демонстрації того, що ФБО виконуються відповідно до проекту верхнього рівня, проекту нижнього рівня та представлення реалізації | |
| | Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ відносно стійкий до такого роду атак з боку Розробника | AVA_VLA.3.1D: Розробник повинен виконати аналіз уразливостей.<br>AVA_VLA.3.2D: Розробник повинен надати документацію аналізу уразливостей.<br>AVA_VLA.3.1C: Документація аналізу уразливостей має містити опис аналізу матеріалів ОО, що постачаються, виконаного для пошуку способів, в які користувач може порушити ПБО.<br>AVA_VLA.3.2C: Документація аналізу уразливостей має містити опис рішення стосовно ідентифікованих уразливостей.<br>AVA_VLA.3.3C: Документація аналізу уразливостей має показувати для всіх ідентифікованих уразливостей, що жодна з них не може бути використана у передбачуваному середовищі ОО.<br>AVA_VLA.3.4C: Документація аналізу уразливостей має містити логічне обґрунтування того, що ОО з ідентифікованими уразливостями стійкий стосовно очевидних атак проникнення.<br>AVA_VLA.3.5C: Документація аналізу уразливостей має показувати, що пошук уразливостей є систематичним | У документації аналізу уразливостей, зазначеній в елементах довіри AVA_VLA.3.1C, AVA_VLA.3.2C та AVA_VLA.3.3C, міститься підтвердження того, що ФБО є відносно стійкими до атак з боку Розробника |

| | | | |
|---|---|---|---|
| Г-6, Г-7 | Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття | ATE_FUN.1.1D, ATE_FUN.2.1D: Розробник повинен протестувати ФБО та задокументувати результати.<br>ATE_FUN.1.2D, ATE_FUN.2.2D: Розробник повинен надати тестову документацію.<br>ATE_FUN.1.1C, ATE_FUN.2.1C: Тестова документація має містити плани та описи процедур тестування, а також очікуваних і фактичних результатів тестування.<br>ATE_FUN.1.2C, ATE_FUN.2.2C: Плани тестування мають ідентифікувати функції безпеки, що перевіряються, та містити викладення цілей виконуваних тестів.<br>ATE_FUN.1.3C, ATE_FUN.2.3C: Описи процедур тестування мають ідентифікувати тести, які необхідно виконати, та містити сценарії для тестування кожної функції безпеки. Ці сценарії мають ураховувати будь-який вплив послідовності виконання тестів на результати інших тестів.<br>ATE_FUN.1.4C, ATE_FUN.2.4C: Очікувані результати тестування мають показати прогнозовані вихідні дані у разі успішного виконання тестів.<br>ATE_FUN.1.5C, ATE_FUN.2.5C: Результати виконання тестів розробником мають демонструвати, що кожна перевірена функція безпеки виконувалась відповідно до специфікацій.<br>ATE_COV.3.1D: Розробник повинен надати аналіз покриття тестами.<br>ATE_COV.3.1C: Аналіз покриття тестами має продемонструвати відповідність між тестами, ідентифікованими у тестовій документації, та описом ФБО у функціональній специфікації.<br>ATE_COV.3.2C: Аналіз покриття тестами має продемонструвати повну відповідність між описом ФБО у функціональній специфікації та тестами, ідентифікованими у тестовій документації.<br>ATE_COV.3.3C: Аналіз покриття тестами має переконливо продемонструвати, що всі зовнішні інтерфейси ФБО, ідентифіковані у функціональній специфікації, | У планах тестування, зазначених в елементах довіри ATE_FUN.1.2C чи ATE_FUN.2.2C, передбачено тестування функцій безпеки, реалізованих усіма компонентами безпеки згідно з ISO/IEC 15408-2, які відповідають всім ФПБ, що надаються КЗЗ ОЕ |
| | Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування | | |
| | Розробник повинен усунути або нейтралізувати всі знайдені "слабкі місця" і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові "слабкі місця " | | |

| | | | |
|---|---|---|---|
| | | повністю перевірені.<br>ATE_DPT.3.1D: Розробник повинен надати аналіз глибини тестування.<br>ATE_DPT.3.1C: Аналіз глибини має показати достатність тестів, ідентифікованих у тестовій документації, для демонстрації того, що ФБО виконуються відповідно до проекту верхнього рівня, проекту нижнього рівня та представлення реалізації | |
| | Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ абсолютно стійкий до такого роду атак з боку Розробника | AVA_VLA.4.1D: Розробник повинен виконати аналіз уразливостей.<br>AVA_VLA.4.2D: Розробник повинен надати документацію аналізу уразливостей.<br>AVA_VLA.4.1C: Документація аналізу уразливостей має містити опис аналізу матеріалів ОО, що постачаються, виконаного для пошуку способів, в які користувач може порушити ПБО.<br>AVA_VLA.4.2C: Документація аналізу уразливостей має містити опис рішення стосовно ідентифікованих уразливостей.<br>AVA_VLA.4.3C: Документація аналізу уразливостей має показувати для всіх ідентифікованих уразливостей, що жодна з них не може бути використана у передбачуваному середовищі ОО.<br>AVA_VLA.4.4C: Документація аналізу уразливостей має містити логічне обґрунтування того, що ОО з ідентифікованими уразливостями стійкий стосовно очевидних атак проникнення.<br>AVA_VLA.4.5C: Документація аналізу уразливостей має показувати, що пошук уразливостей є систематичним.<br>AVA_VLA.4.6C: Документація аналізу уразливостей має містити логічне обґрунтування, що аналіз повністю враховує усі матеріали ОО, що постачаються | У документації аналізу уразливостей, зазначеній в елементах довіри AVA_VLA.3.1C, AVA_VLA.3.2C та AVA_VLA.3.3C, міститься підтвердження того, що ФБО є абсолютно стійкими до атак з боку Розробника |

## 13 Порядок документування результатів зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

13.1 Якщо зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 виконувалося у ході робіт із оцінювання рівня гарантій коректності реалізації ФПБ під час проведення державної експертизи в сфері ТЗІ, результати зіставлення мають бути документовані у порядку, визначеному НД ТЗІ 2.6-001-11, у вигляді відповідного звіту.

Крім цього, факт виконання зіставлення в ході проведення експертних робіт має бути зазначений у розділі "Результати експертних робіт" експертного висновку, складеного за результатами експертизи відповідно до рекомендацій, наведених у Додатку Е до НД ТЗІ 2.6-001-11. При цьому у розділі "Перелік документів, склад програмних та технічних засобів, які надано на експертизу" експертного висновку мають бути наведені посилання на всі документи (матеріали), що містять результати оцінювання (сертифікації) відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи) на відповідність стандарту ISO/IEC 15408, які були використані під час проведення державної експертизи.

13.2 У всіх інших випадках результати зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 документуються у довільній формі.

## Додаток А
**(рекомендований)**

## Відомості щодо застосовності елементів компонентів довіри до безпеки згідно з ISO/IEC 15408 для задоволення вимог критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99

*У таблицях А.1-А.11 Додатка А викладені відомості щодо застосовності елементів компонентів довіри до безпеки сімейств класів довіри згідно з ISO/IEC 15408-3 для задоволення вимог критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99. Відповідні відомості сформульовано на підставі таблиць 7.1 - 12.1 та призначено для спрощення визначення в ході виконання прямого зіставлення груп елементів довіри, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99 щодо різних складових критеріїв гарантій для відповідних рівнів гарантій.*

Таблиця А.1 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо архітектури

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_INT – внутрішня структура ФБО | ADV_INT.1.1D | Г-1 – Г-3 |
| | ADV_INT.1.2D | Г-1 – Г-3 |
| | ADV_INT.1.1C | Г-1 – Г-3 |
| | ADV_INT.1.2C | Г-1 – Г-3 |
| | ADV_INT.1.3C | Г-3 |
| | ADV_INT.2.1D | Г-4 |
| | ADV_INT.2.2D | Г-4 |
| | ADV_INT.2.3D | Г-4 |
| | ADV_INT.2.4D | Г-4 |
| | ADV_INT.2.1C | Г-4 |
| | ADV_INT.2.2C | Г-4 |
| | ADV_INT.2.3C | Г-4 |
| | ADV_INT.2.4C | Г-4 |
| | ADV_INT.2.5C | Г-4 |
| | ADV_INT.2.4C | Г-4 |

Закінчення таблиці А.1

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_INT – внутрішня структура ФБО (продовження) | ADV_INT.3.1D | Г-5 – Г-7 |
| | ADV_INT.3.2D | Г-5 – Г-7 |
| | ADV_INT.3.3D | Г-5 – Г-7 |
| | ADV_INT.3.4D | Г-5 – Г-7 |
| | ADV_INT.3.5D | Г-5 – Г-7 |
| | ADV_INT.3.6D | Г-5 – Г-7 |
| | ADV_INT.3.1C | Г-5 – Г-7 |
| | ADV_INT.3.2C | Г-5 – Г-7 |
| | ADV_INT.3.3C | Г-5 – Г-7 |
| | ADV_INT.3.4C | Г-5 – Г-7 |
| | ADV_INT.3.5C | Г-5 – Г-7 |
| | ADV_INT.3.6C | Г-5 – Г-7 |
| | ADV_INT.3.7C | Г-5 – Г-7 |

Таблиця А.2 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо середовища розробки у частині, що стосується процесу розробки

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ALC_DVS – безпека розробки | ALC_DVS.1.1D | Г-4 – Г-7 |
| | ALC_DVS.1.1C | Г-4 – Г-7 |
| | ALC_DVS.1.2C | Г-4 – Г-7 |
| | ALC.DVS.2.1D | Г-4 – Г-7 |
| | ALC_DVS.2.1C | Г-4 – Г-7 |
| | ALC_DVS.2.2C | Г-4 – Г-7 |

Закінчення таблиці А.2

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ALC_LCD – визначення життєвого циклу | ALC_LCD.1.1D | Г-1 – Г-7 |
| | ALC_LCD.1.2D | Г-1 – Г-7 |
| | ALC_LCD.1.1C | Г-1 – Г-7 |
| | ALC_LCD.1.2C | Г-1 – Г-7 |
| | ALC_LCD.2.1D | Г-1 – Г-7 |
| | ALC_LCD.2.2D | Г-1 – Г-7 |
| | ALC_LCD.2.1C | Г-1 – Г-7 |
| | ALC_LCD.2.2C | Г-1 – Г-7 |
| | ALC_LCD.3.1D | Г-1 – Г-7 |
| | ALC_LCD.3.2D | Г-1 – Г-7 |
| | ALC_LCD.3.1C | Г-1 – Г-7 |
| | ALC_LCD.3.2C | Г-1 – Г-7 |
| ALC_TAT – інструментальні засоби і методи | ALC_TAT.2.1D | Г-3 – Г-6 |
| | ALC_TAT.2.2D | Г-3 – Г-6 |
| | ALC_TAT.2.3D | Г-3 – Г-6 |
| | ALC_TAT.2.1C | Г-3 – Г-6 |
| | ALC_TAT.2.2C | Г-3 – Г-6 |
| | ALC_TAT.2.3C | Г-3 – Г-6 |
| | ALC_TAT.3.1D | Г-7 |
| | ALC_TAT.3.2D | Г-7 |
| | ALC_TAT.3.3D | Г-7 |
| | ALC_TAT.3.1C | Г-7 |
| | ALC_TAT.3.2C | Г-7 |
| | ALC_TAT.3.3C | Г-7 |

Таблиця А.3 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо середовища розробки у частині, що стосується керування конфігурацією

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ACM_AUT – автоматизація керування конфігурацією | ACM_AUT.1.1D | Г-4, Г-5 |
| | ACM_AUT.1.2D | Г-4, Г-5 |
| | ACM_AUT.1.1C | Г-4, Г-5 |
| | ACM_AUT.1.2C | Г-4, Г-5 |
| | ACM_AUT.1.3C | Г-4, Г-5 |
| | ACM_AUT.1.4C | Г-4, Г-5 |
| | ACM_AUT.2.1D | Г-6, Г-7 |
| | ACM_AUT.2.2D | Г-6, Г-7 |
| | ACM_AUT.2.1C | Г-6, Г-7 |
| | ACM_AUT.2.2C | Г-6, Г-7 |
| | ACM_AUT.2.3C | Г-6, Г-7 |
| | ACM_AUT.2.4C | Г-6, Г-7 |
| | ACM_AUT.2.5C | Г-6, Г-7 |
| | ACM_AUT.2.6C | Г-6, Г-7 |
| ACM_CAP – можливості керування конфігурацією | ACM_CAP.3.1D | Г-1 – Г-3 |
| | ACM_CAP.3.2D | Г-1 – Г-3 |
| | ACM_CAP.3.3D | Г-1 – Г-3 |
| | ACM_CAP.3.1C | Г-1 – Г-3 |
| | ACM_CAP.3.2C | Г-1 – Г-3 |
| | ACM_CAP.3.3C | Г-1 – Г-3 |
| | ACM_CAP.3.4C | Г-1 – Г-3 |
| | ACM_CAP.3.5C | Г-1 – Г-3 |
| | ACM_CAP.3.6C | Г-1 – Г-3 |

Продовження таблиці А.3

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ACM_CAP – можливості керування конфігурацією (продовження) | ACM_CAP.3.7C | Г-1 – Г-3 |
| | ACM_CAP.3.8C | Г-1 – Г-3 |
| | ACM_CAP.3.9C | Г-1 – Г-3 |
| | ACM_CAP.3.10C | Г-1 – Г-3 |
| | ACM_CAP.3.11C | Г-1 – Г-3 |
| | ACM_CAP.4.1D | Г-4, Г-5 |
| | ACM_CAP.4.2D | Г-4, Г-5 |
| | ACM_CAP.4.3D | Г-4, Г-5 |
| | ACM_CAP.4.1C | Г-4, Г-5 |
| | ACM_CAP.4.2C | Г-4, Г-5 |
| | ACM_CAP.4.3C | Г-4, Г-5 |
| | ACM_CAP.4.4C | Г-4, Г-5 |
| | ACM_CAP.4.5C | Г-4, Г-5 |
| | ACM_CAP.4.6C | Г-4, Г-5 |
| | ACM_CAP.4.7C | Г-4, Г-5 |
| | ACM_CAP.4.8C | Г-4, Г-5 |
| | ACM_CAP.4.9C | Г-4, Г-5 |
| | ACM_CAP.4.10C | Г-4, Г-5 |
| | ACM_CAP.4.11C | Г-4, Г-5 |
| | ACM_CAP.4.12C | Г-4, Г-5 |
| | ACM_CAP.4.13C | Г-4, Г-5 |
| | ACM_CAP.5.1D | Г-6, Г-7 |
| | ACM_CAP.5.2D | Г-6, Г-7 |
| | ACM_CAP.5.3D | Г-6, Г-7 |

Продовження таблиці А.3

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ACM_CAP – можливості керування конфігурацією (закінчення) | ACM_CAP.5.1C | Г-6, Г-7 |
| | ACM_CAP.5.2C | Г-6, Г-7 |
| | ACM_CAP.5.3C | Г-6, Г-7 |
| | ACM_CAP.5.4C | Г-6, Г-7 |
| | ACM_CAP.5.5C | Г-6, Г-7 |
| | ACM_CAP.5.6C | Г-6, Г-7 |
| | ACM_CAP.5.7C | Г-6, Г-7 |
| | ACM_CAP.5.8C | Г-6, Г-7 |
| | ACM_CAP.5.9C | Г-6, Г-7 |
| | ACM_CAP.5.10C | Г-6, Г-7 |
| | ACM_CAP.5.11C | Г-6, Г-7 |
| | ACM_CAP.5.12C | Г-6, Г-7 |
| | ACM_CAP.5.13C | Г-6, Г-7 |
| | ACM_CAP.5.14C | Г-6, Г-7 |
| | ACM_CAP.5.15C | Г-6, Г-7 |
| | ACM_CAP.5.16C | Г-6, Г-7 |
| | ACM_CAP.5.17C | Г-6, Г-7 |
| | ACM_CAP.5.18C | Г-6, Г-7 |
| | ACM_CAP.5.19C | Г-6, Г-7 |
| | ACM_CAP.5.20C | Г-6, Г-7 |
| | ACM_CAP.5.21C | Г-6, Г-7 |
| | ACM_CAP.5.22C | Г-6, Г-7 |

Закінчення таблиці А.3

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ACM_SCP – область керування конфігурацією | ACM_SCP.1.1D | Г-1 – Г-3 |
| | ACM_SCP.1.1C | Г-1 – Г-3 |
| | ACM_SCP.2.1D | Г-1 – Г-3 |
| | ACM_SCP.2.1C | Г-1 – Г-3 |
| | ACM_SCP.3.1D | Г-4 – Г-7 |
| | ACM_SCP.3.1C | Г-4 – Г-7 |

Таблиця А.4 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується функціональних специфікацій (політики безпеки)

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_FSP – функціональна специфікація | ADV_FSP.1.1D | Г-1 – Г-7 |
| | ADV_FSP.1.1C | Г-1 – Г-7 |
| | ADV_FSP.1.2C | Г-1 – Г-7 |
| | ADV_FSP.1.3C | Г-1 – Г-7 |
| | ADV_FSP.1.4C | Г-1 – Г-7 |
| | ADV_FSP.2.1D | Г-1 – Г-7 |
| | ADV_FSP.2.1C | Г-1 – Г-7 |
| | ADV_FSP.2.2C | Г-1 – Г-7 |
| | ADV_FSP.2.3C | Г-1 – Г-7 |
| | ADV_FSP.2.4C | Г-1 – Г-7 |

Таблиця А.5 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується функціональних специфікацій (моделі політики безпеки)

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_SPM – моделювання політики безпеки | ADV_SPM.1.1D | Г-2 |
| | ADV_SPM.1.2D | Г-2 |
| | ADV_SPM.1.1C | Г-2 |
| | ADV_SPM.1.2C | Г-2 |
| | ADV_SPM.1.3C | Г-2 |
| | ADV_SPM.1.4C | Г-2 |
| | ADV_SPM.2.1D | Г-3 |
| | ADV_SPM.2.2D | Г-3 |
| | ADV_SPM.2.1C | Г-3 |
| | ADV_SPM.2.2C | Г-3 |
| | ADV_SPM.2.3C | Г-3 |
| | ADV_SPM.2.4C | Г-3 |
| | ADV_SPM.2.5C | Г-3 |
| | ADV_SPM.3.1D | Г-4 – Г-7 |
| | ADV_SPM.3.2D | Г-4 – Г-7 |
| | ADV_SPM.3.1C | Г-4 – Г-7 |
| | ADV_SPM.3.2C | Г-4 – Г-7 |
| | ADV_SPM.3.3C | Г-4 – Г-7 |
| | ADV_SPM.3.4C | Г-4 – Г-7 |
| | ADV_SPM.3.5C | Г-4 – Г-7 |

Таблиця А.6 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується проекту архітектури

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_HLD – проект верхнього рівня | ADV_HLD.2.1D | Г-1, Г-2 |
| | ADV_HLD.2.1C | Г-1, Г-2 |
| | ADV_HLD.2.2C | Г-1, Г-2 |
| | ADV_HLD.2.3C | Г-1, Г-2 |
| | ADV_HLD.2.4C | Г-1, Г-2 |
| | ADV_HLD.2.5C | Г-1, Г-2 |
| | ADV_HLD.2.6C | Г-1, Г-2 |
| | ADV_HLD.2.7C | Г-1, Г-2 |
| | ADV_HLD.2.8C | Г-1, Г-2 |
| | ADV_HLD.2.9C | Г-1, Г-2 |
| | ADV_HLD.3.1D | Г-3, Г-4 |
| | ADV_HLD.3.1C | Г-3, Г-4 |
| | ADV_HLD.3.2C | Г-3, Г-4 |
| | ADV_HLD.3.3C | Г-3, Г-4 |
| | ADV_HLD.3.4C | Г-3, Г-4 |
| | ADV_HLD.3.5C | Г-3, Г-4 |
| | ADV_HLD.3.6C | Г-3, Г-4 |
| | ADV_HLD.3.7C | Г-3, Г-4 |
| | ADV_HLD.3.8C | Г-3, Г-4 |
| | ADV_HLD.3.9C | Г-3, Г-4 |
| | ADV_HLD.4.1D | Г-5 |
| | ADV_HLD.4.1C | Г-5 |
| | ADV_HLD.4.2C | Г-5 |

Продовження таблиці А.6

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| | ADV_HLD.4.3C | Г-5 |
| | ADV_HLD.4.4C | Г-5 |
| | ADV_HLD.4.5C | Г-5 |
| | ADV_HLD.4.6C | Г-5 |
| | ADV_HLD.4.7C | Г-5 |
| | ADV_HLD.4.8C | Г-5 |
| | ADV_HLD.4.9C | Г-5 |
| | ADV_HLD.4.10C | Г-5 |
| | ADV_HLD.4.11C | Г-5 |
| | ADV_HLD.5.1D | Г-6, Г-7 |
| | ADV_HLD.5.1C | Г-6, Г-7 |
| | ADV_HLD.5.2C | Г-6, Г-7 |
| | ADV_HLD.5.3C | Г-6, Г-7 |
| | ADV_HLD.5.4C | Г-6, Г-7 |
| | ADV_HLD.5.5C | Г-6, Г-7 |
| | ADV_HLD.5.6C | Г-6, Г-7 |
| | ADV_HLD.5.7C | Г-6, Г-7 |
| | ADV_HLD.5.8C | Г-6, Г-7 |
| | ADV_HLD.5.9C | Г-6, Г-7 |
| | ADV_HLD.5.10C | Г-6, Г-7 |
| | ADV_HLD.5.11C | Г-6, Г-7 |

Закінчення таблиці А.6

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_RCR – відповідність представлень | ADV_RCR.1.1D | Г-2 – Г-4 |
| | ADV_RCR.1.1C | Г-2 – Г-4 |
| | ADV_RCR.2.1D | Г-5 |
| | ADV_RCR.2.1C | Г-5 |
| | ADV_RCR.2.2C | Г-5 |
| | ADV_RCR.3.1D | Г-6, Г-7 |
| | ADV_RCR.3.2D | Г-6, Г-7 |
| | ADV_RCR.3.1C | Г-6, Г-7 |
| | ADV_RCR.3.2C | Г-6, Г-7 |
| | ADV_RCR.3.3C | Г-6, Г-7 |

Таблиця А.7 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується детального проекту

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_LLD – проект нижнього рівня | ADV_LLD.1.1D | Г-1 – Г-3 |
| | ADV_LLD.1.1C | Г-1 – Г-3 |
| | ADV_LLD.1.2C | Г-1 – Г-3 |
| | ADV_LLD.1.3C | Г-1 – Г-3 |
| | ADV_LLD.1.4C | Г-1 – Г-3 |
| | ADV_LLD.1.5C | Г-1 – Г-3 |
| | ADV_LLD.1.6C | Г-1 – Г-3 |
| | ADV_LLD.1.7C | Г-1 – Г-3 |

Продовження таблиці А.7

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_LLD – проект нижнього рівня (продовження) | ADV_LLD.1.8C | Г-1 – Г-3 |
| | ADV_LLD.1.9C | Г-1 – Г-3 |
| | ADV_LLD.1.10C | Г-1 – Г-3 |
| | ADV_LLD.2.1D | Г-4 – Г-6 |
| | ADV_LLD.2.1C | Г-4 – Г-6 |
| | ADV_LLD.2.2C | Г-4 – Г-6 |
| | ADV_LLD.2.3C | Г-4 – Г-6 |
| | ADV_LLD.2.4C | Г-4 – Г-6 |
| | ADV_LLD.2.5C | Г-4 – Г-6 |
| | ADV_LLD.2.6C | Г-4 – Г-6 |
| | ADV_LLD.2.7C | Г-4 – Г-6 |
| | ADV_LLD.2.8C | Г-4 – Г-6 |
| | ADV_LLD.2.9C | Г-4 – Г-6 |
| | ADV_LLD.2.10C | Г-4 – Г-6 |
| | ADV_LLD.3.1D | Г-7 |
| | ADV_LLD.3.1C | Г-7 |
| | ADV_LLD.3.2C | Г-7 |
| | ADV_LLD.3.3C | Г-7 |
| | ADV_LLD.3.4C | Г-7 |
| | ADV_LLD.3.5C | Г-7 |
| | ADV_LLD.3.6C | Г-7 |
| | ADV_LLD.3.7C | Г-7 |
| | ADV_LLD.3.8C | Г-7 |
| | ADV_LLD.3.9C | Г-7 |
| | ADV_LLD.3.10C | Г-7 |

Закінчення таблиці А.7

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_RCR – відповідність представлень | ADV_RCR.1.1D | Г-2 – Г-4 |
| | ADV_RCR.1.1C | Г-2 – Г-4 |
| | ADV_RCR.2.1D | Г-5 |
| | ADV_RCR.2.1C | Г-5 |
| | ADV_RCR.2.2C | Г-5 |
| | ADV_RCR.3.1D | Г-6, Г-7 |
| | ADV_RCR.3.2D | Г-6, Г-7 |
| | ADV_RCR.3.1C | Г-6, Г-7 |
| | ADV_RCR.3.2C | Г-6, Г-7 |
| | ADV_RCR.3.3C | Г-6, Г-7 |

Таблиця А.8 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо послідовності розробки у частині, що стосується реалізації

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_IMP – представлення реалізації | ADV_IMP.1.1D | Г-3, Г-4 |
| | ADV_IMP.1.1C | Г-3, Г-4 |
| | ADV_IMP.1.2C | Г-3, Г-4 |
| | ADV_IMP.2.1D | Г-5, Г-6 |
| | ADV_IMP.2.1C | Г-5, Г-6 |
| | ADV_IMP.2.2C | Г-5, Г-6 |
| | ADV_IMP.2.3C | Г-5, Г-6 |
| | ADV_IMP.3.1D | Г-7 |
| | ADV_IMP.3.1C | Г-7 |
| | ADV_IMP.3.2C | Г-7 |
| | ADV_IMP.3.3C | Г-7 |
| | ADV_IMP.3.4C | Г-7 |
| ADV_RCR – відповідність представлень | ADV_RCR.1.1D | Г-3, Г-4 |
| | ADV_RCR.1.1C | Г-3, Г-4 |
| | ADV_RCR.2.1D | Г-5, Г-6 |
| | ADV_RCR.2.1C | Г-5, Г-6 |
| | ADV_RCR.2.2C | Г-5, Г-6 |
| | ADV_RCR.3.1D | Г-7 |
| | ADV_RCR.3.2D | Г-7 |
| | ADV_RCR.3.1C | Г-7 |
| | ADV_RCR.3.2C | Г-7 |
| | ADV_RCR.3.3C | Г-7 |

Таблиця А.9 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо середовища функціонування

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADO_DEL – постачання | ADO_DEL.2.1D | Г-3 – Г-5 |
| | ADO_DEL.2.2D | Г-3 – Г-5 |
| | ADO_DEL.2.1C | Г-3 – Г-5 |
| | ADO_DEL.2.2C | Г-3 – Г-5 |
| | ADO_DEL.2.3C | Г-3 – Г-5 |
| | ADO_DEL.3.1D | Г-6, Г-7 |
| | ADO_DEL.3.2D | Г-6, Г-7 |
| | ADO_DEL.3.1C | Г-6, Г-7 |
| | ADO_DEL.3.2C | Г-6, Г-7 |
| | ADO_DEL.3.3C | Г-6, Г-7 |
| ADO_IGS – встановлення, генерація і запуск | ADO_IGS.1.1D | Г-1 – Г-7 |
| | ADO_IGS.1.1C | Г-1 – Г-7 |
| | ADO_IGS.2.1D | Г-1 – Г-7 |
| | ADO_IGS.2.1C | Г-1 – Г-7 |

Таблиця А.10 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо документації

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ADV_FSP – функціональна специфікація | ADV_FSP.1.1D | Г-1 – Г-7 |
| | ADV_FSP.1.1C | Г-1 – Г-7 |
| | ADV_FSP.2.1D | Г-1 – Г-7 |
| | ADV_FSP.2.1C | Г-1 – Г-7 |
| AGD_ADM – настанови адміністратора | AGD_ADM.1.1D | Г-1 – Г-7 |
| | AGD_ADM.1.1C | Г-1 – Г-7 |
| | AGD_ADM.1.2C | Г-1 – Г-7 |
| | AGD_ADM.1.3C | Г-1 – Г-7 |
| | AGD_ADM.1.4C | Г-1 – Г-7 |
| | AGD_ADM.1.5C | Г-1 – Г-7 |
| | AGD_ADM.1.6C | Г-1 – Г-7 |
| | AGD_ADM.1.7C | Г-1 – Г-7 |
| | AGD_ADM.1.8C | Г-1 – Г-7 |
| AGD_USR – настанови користувача | AGD_USR.1.1D | Г-1 – Г-7 |
| | AGD_USR.1.1C | Г-1 – Г-7 |
| | AGD_USR.1.2C | Г-1 – Г-7 |
| | AGD_USR.1.3C | Г-1 – Г-7 |
| | AGD_USR.1.4C | Г-1 – Г-7 |
| | AGD_USR.1.5C | Г-1 – Г-7 |
| | AGD_USR.1.6C | Г-1 – Г-7 |

Таблиця А.11 – відомості щодо застосовності елементів довіри для задоволення вимог критеріїв гарантій НД ТЗІ 2.5-004-99 щодо випробувань

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ATE_COV – покриття | ATE_COV.1.1D | Г-1 |
| | ATE_COV.1.1C | Г-1 |
| | ATE_COV.2.1D | Г-2, Г-3 |
| | ATE_COV.2.1C | Г-2, Г-3 |
| | ATE_COV.2.2C | Г-2, Г-3 |
| | ATE_COV.3.1D | Г-4 – Г-7 |
| | ATE_COV.3.1C | Г-4 – Г-7 |
| | ATE_COV.3.2C | Г-4 – Г-7 |
| | ATE_COV.3.3C | Г-4 – Г-7 |
| ATE_DPT – глибина | ATE_DPT.1.1D | Г-1, Г-2 |
| | ATE_DPT.1.1C | Г-1, Г-2 |
| | ATE_DPT.2.1D | Г-2, Г-3 |
| | ATE_DPT.2.1C | Г-2, Г-3 |
| | ATE_DPT.3.1D | Г-4 – Г-7 |
| | ATE_DPT.3.1C | Г-4 – Г-7 |
| ATE_FUN – функціональне тестування | ATE_FUN.1.1D | Г-1 – Г-7 |
| | ATE_FUN.1.2D | Г-1 – Г-7 |
| | ATE_FUN.1.1C | Г-1 – Г-7 |
| | ATE_FUN.1.2C | Г-1 – Г-7 |
| | ATE_FUN.1.3C | Г-1 – Г-7 |
| | ATE_FUN.1.4C | Г-1 – Г-7 |
| | ATE_FUN.1.5C | Г-1 – Г-7 |
| | ATE_FUN.2.1D | Г-1 – Г-7 |

Закінчення таблиці А1.11

| **Сімейство довіри згідно з ISO/IEC 15408-3** | **Елементи компонентів довіри відповідного сімейства** | **Рівні гарантій згідно з НД ТЗІ 2.5-004-99, задоволення вимог щодо яких забезпечують компоненти довіри відповідного сімейства** |
|---|---|---|
| ATE_FUN – функціональне тестування (продовження) | ATE_FUN.2.2D | Г-1 – Г-7 |
| | ATE_FUN.2.1C | Г-1 – Г-7 |
| | ATE_FUN.2.2C | Г-1 – Г-7 |
| | ATE_FUN.2.4C | Г-1 – Г-7 |
| | ATE_FUN.2.4C | Г-1 – Г-7 |
| | ATE_FUN.2.5C | Г-1 – Г-7 |
| AVA_VLA – аналіз уразливостей | AVA_VLA.3.1D | Г-4, Г-5 |
| | AVA_VLA.3.2D | Г-4, Г-5 |
| | AVA_VLA.3.1C | Г-4, Г-5 |
| | AVA_VLA.3.2C | Г-4, Г-5 |
| | AVA_VLA.3.3C | Г-4, Г-5 |
| | AVA_VLA.3.4C | Г-4, Г-5 |
| | AVA_VLA.3.5C | Г-4, Г-5 |
| | AVA_VLA.4.1D | Г-6, Г-7 |
| | AVA_VLA.4.2D | Г-6, Г-7 |
| | AVA_VLA.4.1C | Г-6, Г-7 |
| | AVA_VLA.4.2C | Г-6, Г-7 |
| | AVA_VLA.4.3C | Г-6, Г-7 |
| | AVA_VLA.4.4C | Г-6, Г-7 |
| | AVA_VLA.4.5C | Г-6, Г-7 |
| | AVA_VLA.4.6C | Г-6, Г-7 |