МЕТОДИЧНИЙ ДОКУМЕНТ З МЕТРОЛОГІЇ

МІНЕКОНОМРОЗВИТКУ УКРАЇНИ

ДЕРЖАВНЕ ПІДПРИЄМСТВО
"ВСЕУКРАЇНСЬКИЙ ДЕРЖАВНИЙ НАУКОВО-ВИРОБНИЧИЙ ЦЕНТР СТАНДАРТИЗАЦІЇ, МЕТРОЛОГІЇ, СЕРТИФІКАЦІЇ ТА ЗАХИСТУ ПРАВ СПОЖИВАЧІВ"
(ДП "УКРМЕТРТЕСТСТАНДАРТ")

ЗАТВЕРДЖУЮ

Заступник генерального директора
з метрології, оцінки відповідності
засобів вимірювальної техніки
та наукової діяльності, к.т.н.
_____Ю.В. Кузьменко
«__» _____2025 р.

М.П.

Рекомендація
Метрологія

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗАСОБІВ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ

Методика випробувань при оцінці відповідності

ТИПОВА

РОЗРОБЛЕНО
Начальник науково-виробничого
відділу вимірювань радіоелектронних
величин та іонізуючих випромінювань
_____ В. В. Гаман
«25» Березня 2025 р.
Начальник лабораторії
_____С. М. Курсін
«25» Березня 2025 р.

ПОГОДЖЕНО
Директор Науково-виробничого інституту
вимірювань електромагнітних величин та
оцінки відповідності ЗВТ
ДП «УКРМЕТРТЕСТСТАНДАРТ»
_____ О. М. Величко
«25» Березня 2025 р.

Київ
2025

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: ДЕРЖАВНЕ ПІДПРИЄМСТВО "ВСЕУКРАЇНСЬКИЙ ДЕРЖАВНИЙ НАУКОВО-ВИРОБНИЧИЙ ЦЕНТР СТАНДАРТИЗАЦІЇ, МЕТРОЛОГІЇ, СЕРТИФІКАЦІЇ ТА ЗАХИСТУ ПРАВ СПОЖИВАЧІВ" (ДП "УКРМЕТРТЕСТСТАНДАРТ")

2 ПРИЙНЯТО ТА ВВЕДЕНО В ДІЮ: _____ _____ 2025 р.

3 УВЕДЕНО ВПЕРШЕ

ЗМІСТ

МЕТРОЛОГІЯ

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗАСОБІВ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ

Методика випробувань при оцінці відповідності ТИПОВА

Введено в дію з __.__ 2025 р.

1 Сфера застосування

1.1 Ця методика розповсюджується на ПЗ ЗВТ та допоміжне ПЗ, що працює з ЗВТ, під час проведення випробувань для ОВ ЗВТ.

1.2 Методика використовується для перевірки відповідності ПЗ вимогам ДСТУ 7363 та ДСТУ OIML D 31:2018, результат цієї перевірки використовується при ОВ ЗВТ.

1.3 Методика враховує вимоги та рекомендації WELMEC 7.2:2023.

2 Нормативні посилання

Постанова Кабінету Міністрів України від 13 січня 2016 р. № 94 "Технічний регламент законодавчо регульованих засобів вимірювальної техніки".

Постанова Кабінету Міністрів України від 24 лютого 2016 р. № 163 "Технічний регламент засобів вимірювальної техніки".

ДСТУ 7363:2013 Програмне забезпечення засобів вимірювальної техніки. Загальні технічні вимоги.

ДСТУ OIML D 31:2018 Загальні вимоги до засобів вимірювальної техніки з програмним керуванням (OIML D 31:2008, IDT)

WELMEC 7.2:2023. Issue 9. Software Guide (Measuring Instruments Directive).

Measuring Instruments Directive 2014/32/EU. Директива вимірювальних приладів 2014/32/EU.

3 Познаки та скорочення

ВРВ - високий рівень жорсткість випробувань

ЗВТ – засіб вимірювальної техніки

ЗнР – законодавчо не регульований (законодавчо не релевантний)

ЗР – законодавчо регульований (законодавчо релевантний)

НРВ – низький рівень жорсткість випробувань

ОВ – оцінка відповідності вимогам ТР2 або ТР3

ООВ – орган оцінки відповідності

ОС – операційна система

ПЗ – програмне забезпечення

СРВ - середній рівень жорсткість випробувань

ТР – Технічний регламент

ТР2 – Технічний регламент засобів вимірювальної техніки

ТР3 – Технічний регламент законодавчо регульованих засобів вимірювальної техніки

4 Терміни та визначення

Автентифікація (Authentication): процес перевірки заявленої або передбачуваної особи користувача, процесу, програмного забезпечення або ЗВТ.

Автентичність (Authenticity): результат автентифікації (пройшов або не пройшов).

Аудиторський слід (Audit trail): безперервні дані, що містять інформаційні записи з часовими позначками про події, наприклад, зміни значень параметрів ЗВТ або оновлення програмного забезпечення, або іншу діяльність, яка є законодавчо важливою та критичною для метрологічних характеристик.

Базова конфігурація (Basic configuration): конструкція ЗВТ з урахуванням базової архітектури. Існує дві різні базові конфігурації: ЗВТ із використанням спеціального пристрою та ЗВТ із використанням універсального пристрою.

Вихідний код (Source code): комп'ютерна програма, написана у формі (мова програмування), яку можна читати та редагувати.

Відкрита мережа (Open network): мережа довільних учасників (пристроїв із довільними функціями). Номер, ідентифікатор і місцезнаходження учасника можуть бути динамічними та невідомими іншим учасникам (див. також закриту мережу).

Завантаження програмного забезпечення (Software download): процес автоматичної передачі програмного забезпечення на цільовий ЗВТ або компонент за допомогою будь-яких технічних засобів із локального чи віддаленого джерела (наприклад, змінного носія інформації, портативного комп'ютера, віддаленого комп'ютера) через довільні з'єднання (наприклад, прямі зв'язки, мережі) .

Закрита мережа (Closed network): мережа з фіксованою кількістю учасників із відомою ідентичністю, функціями та розташуванням (див. також відкрита мережа).

Засіб перевірки (Checking facility:): засіб, вбудований у ЗВТ або компонент і який дозволяє виявляти значні дефекти та вживати заходів.

Захисний інтерфейс (Protective interface): ЗР програмний модуль, який обробляє всі потоки ЗР даних, щоб запобігти неприпустимому впливу.

Захист (Protection): засоби для захисту даних вимірювання, параметрів, ЗВТ, компонента або програмного модуля з наміром зробити втручання неможливим або очевидним.

ЗВТ з використанням універсального комп'ютера (тип U) (Measuring instrument using a universal device (type U)): ЗВТ який містить комп'ютер загального призначення, зазвичай систему на базі ПК, для виконання ЗР функцій.

Ідентифікація програмного забезпечення (Software identification): послідовність зрозумілих символів (наприклад, номер версії, контрольна сума), яка представляє програмне забезпечення або програмний модуль, що розглядається.

Інтерфейс користувача (User interface): інтерфейс, який дозволяє обмінюватися інформацією між користувачем/оператором і ЗВТ або його (апаратними) компонентами або програмними модулями.

Інтерфейс (Interface): спільна межа між двома функціональними одиницями, визначена різними характеристиками, що стосуються функцій, фізичних взаємозв'язків, обміну сигналами та іншими характеристиками одиниць, залежно від обставин.

Клас ризику (Risk class): клас типів ЗВТ з майже ідентичними оцінками ризику.

Ключ (Key): відповідна кількість або послідовність символів, які використовуються для кодування та/або декодування інформації.

Компонент (Component): ідентифікована апаратна частина ЗВТ або вузла, яка виконує певну функцію або функції, і яку можна окремо оцінити відповідно до конкретних метрологічних і технічних вимог до характеристик.

Комунікаційний інтерфейс (Communication interface): частина приладу, яка забезпечує передачу інформації між ЗВТ, компонентами ЗВТ або іншими зовнішніми системами.

Конфіденційність (Confidentiality): власність, для якої інформація не надається або не розкривається неавторизовані особи, організації або процеси.

Криптографічні засоби (Cryptographic means): такі засоби, як шифрування та дешифрування з метою приховування інформації від неавторизованих осіб або хешів та електронних підписів забезпечити цілісність і автентичність.

Мітка часу (Time stamp): унікальне значення, наприклад, у секундах, або рядок дати та часу, що позначає дату та/або час, коли стався певний інцидент (наприклад, вимірювання чи подія).

Модуль (Module): програмний об'єкт, такий як програма, підпрограма, бібліотека, параметр або набір даних, тощо. ПЗ ЗВТ складається з одного або кількох модулів.

Неприпустимий вплив (Inadmissible influence)**:** такий вплив, що змінює ЗР дані або параметри недекларованим в технічній документації чином.

Операційна система (Operating System:): програмне забезпечення для керування роботою програми та надання послуг для розподілу ресурсів, планування завдань, керування введенням/виведенням і керування даними.

Перевірка програмного забезпечення (Software examination): технічна операція, яка полягає у визначенні однієї або кількох характеристик програмного забезпечення відповідно до певної процедури (наприклад, аналіз технічної документації або запуск програми в контрольованих умовах).

Перевірка (Verification): Надання об'єктивних доказів того, що даний елемент відповідає визначеним вимогам.

Передача вимірювальних даних (Transmission of measurement data): електронна передача вимірювальних даних через лінії зв'язку або інші засоби до приймача.

Пломбування (Sealing): засіб, призначений для захисту програмного забезпечення, параметрів, даних вимірювань, ЗВТ, компонента або програмного модуля від будь-якої модифікації, переналагодження, видалення компонентів або програмних модулів тощо.

Прийнятне рішення (Acceptable solution): конструкція або принцип програмного модуля чи апаратного компонента, або функції, які вважаються такими, що відповідають конкретній вимозі.

Пристрій зберігання (Storage device): пристрій, який використовується для зберігання даних вимірювання, необхідних для побудови результату вимірювання та/або збереження результату вимірювання доступним після завершення вимірювання для подальших ЗР цілей.

Програмний інтерфейс (Software interface): програмний код і спеціальний домен даних; отримання, фільтрація або передача даних між програмними модулями.

Розділення програмного забезпечення (Software separation): відокремлення програмного забезпечення в ЗВТ або компонентах, яке можна розділити на юридично релевантні програмні модулі та юридично не релевантні програмні модулі.

Спеціалізований ЗВТ (тип Р) (Built-for-purpose device (type P)): ЗВТ, створений для конкретного метрологічного завдання.

Спеціальний ЗВТ (Specific instrument): ЗВТ на який розповсюджується дія Технічного регламенту засобів вимірювальної техніки та Директиви вимірювальних приладів 2014/32/EU.

Суттєвий дефект (Significant defect): інцидент, який має небажаний вплив на відповідність ЗВТ або несправність. Приклади суттєвих дефектів включають: a) видалення контрольного сліду, b) неприпустимі зміни параметрів, c) неавторизовані оновлення та d) випадкові зміни програмного забезпечення через фізичні впливи.

Цілісність (Integrity): властивість того, що програмне забезпечення, дані вимірювань і параметри не змінилися.

Законодавчо релевантний (значущий) (Legally relevant): властивість обов'язкового виконання суттєвих вимог та/або вплив на відповідність суттєвим вимогам ТР.

5 Проведення випробувань програмного забезпечення

5.1 Вибір схеми проведення випробувань

5.1.1 Для ПЗ ЗВТ на які розповсюджується дія ТР2 застосовують процедури випробування Додатку Б відповідно до WELMEC 7.2:2023.

5.1.2 Для законодавчо регульованих (ЗР) ЗР ЗВТ на які розповсюджується дія ТР3 застосовують процедури випробування Додатку Г відповідно до ДСТУ OIML D 31:2018.

5.1.2.1 Для ПЗ ЗР ЗВТ на які розповсюджується дія ТР3 можливо застосовувати процедури Додатку Б на вимогу замовника або за доцільністю.

5.2 Жорсткість випробування ПЗ

5.2.1 Для кожного ЗВТ повинен бути визначено виробником клас ризику. Орган оцінки відповідності (ООВ) перевіряє правильність вибору класу ризику. Конкретні вимоги, що стосуються ПЗ, визначаються класом ризику, що характеризує ЗВТ. Клас ризику визначається можливою шкодою та наслідками, які можуть виникнути при використанні зіпсованого ПЗ або результатів вимірювань ЗВТ із зіпсованим ПЗ, та ймовірністю використання зіпсованого ПЗ.

5.2.2 Для протидії факторам ризику можливі наступні рівні захисту ПЗ, жорсткості випробування та відповідності ПЗ

Для відповідних рівнів використовуються такі визначення.

5.2.2.1 Рівні захисту програмного забезпечення

Низький: не потрібні спеціальні заходи захисту від навмисних змін.

Середній: ПЗ захищено від навмисних змін, внесених за допомогою легкодоступних і простих звичайних програмних засобів (наприклад, текстових редакторів).

Високий: ПЗ захищено від навмисних змін, внесених за допомогою складних програмних засобів (налагоджувачі та редактори жорстких дисків, засоби розробки програмного забезпечення тощо).

5.2.2.2 Рівні жорсткості випробування ПЗ

Низький: виконується перевірка стандартного типу, включаючи функціональне тестування приладу. Додаткове тестування ПЗ не потрібно.

Середній: Крім низького рівня, ПЗ перевіряється на основі його документації. Документація містить опис функцій ПЗ, опис параметрів тощо. Можна проводити практичні випробування функцій, що підтримуються ПЗ (вибіркові перевірки), щоб перевірити правдивість документації та ефективність заходів захисту.

Високий: на додаток до середнього рівня, проводиться поглиблене тестування ПЗ, зазвичай на основі вихідного коду.

5.2.2.3 Рівні відповідності ПЗ

Низький: ЮЗ ПЗ окремих приладів вважається таким, що відповідає ЮЗ ПЗ досліджуваного типу, якщо функціональність ПЗ відповідає технічній документації типу. Сам двійковий код ПЗ не обов'язково повинен бути ідентичним ПЗ цього типу.

Середній: на додаток до рівня відповідності «низький», двійковий код ЮЗ ПЗ окремих інструментів ідентичний ПЗ типу, що перевіряється (або повторно перевіряється). Розділення ПЗ відповідає вимогам.

Високий: двійковий код повного ПЗ, реалізованого в окремих приладах, ідентичний ПЗ досліджуваного типу. Розділення ПЗ не застосовують.

Можливі класи ризику та відповідні їм рівні захисту ПЗ, жорсткості випробувань та ступені відповідності, їх співвідношення для ДСТУ 7363:2013 та ДСТУ OIML D 31:2018 представлені в таблиці 1.

Таблиця 1 – Визначення класу ризику та рівнів жорсткості випробувань ПЗ ЗВТ

Клас ризику	***Рівень захисту ПЗ***	***Рівень жорсткості випробувань***	***Ступінь відповідності***	***Рівень жорсткості випробувань за ДСТУ 7363:2013***	***Відповідний рівень ДСТУ OIML D 31:2018***
A	*Низький*	*Низький*	*Низький*	*Низький*	*Низький*
B	*Середній*	*Середній*	*Низький*	*Середній*	
C	*Середній*	*Середній*	*Середній*		
D	*Високий*	*Середній*	*Середній*		
E	*Високий*	*Високий*	*Середній*	*Високий*	*Високий*
F	*Високий*	*Високий*	*Високий*		

5.2.3 Для спеціальних ЗВТ в рекомендаціях WELMEC 7.2:2023 застосовують класи ризику B, C, D.

5.2.4 Опис класів ризику, ступенів відповідності та жорсткості випробувань відповідно до рекомендацій WELMEC 7.2:2023 наведено в Додатку А

5.2.5 При виборі ***низького*** чи ***високого*** рівнів вимог та жорстокості випробувань відповідно до ДСТУ OIML D 31:2018 для ЗР ЗВТ на які розповсюджується дія ТРЗ необхідно враховувати сфери застосування (торгівля, прямі продажі населенню, охорона здоров'я, правоохоронні органи тощо) та можна враховувати наступні аспекти:

а) ризик шахрайства:

– наслідки та соціальний і суспільний вплив несправності;

– вартість оцінюваного товару;

– використовувана платформа (спеціальні або універсальні пристрої);

– контакт із джерелами потенційного шахрайства (залишений без нагляду пристрій самообслуговування).

б) необхідна відповідність:

– практичні можливості для галузі досягти встановленого рівня.

в) необхідна надійність:

– екологічні умови;

– наслідки та соціальний і суспільний вплив помилок.

г) мотивація шахрая.

д) можливість повторити вимірювання або перервати його.

5.3 Методи випробувань програмного забезпечення засобів вимірювальної техніки

5.3.1 Вибір і послідовність методів строго не визначені і можуть змінюватися в кожному конкретному випадку.

5.3.2 Рекомендовані методи випробувань ПЗ ЗВТ згідно ДСТУ OIML D 31 наведені в додатку В.

5.4 Висновки за результатами випробувань ПЗ

5.4.1 Так як обсяг робіт з випробувань ПЗ визначається рівнем жорсткості випробувань, не проводиться перевірка для рівня жорсткості більшого, ніж встановлено. Тому застосовується бінарне твердження для простого правила прийняття: невідповідність будь-якому додатку при випробуваннях вважається за невідповідність ПЗ встановленим вимогам.

5.5. Оформлення результатів випробування

Результати випробування оформляють протоколом випробувань ПЗ за формою, наведеною в додатку Д до цієї методики.

При цьому робиться висновок щодо відповідності, або не відповідності програмного забезпечення вимогам ТР.

ДОДАТОК А

Опис класів ризику відповідно WELMEC 7.2:2023

А.1 Клас ризику А:

Це найнижчий клас ризику. Перевірка програмного забезпечення є частиною функціонального тестування пристрою. Потрібна відповідність на рівні документації. (Не застосовується)

А.2 Клас ризику В:

Захист програмного забезпечення середній. Рівень жорсткості випробувань середній. Відповідність низька. Перевірка програмного забезпечення проводиться на основі документації.

А.3 Клас ризику С:

Рівень відповідності підвищено до «середнього». Це означає, що двійковий код законодавчо релевантного програмного забезпечення окремих інструментів ідентичний програмному забезпеченню досліджуваного типу. Рівні захисту та жорсткості випробувань середні.

А.4 Клас ризику D:

Рівень захисту ПЗ високий. Рівень жорсткості випробувань середній, тому необхідно надати достатньо інформативну документацію, щоб показати, що вжиті належні заходи захисту. Рівень відповідності середній.

А.5 Клас ризику Е:

Рівень жорсткості випробувань високий. Рівень захисту високий. Ступінь відповідності середній.

А.6 Клас ризику F:

Рівні захисту, жорстокості перевірки та відповідності високі. Всі складові ПЗ є законодавчо-значимими.

ДОДАТОК Б
Процедура випробування ПЗ ЗВТ згідно WELMEC 7.2 2023

Б.1 Вибір основної конфігурації

Б.1.1 Слід використовувати тільки один з двох наборів вимог для основних конфігурацій ЗВТ. Визначається, до якої основної конфігурації відноситься даний ЗВТ: до спеціалізованого ЗВТ (тип ***P***) або до ЗВТ, що (здебільшого) використовує універсальний комп'ютер (тип ***U***).

Б.1.2 Якщо на питання 1, 3, 4 таблиці Б.1 надано відповідь «так», а на питання 2 та 5 – відповідь «ні», такий ЗВТ відноситься до типу ***P,*** в усіх інших випадках – до типу ***U***.

Таблиця Б.1 - вибір типу (***U*** або ***P***) засобу вимірювальної техніки

№ зп	Питання	Відповідь (так або ні)	Обраний тип ЗВТ
1.	Пропоноване програмне забезпечення повністю створено для вимірювального завдання?		
2.	Якщо є програмне забезпечення загального призначення, чи доступне воно користувачеві?		
3.	Якщо користувач позбавлений доступу до операційної системи, чи можливо переключення операційної моди, яка не є об'єктом сфери законодавчо регульованої метрології?		
4.	Виконавчі програми і програмна оболонка є незмінними (крім оновлення)?		
5.	Чи є засоби програмування?		

Б.2 Вибір необхідних доповнень та спеціальних програмних вимог

Б.2.1 Конфігурації, що пропонуються інформаційними технологіями, містять в собі: довготривале зберігання ЗР даних (***L***), передачу таких даних (***T***), програмне розділення (***S***) та оновлення ПЗ в процесі експлуатації (***D***), операційна система (***O***). Відповідні набори вимог незалежні одне від одного.

Б.2.2 Застосування спеціальних програмних вимог вводиться для певних ЗВТ, на які розповсюджуються вимоги ТР2. Якщо ці вимоги до ПЗ присутні (***Ix***), то їх необхідно відповідним чином використовувати.

Б.2.3 Спеціальні програмні вимоги вводиться для лічильників води - ***I1***, лічильників та перетворювачів об'єму газу - ***I2***, лічильників активної електричної енергії - ***I3***, лічильників кількості теплоти - ***I4***, систем для безперервного та динамічного вимірювання об'єму рідин, крім води - ***I5***, автоматичних ваг - ***I6***, таксометрів - ***I7***, аналізаторів вихлопних газів – ***I10***).

Б.3 Вимоги до вбудованого в спеціалізовані ЗВТ програмного забезпечення (тип ***P***)

Б.3.1 Набір вимог, що наведено в цьому розділі, висувається до спеціалізованих ЗВТ з вбудованим ПЗ або до компоненту, який використовує те ж ПЗ.

Б.3.2 ЗВТ типу ***P*** являє собою ЗВТ з вбудованою інформаційно-технологічною системою (в загальному випадку це мікропроцесорна або мікроконтролерна система). Він характеризується наступними особливостями:

– все ПЗ розробляється для конкретної вимірювальної задачі, воно включає в себе як функції, що підлягають контролю, так і інші функції;

– інтерфейс користувача призначений для вимірювальних цілей, тобто в загальному режимі є предметом законодавчого контролю;

– відсутня ОС, що має оболонку, доступну користувачу (завантажувальні програми, передача команд ОС тощо);

– ПЗ та його оточення є незмінним, відсутні засоби для програмування або зміни його ЗР функцій;

– допускаються інтерфейси для передачі виміряних даних за допомогою відкритих та закритих мереж зв'язку;

– допускається зберігання виміряних даних на вбудованих, віддалених або переносних носіях.

Б.3.3 Спеціальні вимоги для ПЗ типу ***P***

Б.3.3.1 Ідентифікація ПЗ.

ЗР ПЗ повинно бути однозначно ідентифіковане. Ідентифікація повинна бути жорстко прив'язана до самої програми. Вона повинна бути представлена або у вигляді команди, або проявлятися протягом дії програми.

Додатково для СРВ документація повинна містити опис заходів, прийнятих для захисту програмної ідентифікації від фальсифікації.

Б.3.3.2 Вплив через інтерфейс користувача.

Команди, введені через інтерфейс користувача, не повинні надавати неприпустимий вплив на ЗР ПЗ і дані вимірювань. Команди можуть бути як поодинокими, так і у вигляді послідовності перемикань або клавішних маніпуляцій, що виконуються вручну. Для кожної команди повинно бути однозначне призначення для ініціювання функції або зміни даних. Перемикання або клавішні маніпуляції, що не декларовані і не документовані як команди, не повинні надавати впливу на функції ЗВТ і дані вимірювань.

Для СРВ документація повинна містити опис всіх команд, їх призначення і вплив на дані і функції ЗВТ.

Б.3.3.3 Вплив через комунікаційні інтерфейси.

Команди, що вводяться через комунікаційні інтерфейси ЗВТ, не повинні неприпустимим чином впливати на ЗР ПЗ, параметри ЗВТ та результати вимірювань.

Якщо прилад має інтерфейс, документація повинна містити:

– опис команд та їх вплив на ЗР ПЗ, специфічні параметри пристрою та дані вимірювань;

– опис того, як ЗР ПЗ, специфічні параметри пристрою та дані вимірювань захищені від впливу інших вхідних даних.

Б.3.3.4 Захист від випадкових або ненавмисних змін.

ЗР ПЗ, специфічні параметри пристрою та дані вимірювань повинні бути захищені від випадкових або ненавмисних змін.

Документація повинна показувати заходи, вжиті для захисту ПЗ від випадкових змін.

Б.3.3.5 Захист від навмисних змін.

ЗР ПЗ та дані вимірювань повинні бути захищені від неприпустимої навмисної модифікації, завантаження або заміни апаратної пам'яті.

Документація повинна гарантувати, що ЗР ПЗ не може бути модифіковано неприпустимим чином, опис заходів, вжитих для захисту від навмисних змін.

Б.3.3.6 Захист параметрів.

Специфічні параметри ЗВТ повинні бути захищені від неприпустимих змін.

У документації повинні бути описані специфічні параметри ЗВТ, чи можна їх налаштовувати, як вони налаштовуються та як вони захищені.

Б.3.3.7 Автентифікація даних вимірювань.

Повинна бути гарантована достовірність представлених даних вимірювань.

У документації має бути описано, як гарантується достовірність даних вимірювань.

Б.4 Вимоги до ПЗ ЗВТ, що використовують універсальний комп'ютер (тип ***U***)

Б.4.1 Набір вимог, що наведено в цьому розділі, висувається до ЗВТ, що використовують комп'ютер загального користування. З системою типу ***U*** мають справу тоді, коли умови реалізації ЗВТ типу ***P*** не виконуються.

Б.4.2 Технічний опис ЗВТ типу ***U***:

Апаратна конфігурація:

– система будується на комп'ютері загального користування, вона може складатись з одного комп'ютера, бути частиною закритої мережі (наприклад, кабельної), багатопроцесорної системи LAN, або частиною відкритої системи (наприклад, Інтернет);

– оскільки система є системою загального користування, то датчик повинен бути зовнішнім пристроєм по відношенню до комп'ютера і повинен бути зв'язаним з ним за допомогою закритої лінії зв'язку або захищеної лінії відкритого зв'язку (наприклад, мережа, за допомогою якої можуть бути зв'язані декілька датчиків);

– інтерфейс користувача може перемикатись від режиму функціонування, який не підлягає законодавчому регулюванню, до режиму, який є об'єктом контролю, і навпаки;

– зберігання виміряних даних може бути локалізованим (наприклад, на жорсткому диску) або віддаленими (наприклад, на сервері файлів, який може бути розташованим де завгодно), може бути фіксованим (наприклад, жорсткому диску) або переносним (наприклад, на дискетах, CD, DVD, флеш-накопичувачах).

Конфігурація ПЗ:

– може використовуватись будь яка ОС;

– в додаток до прикладної програми, що використовується для вимірювання, в системі одночасно можуть існувати інші програми;

– частина ПЗ, що відноситься до прикладної програми ЗВТ і є предметом законодавчого регулювання не може модифікуватись після затвердження типу, а частина ПЗ, що не є предметом контролю, може бути вільно модифікована;

– ОС та драйвери низького рівня (наприклад, відеодрайвери, драйвери принтера, драйвери накопичувача тощо) не підлягають законодавчому регулюванню, якщо вони спеціально не запрограмовані для виконання вимірювальних завдань.

Б.4.3 Спеціальні вимоги для ПЗ ЗВТ типу ***U***

Б.4.3.1 Ідентифікація ПЗ.

ЗР ПЗ повинно бути однозначно ідентифікованих. Ідентифікація повинна бути жорстко прив'язана до самої програми. Вона повинна бути представлена або у вигляді команди, або проявлятися протягом дії програми.

Ідентифікація не поширюється на ОС і драйвери низького рівня, наприклад, відеодрайвери, драйвери принтера, драйвери дисків тощо, але вона поширюється на драйвери, спеціально запрограмовані для виконання ЗР вимірювальних завдань. Драйвери (низького рівня), які визначені як значимі, повинні бути ідентифіковані.

Ідентифікація може застосовуватися для різних рівнів, наприклад, до програми в цілому, до модулів, функцій тощо.

Додатково для СРВ документація повинна містити опис заходів, прийнятих для захисту програмної ідентифікації від фальсифікації.

Б.4.3.2 Вплив через інтерфейс користувача.

Команди, введені через інтерфейс користувача, не повинні надавати неприпустимий вплив на ЗР ПЗ і дані вимірювань. Команди можуть бути як поодинокими, так і у вигляді послідовності перемикань або клавішних маніпуляцій, що виконуються вручну. Для кожної команди повинно бути однозначне призначення для ініціювання функції або зміни даних. Виробник повинен декларувати у своїй технічній документації весь перелік команд та способів їх введення, доводити із застосуванням апаратних чи програмних засобів про винятковість цих команд, забезпечити уникання реакції ПЗ на випадкову комбінацію перемикань або клавішних маніпуляцій.

Для СРВ документація повинна містити опис всіх команд, їх призначення і вплив на дані і функції ЗВТ.

Б.4.3.3 Вплив через комунікаційні інтерфейси.

Команди, що вводяться через комунікаційні інтерфейси ЗВТ, не повинні неприпустимим чином впливати на ЗР ПЗ, параметри ЗВТ та результати вимірювань.

Якщо прилад має інтерфейс, документація повинна містити:

– опис команд та їх вплив на ЗР ПЗ, специфічні параметри пристрою та дані вимірювань;

– опис того, як ЗР ПЗ, специфічні параметри пристрою та дані вимірювань захищені від впливу інших вхідних даних.

Б.4.3.4 Захист від випадкових або ненавмисних змін.

ЗР ПЗ повинно бути захищене від випадкових або ненавмисних змін.

Документація повинна показувати заходи, вжиті для захисту ПЗ від випадкових змін.

Б.4.3.5 Захист від навмисних змін.

ЗР ПЗ повинно бути захищене від несанкціонованої модифікації або оновлення.

Для СРВ документація повинна гарантувати, що ЗР ПЗ не може бути модифіковано неприпустимим чином, опис заходів, вжитих для захисту від навмисних змін.

Б.4.3.6 Захист параметрів.

Специфічні параметри ЗВТ повинні бути захищені від неприпустимих змін.

У документації повинні бути описані специфічні параметри ЗВТ, чи можна їх налаштовувати, як вони налаштовуються та як вони захищені.

Б.4.3.7 Автентифікація даних вимірювань.

Повинна бути гарантована достовірність представлених даних вимірювань.

У документації має бути описано, як гарантується достовірність даних вимірювань.

Б.4.3.8 Вплив іншого ПЗ.

ЗР ПЗ має бути розроблено таким чином, щоб інше ПЗ не впливало на нього неприпустимим чином.

Ця вимога передбачає поділ ПЗ на ЗР та ЗнР з огляду на найсучасніші розробки ПЗ для модульних або об'єктно-орієнтованих концепцій. Слід дотримуватися розширення S.

Б.5 Додаткові вимоги до ПЗ: довготривале збереження даних вимірювань (додаток ***L***)

Б.5.1 Набір вимог, що наведено в цьому розділі, висувається до ПЗ, вбудованого в ЗВТ цільового призначення (тип ***P***) та до ПЗ, що використовує універсальний комп'ютер (тип ***U***), якщо застосовується зберігання законодавчо значимих даних вимірювань.

Б.5.2 Технічний опис

Існує три різні конфігурації для накопичувачів тривалого зберігання:

– вбудований накопичувач ЗВТ цільового призначення, який є частиною ЗР ПЗ та апаратного забезпечення;

– накопичувач універсального комп'ютера, який може бути вилучений з приладу, також його вміст може бути скопійовано будь куди всередині комп'ютера або на віддалені сервери;

– з'ємні або віддалені накопичувачі (наприклад, дискети, зовнішні жорсткі диски, флеш-накопичувачі).

Б.5.3 Особливі вимоги додатку ***L***

Б.5.3.1 Повнота даних вимірювань, що зберігаються

ЗР дані (виміряні дані, параметри), що зберігаються, повинні містити всю значиму інформацію, необхідну для відновлення даних вимірювання. Вимірювальні дані, які зберігаються, можуть стати потрібними пізніше, наприклад, під час перевірки рахунків. Вся інформація для законодавчих та метрологічних потреб повинна зберігатися разом з даними вимірювання.

Документація повинна містити опис всіх масивів даних, що зберігаються.

Б.5.3.2 Захист від випадкових або ненавмисних дій

ЗР дані, що зберігаються, повинні бути захищені від випадкових та ненавмисних дій користувача або зовнішніх факторів.

Документація повинна демонструвати заходи, вжиті для захисту даних від випадкових дій.

Б.5.3.3 Захист від навмисних змін.

ЗР дані повинні бути захищені від несанкціонованої модифікації або видалення.

Документація повинна гарантувати, що ЗР дані не можуть бути модифіковані неприпустимим чином, опис заходів, вжитих для захисту від навмисних змін.

Б.5.3.4 Простежуваність збережених даних вимірювань.

Збережені дані вимірювання повинні мати простежуваність до вимірювання та ЗВТ, який їх згенерував. Достовірність передбачає ідентифікацію масиву даних.

Документація повинна містити опис методу, який забезпечує достовірність даних, що зберігаються.

Б.5.3.5 Конфіденційність ключів.

Ключі та пов'язана з ними інформація повинні розглядатися як дані вимірювань і зберігатися в таємниці та бути захищеними від компрометації.

Документація повинна містити опис управління таємною інформацією, засобів збереження ключів та іншої інформації в таємниці.

Б.5.3.6 Отримання, перевірка та індикація збережених даних вимірювань.

Має бути передбачене ЗР ПЗ для зчитування, перевірки та індикації збережених даних вимірювань. ПЗ, яке використовується для перевірки баз даних вимірювання, повинно відображати або роздруковувати ці дані, перевіряти їх на наявність змін, та попереджувати, якщо вони сталися. Дані, які були визначені як пошкоджені, не повинні використовуватися.

Документація повинна містити опис виявлення пошкоджених даних та функцій вилучення даних.

Б.5.3.7 Механізм збереження даних.

Дані вимірювань, в залежності від сфери застосування ЗВТ, повинні зберігатися автоматично або можуть зберігатися по команді користувача. Коли зберігання повинно відбуватися автоматично, функція збереження не повинна залежати від рішення користувача.

Якщо в процесі автоматичного або керованого збереження виникають виключні випадки, повинні існувати функції керування виключними випадками при збереженні даних.

Документація повинна містити опис механізму збереження даних, а також керування виключними випадками при збереженні даних.

Б.5.3.8 Ємність накопичувача.

Пристрій збереження повинен бути досить містким для забезпечення збереження даних за певний період часу. Коли пристрій збереження повністю заповнений або відключений від ЗВТ, користувачу повинен отримати попередження.

Документація повинна містити дані про ємність накопичувача, а також керування виключними випадками при збереженні даних.

Б.6 Додаткові вимоги до ПЗ: передача даних вимірювань через телекомунікаційні мережі (додаток ***T***)

В5.6.1 Набір вимог, що наведено в цьому розділі, висувається до ПЗ, вбудованого в ЗВТ цільового призначення (тип ***P***) та до ПЗ, що використовує універсальний комп'ютер (тип ***U***), якщо застосовується передача ЗР даних вимірювань.

Б.6.2 Технічний опис

Існує три конфігурації мереж передачі даних:

– *закрита мережа, повністю ЗР*, вона пов'язує тільки фіксовану кількість учасників (складових частин) з відомою ідентифікацією, функціональними можливостями та розташуванням; всі пристрої підлягають законодавчому контролю, в мережі відсутні пристрої, які не підлягають законодавчому контролю;

– *закрита мережа, частково ЗР*, вона пов'язує тільки фіксовану кількість учасників (складових частин) з відомою ідентифікацією, функціональними можливостями та розташуванням; не всі пристрої підлягають законодавчому контролю, їх функціональні можливості не завжди відомі;

– *відкрита мережа*, будь які учасники (пристрої з довільними функціями) можуть бути з'єднані такою мережею; ідентифікація і функціональні можливості та розташуванням можуть бути не відомі іншим учасникам мережі; бездротові мережі зв'язку (прилади з інфрачервоним зв'язком, Wi-Fi мережі) розглядаються як відкриті.

Б.6.3 Особливі вимоги додатку ***T***

Б.6.3.1 Повнота даних вимірювань, що передаються

ЗР дані (виміряні дані, команди), що передаються, повинні містити всю значиму інформацію, необхідну для її подання або для подальшої обробки результатів вимірювання в приймальному пристрої. Метрологічна частина переданих даних повинна включати одне або кілька значень вимірювання із заданою похибкою, законодавчо прийняту одиницю вимірювання і, в залежності від завдання, ціну поділки або шкалу та місце проведення вимірювання.

Документація повинна містити опис всіх масивів даних, що передаються.

Б.6.3.2 Захист від випадкових або ненавмисних дій

ЗР дані, що передаються, повинні бути захищені від випадкових та ненавмисних дій користувача або зовнішніх факторів.

Документація повинна демонструвати заходи, вжиті для захисту даних від випадкових дій.

Б.6.3.3 Захист від навмисних змін.

ЗР дані повинні бути захищені від навмисних дій.

Документація повинна гарантувати, що законодавчо значимі дані не можуть бути модифіковані неприпустимим чином, опис заходів, вжитих для захисту від навмисних змін.

Б.6.3.4 Простежуваність переданих даних вимірювань.

Для програм, які приймають відповідну інформацію, що передається, повинна існувати можливість перевірки автентичності та приписування даних вимірювання до певного вимірювання. У відкритій мережі необхідно ідентифікувати початкові дані вимірювання, які було передано без спотворень. В закритій мережі ніяких додаткових заходів не потрібно, якщо топологія мережі зафіксована шляхом опечатування.

Під час передачі можливі непередбачувані затримки. Для правильного приписування отриманих даних вимірювання до певного вимірювання необхідно реєструвати час вимірювання.

Документація повинна містити опис структури мережі, опис забезпечення достовірності даних, що передаються.

Б.6.3.5 Конфіденційність ключів.

Ключі та пов'язана з ними інформація повинні розглядатися як дані вимірювань і зберігатися в таємниці та бути захищеними від компрометації.

Документація повинна містити опис управління таємною інформацією, засобів збереження ключів та іншої інформації в таємниці.

Б.6.3.6 Отримання, перевірка та обробка переданих даних вимірювань.

Якщо є ЗР дані вимірювань, що передаються, повинен існувати відповідний компонент або модуль для отримання, перевірки та обробки переданих даних вимірювань.

Документація повинна містити опис виявлення пошкоджених даних та функцій вилучення даних.

Б.6.3.7 Затримка передачі.

Процес вимірювання не повинен залежати від недопустимого впливу затримки передачі. Виробник повинен гарантувати, що і в найгіршому випадку вимірювання не будуть піддаватися неприпустимому впливу.

Документація повинна містити опис механізму передачі даних, опис рішення захисту вимірювання від затримки передачі.

Б.6.3.8 Доступність послуг передачі.

Якщо послуги мережі передачі стануть недоступні, жодні дані вимірювань не повинні втрачатися. Користувач не повинен мати можливість спотворювати дані вимірювання через уповільнення або відмови функції передачі. Не можуть бути виключені

випадкові порушення передачі, засоби передачі даних повинні мати можливість врегулювання таких ситуацій.

Документація повинна містити опис механізму передачі даних, опис захисних заходів від переривання передачі та інших відмов системи.

Б.7 Додаткові вимоги до ПЗ: розділення ПЗ (додаток ***S***)

Б.7.1 Розділення ПЗ є не обов'язковим доповненням, яке дозволяє легко модифікувати ЗнР ПЗ. Якщо розділення ПЗ проведено, то цей додаток повинен розглядатись як доповнення до основних вимог до ЗВТ типу ***P*** та типу ***U***.

Б.7.2 Особливі вимоги додатку ***S***

Б.7.2.1 Реалізація програмного розділення

Повинна існувати частина ПЗ, що містить ЗР ПЗ та параметри, які чітко відокремлені від інших частин ПЗ.

До ЗР ПЗ відносяться всі частини ПЗ (програмні блоки, процедури, функції, класи, програми, бібліотеки тощо), які:

– беруть участь в розрахунках значень вимірювань або впливають на них,

– беруть участь у допоміжних функціях таких, як відображення даних, їх захист і збереження, ідентифікація ПЗ, здійснення його завантаження та оновлення, передача даних і збереження, перевірка прийнятих або збережених даних тощо.

Всі змінні, тимчасові файли та параметри, які впливають на величину вимірювання або на ЗР функції або інформацію, відносяться до ЗР ПЗ. Компоненти захищеного програмного інтерфейсу є частиною ЗР ПЗ.

ЗР ПЗ (або його частини) повинне мати чітку ідентифікацію (Пп. Б.3.3.1, Пп. Б.4.3.1). ЗнР ПЗ включає в себе програмні одиниці, дані або параметри, які не вказані вище.

Документація повинна містити опис всіх компонентів, що відносяться до ЗР та ЗнР ПЗ, обґрунтування розділення.

Б.7.2.2 Реалізація змішаної індикації

Додаткова інформація, створена ЗнР ПЗ, може бути показана на дисплеї або виводитися для роздрукування лише у випадку, якщо її не можна переплутати з інформацією, яка надається ЗР частиною. Виробник повинен гарантувати, що вся інформація, яка відображається, відповідає необхідним вимогам.

Документація повинна містити опис функцій, що реалізують індикацію та опис того, яким чином забезпечується індикація ЗР та ЗнР інформації.

Б.7.2.3 Захищений інтерфейс ПЗ

Обмін інформацією між ЗР та ЗнР частинами ПЗ повинен відбуватися через захисний програмний інтерфейс, який включає взаємодію та обмін даними.

Всі взаємодії і потоки даних не повинні надавати неприпустимий вплив на ЗР ПЗ, включаючи динамічний характер вимірювального процесу. Повинно існувати однозначне призначення кожного набору команд, переданих через інтерфейс ПЗ, для початкової функції або зміни даних в законодавчо значимому ПЗ. Коди і дані, що не декларовані і не документовані як команди, не повинні чинити жодного ефекту на ЗР ПЗ.

Документація повинна містити опис інтерфейсу ПЗ, повний список команд разом з декларацією про їх повноту, короткий опис їх призначення та вплив на функції ЗВТ. В документації повинна бути показана реалізація захищеного інтерфейсу ПЗ.

Б.8 Додаткові вимоги до ПЗ: завантаження ЗР ПЗ (додаток ***D***)

Б.8.1 Цей додаток використовується за наявності можливості завантаження ПЗ (наприклад, для обновлення) ЗВТ типу ***P*** та типу ***U***.

Б.8.2 Особливі вимоги додатку ***D***

Б.8.2.1 Механізм оновлення

Завантаження і подальше оновлення ПЗ повинні бути автоматичними і повинні гарантувати, що захист ПЗ знаходиться на затвердженому рівні.

ЗВТ повинен бути здатним визначати неможливість виконання завантаження або оновлення. Повинно надаватися попередження. Якщо завантаження або оновлення невдалі або перериваються, ПЗ повинне залишитися незмінним. Якщо при оновленні виникла помилка і ПЗ змінилося, ЗВТ повинен блокувати можливість проведення вимірювань до усунення помилки.

Кількість спроб повторення оновлення в разі помилки повинна бути обмежена.

В процесі оновлення вимірювання повинні припинятися або повинна бути гарантована коректність вимірювань.

В разі розділення ПЗ (П. 5.7), вимоги стосуються лише ЗР частини.

Документація повинна містити опис реалізації механізму завантаження та оновлення, опис заходів при невдалі спробі завантаження чи оновлення ЗР частини ПЗ.

Б.8.2.2 Автентичність завантаженого оновлення ПЗ

До завантаження оновлення ПЗ повинно автоматично перевірятися, що:

– оновлення ПЗ є автентичним (має унікальну ідентифікацію і дані, що вказують на походження оновлення);

– оновлення ПЗ є затвердженим для даного типу ЗВТ.

Засоби, з допомогою яких ідентифікується статус затвердження ПЗ уповноваженим органом, повинні бути захищені для запобігання підробки цього статусу.

Документація повинна містити опис того, як гарантується ідентифікація автентичності оновлення, автентичність затвердження уповноваженого органу. В документації повинна бути відображена реалізація автентичності оновлень ПЗ.

Б.8.2.3 Цілісність завантаженого оновлення ПЗ

Повинні бути застосовані заходи, які гарантують ~~те~~, що завантажене оновлення ПЗ протягом завантаження не змінюється неприпустимим чином.

Документація повинна містити опис того, як гарантується цілісність завантаженого оновлення ПЗ. В документації повинні бути показані гарантії цілісності.

Б.8.2.4 Простежуваність оновлень ЗР ПЗ

Повинна бути гарантія того, що оновлення ЗР ПЗ є придатним для подальшого контролю. Засоби запису та простежування є частиною ЗР ПЗ та повинні бути захищені в цій якості.

Документація повинна містити опис того, як засоби простежуваності впроваджуються та захищаються, як оновлення ПЗ може бути простежене. В документації повинні бути показані гарантії простежуваності.

Б.9 Додаткові вимоги до ПЗ: Операційні системи загального призначення (додаток ***O***)

Б.9.1 Вимоги додатку застосовуються, лише якщо операційна система вимірювального приладу є ЗР, тобто операційна система використовується для виконання основних вимог MID. Вимоги є доповненням до спеціальних вимог до програмного забезпечення для ЗВТ, що використовують універсальний пристрій (типу U). Ці вимоги не повинні застосовуватися до ЗВТ типу P.

Б.9.2 Технічний опис

Програмне забезпечення описується як операційна система загального призначення, якщо системні ресурси ЗВТ (ЦП, пам'ять, інтерфейси) управляються цим програмним забезпеченням і стають доступними для ЗР ПЗ. Крім того, операційна система має багатокористувацький доступ і режим адміністрування (багатокористувацька операційна система). Будь-яка операційна система загального призначення, оцінена згідно з цим додатком, повинна відповідати таким вимогам:

– повинна бути перевірена у використанні,

– повинна бути придатною для загального призначення,

– повинна бути найсучаснішою, до якої застосовано виправлення всіх відомих

помилок та вразливостей,

– не повинна бути розроблена виробником ЗВТ. Однак виробник ЗВТ може зробити внесок в ОС щодо драйверів або модулів, що виконують ЗР функції та мають ідентифікацію та захист. У цьому випадку перевірку програмного забезпечення операційної системи загального призначення можна звести до перевірки ЮЗ конфігурації на основі вимог додатка ***О***.

Б.9.3 Особливі вимоги додатку ***О***

Б.9.3.1 Обладнання

Апаратна частина, на якій працює ЗР ОС, повинна бути захищена від несанкціонованого доступу. ЗР ОС має бути захищена від видалення або обміну. Апаратні інтерфейси, які можуть впливати на ОС, мають бути або відключені від джерела живлення, відключені ОС, захищені апаратною пломбою або прив'язані до захисного програмного інтерфейсу. Інтерфейси з прямим доступом до пам'яті мають бути захищені апаратною пломбою. Операційна система повинна використовувати захист пам'яті, щоб запобігти вилученню конфіденційного криптографічного матеріалу.

Документація повинна містити:

– список усіх компонентів з операційною системою;

– опис заходів безпеки для масових сховищ;

– опис заходів захисту апаратних інтерфейсів.

У разі використання криптографічного матеріалу документація повинна містити опис захисних заходів для енергонезалежної пам'яті та пристроїв зберігання (для класів ризику D, E).

Б.9.3.2 Процес завантаження

Процес завантаження операційної системи має бути однозначним і відтворюваним. ЗР ПЗ включається в процедуру запуску універсального пристрою. Конфігурація завантаження має бути захищена від змін. Завантаження через відкриті інтерфейси заборонено. Процес завантаження повинен бути забезпечений відповідними засобами, залежно від рівня захисту.

Документація повинна містити:

– інформацію щодо конфігурації завантаження операційної системи (наприклад, накопичувач, розділи, параметри ядра);

– опис захисних заходів для процесу завантаження;

– опис середовища завантаження ОС ЗР ПЗ.

Б.9.3.3 Системні ресурси

Конфігурація операційної системи повинна забезпечувати наявність достатніх

ресурсів для роботи ЗР ПЗ. Ресурси ЗР ПЗ не зменшуються нижче необхідного мінімуму іншим програмним забезпеченням ЗР ПЗ та ЗнР ПЗ.

Документація повинна містити:

Інформацію щодо конфігурації встановлених частин операційної системи.

Інформація про поточні процеси під час використання вимірювального приладу.

5.9.3.4 Захист під час використання

Операційна система повинна бути налаштована таким чином, щоб функції операційної системи або інше програмне забезпечення не могли неприпустимо вплинути на ЗР ПЗ. Режими адміністрування ЗР ПЗ (ПЗ та ОС) мають бути захищені. Контроль доступу повинен бути налаштований таким чином, щоб не можна було неприпустимо вплинути на використання за призначенням. Дозволи на доступ повинні регулярно перевірятися ЗР ОС. ОС повинна бути налаштована так, щоб запобігти видаленню ЗР ПЗ. Підключення допоміжних пристроїв не повинно мати неприпустимого впливу на ОС або налаштування конфігурації.

Документація повинна містити:

– список використовуваних носіїв даних з їхніми атрибутами та правилами обмеження їх використання;

– опис адміністрування контролю доступу користувача та захисту облікового запису адміністратора;

– опис режиму роботи графічного інтерфейсу користувача;

– опис підключення допоміжних пристроїв.

Б.9.3.5 Захищені інтерфейси

Функції операційної системи, доступні через відкриті інтерфейси, не повинні неприпустимим чином впливати на ЗР ПЗ. Зв'язок із ЗР ОС здійснюється через захищені інтерфейси. У разі розділення програмного забезпечення в операційній системі, вимоги додатку ***S*** і додатку ***T*** до відкритих мереж застосовуються для передачі ЗР даних через програмні інтерфейси операційної системи. Якщо конфігурація ОС гарантує, що комунікаційний партнер, підключений до відкритого інтерфейсу, може бути лише сертифікованим компонентом і з'єднання захищене, подальша перевірка інтерфейсу не потрібна.

Документація повинна містити:

– опис конфігурації ОС для відкритого апаратного та програмного інтерфейсів;

– список відкритих апаратних і програмних інтерфейсів, неналаштовуваних ОС;

– список усіх прийнятих команд та їх вплив на всі відкриті інтерфейси, якими керує ОС.

Б.9.3.6 Ідентифікація ОС та її конфігурації

ОС та конфігурація ОС повинні бути ідентифікованими. Ідентифікація ОС та ідентифікація конфігурації ОС повинні бути представлені за командою або під час роботи. Якщо ЗР функції та обліковий запис вимірювального завдання захищені конкретною конфігурацією ОС, відповідні файли конфігурації повинні мати власний ідентифікатор. Ідентифікація включає в себе драйвери та модулі ОС, які були модифіковані або спеціально запрограмовані для ЗР завдання.

Документація повинна містити:

– загальна інформація про ОС (виробник, розповсюдження, назва продукту, версія ядра).

Інформація щодо ідентифікації тих частин ОС, налаштованих для ЗР завдання.

Інформація щодо ідентифікації модифікованих або доданих частин ОС, розроблених власними силами, для ЗР завдання (модулі ядра, драйвери, бібліотеки)

Перелік усіх використаних ідентифікаторів, а також опис того, як вони створюються, їх індикація та як відрізнити їх від ЗнР ідентифікаторів.

Б.9.3.7 Захист операційної системи

Операційна система має бути захищена таким чином, щоб були доступні докази втручання. Драйвери або модулі, які спеціально запрограмовані для ЗР завдань, повинні мати власний захист. Захист ОС повністю охоплює усі ЗР частини. Якщо використовується контрольна сума або еквівалентний показник цілісності, їх слід обчислювати за допомогою операційної системи. Розрахована контрольна сума повинна вказуватися операційною системою ЗР ПЗ. Цілісність ЗР ОС періодично перевіряється . Якщо перевірка цілісності не вдається, необхідні відповідні реакції. Ця вимога не стосується оновлень ЗР частин ОС. Такі оновлення належать до розширення D. Контрольна сума повинна бути отримана криптографічно стійкими методами.

Документація повинна містити:

– документація захисних заходів ОС;

– опис методів створення та індикації міри цілісності;

– вичерпний перелік ЗР частин ОС;

– список усіх частин ОС, на які поширюється міра цілісності.

Б.10 Спеціальні вимоги до ПЗ ЗВТ (додаток ***I***)

Б.10.1 Цей додаток використовується як доповнення до загальних вимог до ПЗ, що розглядаються в додатках ***P*** або ***U*** та додаткових вимог додатків ***L***, ***T***, ***S***, ***D*** і окремо від них розглядатись не може.

Б.10.2 Спеціальні вимоги формуються на основі додатків Measuring Instruments Directive 2014/32/EU, що містять спеціальні аспекти та вимоги для ЗВТ або систем (підсистем), в залежності від сфери застосування.

Б.10.3 Спеціальні вимоги додатку ***I***

Б.10.3.1 Виявлення (*I6-1*) та усунення несправності (*I1-1*, *I2-1*, *I3-1*, *I4-1*, *I5-1*)

ПЗ повинно виявляти, що нормальна обробка порушена, відновлювати нормальне функціонування в разі порушення нормальної обробки. Кожен факт збою повинен реєструватися в журналі подій з відміткою дати та часу.

Документація повинна містити опис механізму виявлення порушень обробки та відновлення від збоїв, коли вони виникають.

Б.10.3.2 ЗнР ПЗ та динамічна поведінка (*I1-2*, *I2-2*, *I3-2*, *I4-2*, *I5-2*)

ЗнР ПЗ не повинно негативно впливати на динамічну поведінку процесу вимірювання.

Виробник повинен гарантувати, що при застосуванні лічильника в реальному часі динамічна поведінка ЗР ПЗ не зазнає неприпустимого впливу ЗнР ПЗ, тобто ресурси ЗР ПЗ не будуть неприпустимо зменшені через ЗнР частину.

Документація повинна містити опис динамічної поведінки процесу вимірювання.

Б.10.3.3 Додаткові функції (*I1-3*, *I2-4*, *I3-3*, *I4-3*, *I5-3*)

Додаткові функції, наприклад, передоплата або інтервальне вимірювання, не повинні впливати на ЗР вимірювальні функції.

Відповідність вимозі перевіряється в разі розділення ПЗ на ЗР та ЗнР частини при роботі з додатком ***S***.

Б.10.3.4 Засоби резервування (*I1-4*, *I2-3*, *I3-4*, *I4-4*, *I5-4*, *I6-2*, *I7-1*)

Може застосовуватися засіб, що забезпечує періодичне дублювання даних вимірювання та станів ЗВТ в енергонезалежній пам'яті на випадок порушень в роботі ЗВТ. Мінімальний інтервал збереження повинен бути розрахованим таким чином, щоб розбіжність між поточними і накопиченими даними резервування була некритичною.

Документація повинна містити опис того, які дані дублюються і коли це відбувається.

Б.10.3.5 Завантаження ПЗ (*I1-5*, *I2-5*, *I3-5*, *I4-5*, *I5-5*)

Під час оновлення ПЗ процес вимірювання не повинен бути припинено більше, ніж на одну хвилину в цілому. Якщо оновлення ПЗ займає більше часу, необхідно вжити додаткових заходів (наприклад, оновлення проводити при мінімальному споживанні енергоресурсу, призупиненні вимірювань).

Документація повинна містити опис механізму оновлення ПЗ.

Відповідність вимозі перевіряється в разі можливості оновлення ПЗ при роботі з додатком ***D***.

Б.10.3.6 Заборона скидання сукупних значень вимірювань (*I1-6*, *I2-6*, *I3-6*, *I4-6*)

Для комунальних ЗВТ накопичені значення вимірювань, що використовуються для розрахунків, не повинні бути скинуті під час експлуатації.

Документація повинна містити опис механізму захисту регістрів накопичення ЗВТ.

Б.10.3.7 Зчитування результатів вимірювання (*I1-7*, *I2-7*, *I3-7*, *I4-7*)

Результати вимірювань, які служать основою для оплати, можуть бути зчитані дистанційно, періодично або через інтерфейс користувача.

Документація повинна містити опис механізму зчитування результатів вимірювання.

Б.10.3.8 Захист від навмисних змін лічильників з механічним лічильником (*I1-8*, *I2-8*, *I3-8*, *I4-8*), друкований ідентифікатор ПЗ (*I5-6*)

Якщо неможливе відображення ідентифікатору ПЗ на інтерфейсі користувача, відбиток контрольної суми або альтернативна індикація ідентифікатору ПЗ на заводській таблиці приладу є прийнятним, якщо виконуються всі умови:

– інтерфейс користувача не має можливості керування для активації значення контрольної суми, або дисплей технічно не дозволяє відображати ці значення;

– прилад не має жодного інтерфейсу для передачі ідентифікатора ПЗ;

– після виготовлення лічильника зміна ПЗ неможлива або можлива за умови зміни апаратної частини, яка містить ПЗ.

Документація повинна містити опис механізму відображення ідентифікатору ПЗ.

Відповідність вимозі перевіряється при роботі з додатком ***P*** (*I6*).

Б.10.3.9 Кількість розрядів (*I1-9*, *I2-9*, *I3-9*, *I4-9*)

Дисплей загальної кількості виміряних значень повинен мати достатню кількість розрядів.

Для лічильників води, в залежності від постійної витрати, мінімальний діапазон індикації повинен відображати спожитий об'єм не менше ніж за 1587 годин безперервної роботи за максимальної витрати. Мінімальна кількість розрядів – 4. Крім того, поділка шкали повинна бути достатньо малою, щоб гарантувати, що похибка роздільної здатності не перевищувала 0,25 % для вимірювачів класу 1 та 0,5 % для класу точності 2 для об'єму, що пройшов за 90 хвилин за мінімальної швидкості потоку.

Лічильники газу повинні мати можливість зберігати та відображати дані вимірювань протягом 8000 годин за максимального значення витрати, що може бути зареєстроване лічильником.

Лічильники електричної енергії повинні мати можливість зберігати та відображати дані вимірювань протягом 4000 годин при повному навантаженні (максимальний струм при номінальному значенні напруги і коефіцієнті потужності 1).

Теплолічильники повинні мати можливість зберігати та відображати дані вимірювань протягом 3000 годин при верхній межі теплової потужності. Кількість теплоти, виміряна теплолічильником, що працює на верхній межі теплової потужності протягом 1 години, повинна відповідати принаймні одному значенню найменшого розряду індикації.

Б.10.3.10 Тест дисплею (*И1-10*, *И3-10*)

Для перевірки правильності функціонування всіх сегментів електронного дисплею повинна існувати можливість виконання тесту дисплею. Кожен крок перевірки повинен тривати щонайменше 1 с.

Документація повинна містити опис проведення перевірки дисплею.

Б.10.3.11 Термін служби джерела живлення (*И2-10*)

У відповідного джерела живлення період експлуатації повинен бути щонайменше п'ять років. Після закінчення 90% даного періоду повинно бути зроблено попередження. При заміні джерела живлення не повинно відбуватися ніяких порушень збережених ЗР даних та параметрів.

Документація повинна містити дані щодо внутрішнього джерела живлення (в тому числі максимальний термін служби), заходи щодо визначення рівня спожитої або доступної для споживання енергії, опис заходів щодо попередження низької кількості енергії, доступної для споживання.

Б.10.3.12 Тестовий елемент (*И2-11*)

Газовий лічильник повинен мати тестовий елемент, який може проводити тестування протягом резонного строку. Протягом періоду тестування процес вимірювання повинен виконуватися як за умов звичайного режиму експлуатації.

Документація повинна містити опис тестового елементу та інструкцію для активації режиму тестування.

Б.10.3.13 Електронний пристрій перетворення (*И2-12*)

Електронний пристрій перетворення об'єму повинен мати функцію виявлення, якщо він експлуатується за межами діапазону, встановленого виробником, для параметрів, які стосуються точності вимірювань. В такому випадку пристрій перетворення повинен зупинити обробку перетворених величин та повинен окремо підрахувати перетворені величин для того проміжку часу, коли він експлуатувався за межами робочого діапазону. Повинно існувати відображення ознак несправного стану та реєстрація в журналі подій.

Документація повинна містити опис різних реєстрів для перетворених величин та несправного стану.

Б.10.3.14 Перерахунок коефіцієнту перетворення (*I2-13*)

В електронних пристроях для перетворення об'єму газу коефіцієнт повинен перераховуватися з інтервалами, що не перевищують 1 хв. для пристрою перетворення температури, та з інтервалами, що не перевищують 30 с для інших типів перетворення об'єму газу.

Однак, якщо сигнал об'єму не отримано від лічильника газу за вказаний час, перерахунок не повинен проводитися до отримання наступного сигналу.

Б.10.3.15 Налаштування параметрів (*I5-7*)

З метою перевірки повинна бути можливість відобразити або надрукувати поточні налаштування параметрів, які фіксують ЗР характеристики ЗВТ. Параметри мають бути захищені (див. *P7 / U7*).

Документація повинна містити опис механізму перевірки параметрів.

Б.10.3.16 Допоміжні та додаткові пристрої (*I5-8*)

Якщо допоміжний / додатковий пристрій, що містить ЗР ПЗ, є частиною ЗВТ, який можна від'єднати, повинен застосовуватися додаток ***T***.

Б.10.3.17 Тривале зберігання (*I7-2*)

Повинно існувати пристосування, яке автоматично зберігає сумарні значення у разі відключення від джерела живлення.

Документація повинна містити короткий опис того, які дані зберігаються та коли це відбувається.

Б.10.3.18 Захист від навмисного втручання (*I7-3*)

Повинно існувати пристосування, яке перевіряє достовірність сигналів вимірювання відстані.

Документація повинна містити короткий опис того, як підпрограми перевіряють достовірність.

Б.11 Висновки за результатами випробувань ПЗ

Б.11.1 Так як обсяг робіт з випробувань ПЗ визначається рівнем жорсткості випробувань, не проводиться перевірка для рівня жорсткості більшого, ніж встановлено. Тому застосовується бінарне твердження для простого правила прийняття: невідповідність будь-якому додатку при випробуваннях вважається невідповідністю ПЗ встановленим вимогам. Виключенням є НРВ для класу ризику "А", оскільки для нього допускається найменша можлива ступінь відповідності.

ДОДАТОК В

Основні методи випробування ПЗ ЗВТ

В.1 В таблиці В.1 представлено рекомендовані OIML D 31:2008 методи випробування ПЗ ЗВТ, їх позначення, опис, умови застосування, необхідні інструменти та навички

Таблиця В.1 - Основні методи випробування ПЗ ЗВТ

Скоро-чення	Опис	Застосування	Передумови, інструменти для застосування	Спеціальні навички для виконання
1	2	3	4	5
AD	Аналіз документації та перевірка правильності проекту	Завжди	Документація	–
VFTM	Перевірка функціональним тестуванням метрологічних функцій	Коректність алгоритмів; невизначеності, компенсуючі і коригувальні алгоритми, правила для обчислення цін	Документація	–
VFTSw	Перевірка функціональним тестуванням програмних функцій	Правильне функціонування комунікації, індикації, захисту від шахрайства, захист від операційних помилок, захист параметрів, виявлення несправностей	Документація, загальні (не спеціальні) програмні інструменти	–
DFA	Аналіз потоку метрологічних даних	програмне розділення, оцінка впливу команд на функції ЗВТ	Вихідний код, загальні (не спеціальне) програмні інструменти (проста процедура), спеціальні	Знання мов програмування, необхідні інструкції для проведення даного методу перевірки

1	2	3	4	5
			програмні засоби (складна процедура)	
CIWT	Перевірка коду і наскрізний контроль	Для всіх цілей	Вихідний код, загальні (не спеціальні) програмні інструменти	Знання мов програмування, протоколів, і інших аспектів у сфері ІТ
SMT	Тестування програмних модулів	Для всіх цілей, коли вхід і вихід можуть бути чітко визначені	Вихідний код, середовище для тестування, спеціальні програмні засоби	Знання мов програмування, протоколів, і інших аспектів у сфері ІТ, необхідні інструкції для проведення перевірки

В.2 Опис процедур методів

В.2.1 Аналіз документації та перевірка правильності проекту (AD)

Це основна процедура, яка повинна застосовуватися в будь-якому випадку, базується на документації виробника ЗВТ.

Експерт оцінює функції і особливості ЗВТ і вирішує питання про відповідність ЗВТ встановленим вимогам, використовуючи вербальний опис і графічне представлення. Повинні розглядатися і оцінюватися метрологічні і програмно-функціональні вимоги (ідентифікація і програмне розділення, захист від несанкціонованих змін, вимоги до оновлення ПЗ та ін.).

Основні процедури, що виконуються при перевірці документації:

В.2.1.1 Перевірка ідентифікації ПЗ

Залежно від вимог у документації повинні бути зазначені:

- ідентифікація (версія) ПЗ і опис того, як ідентифікація здійснюється;

- опис того, яким чином ідентифікація пов'язана з ПЗ, структура ідентифікації;

- яким чином користувач може отримати доступ до ідентифікації;

- як за структурою ідентифікаційного номера можна розрізняти зміни версії ПЗ, при яких потрібно або не потрібно проведення додаткових робіт з випробування ПЗ;

- в документації повинні бути описані заходи, прийняті для захисту ідентифікації ПЗ від фальсифікації.

В.2.1.2 Перевірка повноти наданої документації

Вся документація, що описує ЗВТ, повинна перевірятися на повноту.

Залежно від вимог документація, що додається до ЗВТ, повинна містити:

- інструкцію з експлуатації;

- однозначну ідентифікацію ПЗ;

- опис всіх характеристик і властивостей ЗВТ;

- опис ПЗ ЗВТ (опис законодавчо-контрольованих функцій, параметрів, комутаторів і ключів);

- опис точності алгоритмів вимірювання (наприклад, алгоритми розрахунку і округлення цін);

- опис інтерфейсу користувача, меню і діалогів користувача;

- огляд застосованих заходів захисту ПЗ від несанкціонованих вимірювань, захисту облікових записів користувачів та ін.

В.2.1.3 Вивчення керівництва по експлуатації та технічної документації

Залежно від вимог, керівництво з експлуатації та технічна документація повинні містити:

- огляд ПЗ і пояснення загальної логіки структури ПЗ;

- докладний опис всіх функцій ПЗ ЗВТ;

- докладний опис всіх параметрів, що визначають функціональні можливості ЗВТ;

- опис алгоритму вимірювання;

- опис меню і опис діалогів під час роботи з меню.

Всі функції, які описуються в документації на ЗВТ, повинні бути визначені і зрозумілі.

Всі характеристики ЗВТ повинні відповідати документованим і всі вимоги, що містяться в документації, повинні бути виконані.

В ході проведення даної процедури можуть виявлятися помилки в законодавчо-контрольованих функціях, описаних в керівництві з експлуатації і в технічній документації на ЗВТ.

В.2.1.4 Перевірка специфікації:

а) проводиться перевірка специфікації:

- специфікації зовні доступних функцій ЗВТ в загальному вигляді (якщо не має будь-яких інтерфейсів, крім дисплея, всі властивості можуть бути перевірені методом функціонального тестування, малий ризик шахрайства);

- специфікації функцій ЗВТ та інтерфейсів (необхідна для ЗВТ з інтерфейсами і для функцій ПЗ, які не можуть пройти функціональну перевірку, а також якщо існує підвищений ризик шахрайства)

б) документація повинна включати повний список команд або сигналів, які ПЗ здатне обробляти, а також опис того, як ЗВТ реагує на документовані і недокументовані команди.

в) при проведенні випробувань ПЗ може знадобитися додаткова документація на ПЗ з описом складних вимірювальних алгоритмів, криптографічних функцій, критичних тимчасових обмежень тощо; в цьому випадку розробник ПЗ зобов'язаний надати відповідну документацію.

В результаті проведення процедури оцінюються всі характеристики ЗВТ, якщо відповідна документація була надана на розгляд виробником ЗВТ.

В.2.3 Методи на основі функціональної перевірки

В.2.3.1 Перевірка функціональним тестуванням метрологічних функцій (VFTM).

Застосовується для визначення коректності алгоритмів, використовуваних для обробки даних, для компенсації впливу робочого середовища на ЗВТ, лінеаризації характеристики, визначення величини округлення при обчисленні ціни тощо.

Для проведення процедури необхідні: керівництво з експлуатації, функціонуючий зразок ЗВТ, метрологічні референції (еталони), випробувальне обладнання.

Більшість методів проведення випробувань, описаних у рекомендаціях OIML, ґрунтуються на стандартних вимірюваннях за різних умов. Конструкція ЗВТ не накладає обмеження на можливість проведення перевірки цього ЗВТ з використанням еталонів.

Незважаючи на те, що проведення таких випробувань не спрямоване в першу чергу на перевірку ПЗ, результат тесту можна інтерпретувати як перевірку деяких модулів програмного забезпечення, загалом навіть найважливіших з метрологічної точки зору. Якщо випробування, описані у відповідній Рекомендації, охоплюють усі метрологічно значимі характеристики приладу, відповідне ПЗ можна вважати верифікованим. Загалом, для перевірки метрологічних характеристик ЗВТ не потрібно застосовувати додатковий аналіз ПЗ чи тестування.

В результаті перевірки метрологічних функцій ПЗ ЗВТ методом функціонального тестування визначається коректність застосовуваних алгоритмів обробки даних, а також знаходження результатів вимірювань в межах максимально допустимої похибки.

В.2.3.2 Перевірка функціональним тестуванням програмних функцій (VFTSw)

Для проведення процедури необхідні:

- Інструкція з експлуатації;
- документація на ПЗ;
- функціонуючий зразок ЗВТ;
- обладнання для проведення тестування.

Мета: виявлення помилок в законодавчо значущих функціях ЗВТ.

Опис: під час проведення тестів визначається, чи відповідають реальні характеристики ЗВТ тим, що були вказані в документації (перевіряється захищеність ЗВТ від змін, правильність програмної ідентифікації, функція виявлення несправностей за допомогою ПЗ, конфігурація системи тощо).

На вхід ЗВТ подаються дані (параметри даних повинні відповідати специфікації), потім перевіряється реакція ПЗ на ці дані і порівнюється з описом, наведеним в специфікації. Якщо реакція ПЗ на введені дані не відповідає наведеній в специфікації або виявляється неповнота специфікації, всі відхилення реєструються і заносяться до протоколу результатів випробувань.

Всі законодавчо значущі функції ЗВТ повинні бути перевірені.

Якщо деякі характеристики ЗВТ є програмно-контрольованими і вони функціонують правильно, то можуть вважатися підтвердженими без подальшого аналізу ПЗ.

До властивостей ЗВТ, які можуть бути перевірені при функціональному тестуванні, відносяться, наприклад:

- можливість візуалізувати ідентифікацію ПЗ так, як описано в документації;
- правильність відображення ідентифікації;
- проведення практичних випробувань (вибіркових перевірок) документованих і недокументованих команд, перевірка всіх пунктів меню, якщо вони є;
- проведення практичних випробувань (вибіркових перевірок), із застосуванням периферичного обладнання, якщо воно є.
- перевірка за допомогою вибіркових перевірок щодо подачі попередження перед стиранням збережених даних вимірювань;

- проведення практичних випробувань (вибіркових перевірок), із застосуванням периферичного обладнання, якщо воно є;

- перевірка повноти представленої інформації відповідно до поданої документації.

Знання внутрішньої структури системи для проведення тестування не потрібно.

В результаті проведення даної процедури визначається, чи правильно функціонують програмно-контрольовані функції ~~чи ні~~.

Перевірка на практиці деяких програмно-контрольованих властивостей або функцій ЗВТ може бути пов'язана з деякими труднощами (наприклад, якщо ПЗ не має інтерфейсу зв'язку, то в загальному випадку неможливо визначити несанкціоновані команди, просто намагаючись вводити їх випадковим чином). За необхідності, в цьому випадку призначається проведення інших видів випробувань.

B.2.4 Методи на основі аналізу вихідного коду

B.2.4.1 Аналіз потоку метрологічних даних (DFA)

Аналіз потоку даних являє собою статичний метод тестування, який поєднує в собі отримання інформації за допомогою аналізу потоків даних, що підлягають законодавчому контролю, та інформації про те, які змінні зчитуються або записуються в різних частинах коду.

Цей метод рекомендується застосовувати, якщо здійснено програмне розділення і потрібен високий рівень відповідності або високий рівень захисту від навмисних і ненавмисних змін.

Для проведення процедури необхідна наявність:

- документації на ПЗ;

- вихідного коду;

- текстового редактора;

- програми пошуку тексту або спеціальних програмних засобів;

- знання мов програмування.

Під час проведення процедури відбувається пошук підпрограми, що зчитує необроблені дані від датчика і зберігає ці дані (можливо після деяких підрахунків) в змінну. Потім дані зчитуються іншою підпрограмою, обробляються, зберігаються тощо. В кінці завершене значення вимірювання виводиться на дисплей. Всі змінні, які використовуються для зберігання проміжних значень вимірювань, можуть бути знайдені в вихідному коді за допомогою текстового редактора і програми пошуку тексту.

Об'єктом аналізу потоку даних можуть бути:

- змінні, які можуть бути прочитані, перш ніж їм присвоєне значення (уникнути цього можна, завжди привласнюючи значення при оголошенні нової змінної);

- змінні, які написані більше одного разу без читання (це може означати, що опущена частина коду);

- змінні, які написані, але жодного разу не зчитуються (це може свідчити про наявність надлишкового коду).

Описані невідповідності в коді не завжди є причиною виникнення помилок в процесі роботи програми, але якщо уникати їх появи, ймовірність появи помилок програми буде менше.

B.2.4.2 Тестування програмних модулів (SMT)

Цей метод застосовується, лише тоді, коли перевірки друкованої документації недостатньо для формування переконаності в тому, що програмні функції ПЗ ЗВТ працюють так, як потрібно. Тестування програмних модулів може бути застосовано для пошуку несправностей в логіці і є економічно вигідним при затвердженні динамічних вимірювальних алгоритмів.

Метод рекомендується застосовувати, якщо потрібен високий рівень відповідності або високий рівень захисту від навмисних і ненавмисних змін.

Умови для проведення процедури: вихідний код модуля, що тестується (ТМ), інструменти розробки (як мінімум компілятор), програмний модуль, що підлягає тестуванню, набір вхідних даних і відповідний набір правильних еталонних вихідних даних або інструменти для генерування вхідних і вихідних даних, знання мов програмування. Рекомендується вести співпрацю з програмістом-розробником програмного модуля, що підлягає тестуванню.

ТМ інтегрується в спеціальний тестовий програмний модуль - середовище тестування, що імітує обмін інформацією між даними модулем і іншими частинами ПЗ в процесі роботи ЗВТ. На вхід ТМ подається набір даних, потім дані на виході зчитуються і порівнюються з еталонними даними. Також може використовуватися генератор еталонних даних.

ТМ може бути перевірений як «чорний ящик», коли логіка і структура вихідного коду не досліджуються, або як «скляний ящик», коли вихідний код перевіряється. Тести вибираються для покриття різних частин коду, різних алгоритмів, структур даних і ін.

В результаті проведення процедури визначається коректність застосовуваного вимірювального алгоритму і інших перевірених функцій.

В.2.4.3 Перевірка коду і наскрізний контроль (CIWT)

За допомогою цього методу може бути перевірено будь-яку властивість ~~ЗВТ~~ ПЗ. Застосовується при підвищеній глибині досліджень.

Для проведення процедури необхідні:

- вихідний код;
- текстовий редактор;
- програмні інструменти;
- знання мов програмування.

Експерт послідовно переглядає вихідний код і на основі його аналізу приймає рішення про правильність реалізації відповідних програмних функцій і властивостей.

Експерт може концентрувати увагу на окремих частинах коду з підвищеною ймовірністю появи помилок, недостатньо документованих або складних частинах коду.

Перш, ніж використовувати аналіз вихідного коду, експерт повинен ідентифікувати законодавчо-значиму частину ПЗ (наприклад, за допомогою аналізу потоків метрологічних даних – В 2.4.1).

Цей метод є більш глибоким, додатковим по відношенню до методів, заснованим на перевірці документації, і методу перевірки за допомогою аналізу потоку метрологічних даних. Зазвичай цей метод застосовується тільки для вибіркових перевірок у окремих випадках.

ДОДАТОК Г
Процедура випробування ПЗ ЗВТ згідно ДСТУ OIML D 31:2018

Г.1 Загальні вимоги

Г.1.1 Ідентифікація ПЗ

ПЗ ЗВТ має бути чітко ідентифіковане. Ідентифікація може складатися з більш ніж однієї частини, але принаймні одна частина має бути призначена для ПЗ цілей. Ідентифікація має бути відображена або надрукована за командою або під час роботи або під час запуску для ЗВТ. Якщо ЗВТ не має дисплея або принтера, ідентифікація має бути відправлена через комунікаційний інтерфейс для відображення/друку на іншому пристрої.

Як виняток, позначення ідентифікації ПЗ на приладі буде прийнятним рішенням за наступних умов:

а) Інтерфейс користувача не має можливості відобразити індикацію ідентифікації ПЗ на дисплеї або дисплей технічно не дозволяє відобразити ідентифікацію ПЗ (аналоговий індикатор або електромеханічний лічильник).

б) Прилад не має інтерфейсу комунікації для відправлення ідентифікації ПЗ.

в) Після виготовлення ЗВТ зміна ПЗ неможлива або можлива лише за умови зміни апаратного забезпечення.

Г.1.2 Відповідність алгоритмів та функцій

Вимірювальні алгоритми та функції ЗВТ мають бути відповідними та функціонально правильними для даного застосування та типу ЗВТ (точність алгоритмів, розрахунок ціни згідно з певними правилами, алгоритми округлення тощо). Результат вимірювання та супроводжуюча інформація повинні бути правильно відображені або надруковані. Повинна існувати можливість перевірки алгоритмів та функцій шляхом метрологічних тестів, тестів ПЗ, або огляду ПЗ.

Не повинно існувати прихованих або недокументованих функцій чи параметрів.

Г.1.3 Захист ПЗ

Г.1.3.1 Запобігання втручанням

ЗВТ має бути сконструйований таким чином, щоб можливості для ненавмисного, випадкового або навмисного втручання були мінімальними. Представлення результатів вимірювання має бути однозначним для всіх зацікавлених сторін.

Г.1.3.2 Докази втручання

Г.1.3.2.1 ПЗ повинно бути захищене таким чином, щоб були доступні докази будь-якого втручання (наприклад, оновлення ПЗ, зміни параметрів). ПЗ має бути захищене від несанкціонованої модифікації, завантаження або змін шляхом заміни пристрою пам'яті. Для захисту ЗВТ можуть бути необхідні механічні або інші технічні засоби. Аудиторські сліди (audit trails) вважаються частиною ЗР ПЗ та повинні бути захищені як такі.

Г.1.3.2.2 Лише чітко задокументовані функції можуть бути активовані через інтерфейс користувача. Команди не мають впливати на метрологічні характеристики ЗВТ.

Г.1.3.2.3 Параметри, що визначають ЗР характеристики ЗВТ, повинні бути захищені від модифікації. Повинна бути можливість відобразити або надрукувати поточні налаштування параметрів, якщо необхідно для перевірки ЗВТ.

Г.1.3.2.4 Захист ПЗ має включати відповідні механічні, електронні та/або криптографічні засоби, що робить втручання неможливим або очевидним.

Г.1.4 Підтримка апаратних функцій

Г.1.4.1 Виявлення суттєвих дефектів

Якщо необхідна функція виявлення суттєвих дефектів, виробник повинен передбачити засоби перевірки в ПЗ чи апаратних частинах або забезпечити засоби, за допомогою яких апаратні частини можуть бути підтримані ПЗ ЗВТ. Якщо ПЗ залучене до виявлення суттєвих дефектів, необхідна відповідна дія щодо виявленого дефекту. Наприклад, може бути передбачено, що прилад вимикається або створюється сигнал тривоги, запис в журналі помилок у випадку виявлення суттєвого дефекту.

Документація, що подається для оцінки типу, має містити перелік суттєвих дефектів, які будуть виявлені програмним забезпеченням, та очікувану реакцію, а в разі потреби для розуміння його роботи, опис алгоритму виявлення.

Г.1.4.2 Захист довговічності (Durability protection)

Виробник сам обирає спосіб реалізації засобів захисту довговічності у програмному або апаратному забезпеченні, або дозволяє апаратним засобам підтримуватися програмним забезпеченням.

Г.1.5 Мітки часу (Timestamps)

Мітка часу повинна бути в узгодженому форматі, що дозволяє легко порівнювати два різні записи та відстежувати прогрес з часом. Мітка часу повинна зчитуватися з годинника приладу. Внутрішній годинник автономного ЗВТ може мати значну

невизначеність, якщо не передбачено засобів для синхронізації цього годинника з всесвітнім координованим часом (UTC). У випадках, коли конкретна галузь застосування вимагає високої точності інформації про точний час вимірювання, необхідно підвищити надійність внутрішнього годинника за допомогою спеціальних засобів.

Г.2 Вимоги, до спеціальних конфігурацій

Г.2.1 Загальні положення

Вимоги, наведені в цьому пункті, ґрунтуються на типових технічних рішеннях в інформаційних технологіях.

Г.2.2 Специфікація та розділення ЗР частин інтерфейсів

Ця вимога застосовується, якщо ЗВТ має інтерфейси для взаємодії з іншими приладами, з користувачем чи з іншими програмними частинами, окрім ЗР частин в межах ЗВТ. ЗР частини ЗВТ (програмні або апаратні) – не повинні недопустимо впливати на інші частини ЗВТ.

Г.2.2.1 Розділення компонентів

Г.2.2.1.1 Компоненти ЗВТ, які виконують ЗР функції, повинні бути ідентифіковані, чітко визначені та задокументовані. Вони утворюють ЗР частину ЗВТ.

Г.2.2.1.2 Повинно бути продемонстровано, що функції та дані компонентів, які підпадають під законодавче регулювання, не зазнають впливу через командні інтерфейси від ЗнР частин. Це передбачає однозначне призначення кожної команди для всіх ініційованих функцій або змін даних у компоненті.

Г.2.2.2 Специфікація та розділення частин ПЗ

Г.2.2.2.1 Усі програмні модулі (програми, підпрограми, об'єкти тощо), які виконують ЗР функції або обробляють ЗР вимірювальні дані, утворюють ЗР частину ПЗ ЗВТ, яка повинна бути ідентифікована. Якщо розділення ПЗ не можливе або не потрібне, ПЗ вважається ЗР в цілому.

Г.2.2.2.2 Якщо ЗР частина ПЗ взаємодіє з іншими частинами ПЗ, має бути визначений програмний інтерфейс. Усі комунікації повинні виконуватися виключно через цей інтерфейс. ЗР частина ПЗ і інтерфейс повинні бути чітко задокументовані. Усі ЗР функції та області даних ПЗ повинні бути описані, щоб забезпечити здатність органу оцінки прийняти рішення щодо коректного розділення ПЗ. Програмний інтерфейс складається з програмного коду та визначених областей даних.

Г.2.2.2.3 Повинне бути однозначне визначення кожної команди для всіх функцій або змін даних у ЗР частині ПЗ. Функції, які викликаються через програмний інтерфейс,

повинні бути оголошені і задокументовані. Через програмний інтерфейс можуть бути активовані лише задокументовані функції.

Г.2.2.2.4 Якщо ЗР частина ПЗ була відокремлена від ЗнР програмної частини, ЗР частина ПЗ має пріоритет у використанні ресурсів перед ЗнР програмною частиною. ЗР процес не повинен бути недопустимо перерваний ЗнР програмою. Процес вимірювання (реалізований ЗР частиною ПЗ) не повинен бути затриманий або заблокований іншими процесами.

Г.2.3 Загальнодоступна індикація

Для відображення інформації як ЗР частини ПЗ, так і з іншої може використовуватися екран або вивід на друк. ЗР інформація завжди повинна бути читабельною і чітко відрізнятися від іншої інформації.

Г.2.4 Зберігання даних

Г.2.4.1 Загальне

Якщо вимірювальні дані зберігаються для ЗР цілей, застосовуються вимоги з Г.2.4.2 по Г.2.4.4.

Г.2.4.2 Повнота збережених даних

Збережені вимірювальні дані повинні супроводжуватися всією інформацією, необхідною для майбутнього ЗР використання.

Г.2.4.3 Захист збережених даних

Збережені вимірювальні дані повинні бути захищені програмними засобами для гарантії автентичності, цілісності та, за потреби, правильності інформації щодо часу вимірювання. ПЗ, яке відображає або в подальшому обробляє вимірювальні дані та супровідні дані або результат вимірювання, повинно перевіряти час вимірювання, автентичність та цілісність даних після їх зчитування зі сховища. Якщо виявлено невідповідність, дані повинні бути відкинуті або позначені як непридатні до використання. Програмні модулі, які підготовляють дані для зберігання або перевіряють дані після зчитування, вважаються частиною ЗР ПЗ.

Г.2.4.4 Автоматичне зберігання

Г.2.4.4.1 Вимірювальні дані повинні зберігатися автоматично після завершення вимірювання, тобто після того, як був сформований кінцевий результат вимірювання, який використовується для ЗР цілей. Пристрій зберігання повинен забезпечити непошкоджуванність вимірювальних даних в умовах нормального зберігання. Повинно бути достатньо пам'яті для зберігання всіх необхідних даних. Всі дані, які враховуються у результаті вимірювання, повинні бути автоматично збережені разом із кінцевим значенням.

Примітка 1: У випадку накопичувальних вимірювань може виникнути ситуація, коли одна і та ж область даних (змінна програми) використовується повторно. У цьому випадку ємність зберігання може бути ЗнР.

Г.2.4.4.2 Збережені дані можуть бути видалені, якщо транзакція закрита, або ці дані надруковані друкуючим пристроєм, що підлягає контролю як ЗР.

Г.2.5 Передача даних через лінії комунікацій

Якщо вимірювальні дані передаються до того, як вони будуть використані для ЗР цілей, застосовуються наступні вимоги.

Г.2.5.1 Повнота переданих даних

Передані вимірювальні дані повинні супроводжуватися всією необхідною інформацією для майбутнього ЗР використання.

Г.2.5.2 Захист переданих даних

Передані дані повинні бути захищені програмними засобами для гарантії автентичності, цілісності та, за потреби, правильності інформації щодо часу вимірювання. ПЗ, яке відображає або в подальшому обробляє вимірювальні та супровідні дані, повинно перевіряти час вимірювання, автентичність та цілісність даних, отриманих з каналу передачі. Якщо виявлено невідповідність, дані повинні бути відкинуті або позначені як непридатні до використання. Програмні модулі, які підготовляють дані вимірювань для відправлення або перевіряють дані вимірювань після отримання, вважаються ЗР частиною ПЗ.

Г.2.5.3 Затримка або переривання передачі

На вимірювання не повинна недопустимо впливати затримка або переривання передачі даних. Якщо мережеві служби стають недоступними або дуже повільними, жодні вимірювальні дані не повинні бути втрачені. Можливо, буде необхідно призупинити процес вимірювання, щоб уникнути втрати вимірювальних даних.

Г.2.6 Сумісність операційних систем та апаратного забезпечення

Г.2.6.1 Загальні положення

Якщо операційна система є частиною ЗВТ, вимоги згідно з п. Г.2.6.2 по п. Г.2.6.7 повинні бути виконані. Захист можливий як на рівні апаратної частини так і на рівні ОС.

Г.2.6.2 Апаратні інтерфейси

Апаратні інтерфейси, які не мають захищеного програмного інтерфейсу, не повинні мати змоги недопустимо впливати на ЗР частину ПЗ (наприклад, шляхом перешкоджання використанню інтерфейсу за допомогою фізичної пломби).

Г.2.6.3 Процеси завантаження

Г.2.6.3.1 Якщо необхідний безпечний процес завантаження для захисту ЗР частини ПЗ, застосовуються вимоги пп. Г.2.6.3.2 - Г.2.6.3.5

Г.2.6.3.2 Для забезпечення цілісності та автентичності ЗР частини ПЗ повинен бути встановлений ланцюжок довіри (a chain of trust) через окремі компоненти процесу завантаження.

Г.2.6.3.3 Обробка ланцюжка довіри може бути перервана, за умови збереження його цілісності.

Г.2.6.3.4 Конфігурацію завантаження повинно бути захищено від змін.

Г.2.6.3.5 Запуск через відкриті інтерфейси має бути заборонений.

Г.2.6.4 Ресурси системи

Ресурси системи мають бути достатніми для забезпечення функціонування комбінації ЗР частини ПЗ та ОС.

Г.2.6.5 Захист під час використання

Г.2.6.5.1 Робота ПЗ, яке не є ЗР, не повинна неприпустимо впливати на ЗР ПЗ.

Г.2.6.5.2 Комбінація ЗР частини ПЗ та ОС повинна забезпечувати відображення ЗР інформації.

Г.2.6.5.3 Налаштування контролю доступу унеможливлюють неприпустимі впливи.

Г.2.6.5.4 Адміністративні завдання ЗР частини ПЗ повинні бути захищені.

Г.2.6.6 Комунікація з ЗР частиною ПЗ

Комунікація з ЗР частиною ПЗ повинна здійснюватися через захищені інтерфейси.

Г.2.6.7 Ідентифікація та простежуваність

Г.2.6.7.1 Конфігурацію операційної системи повинно бути ідентифіковано. Ідентифікатор повинен відображатися на ЗВТ за командою або під час роботи.

Г.2.6.7.2 Налаштування конфігурації операційної системи повинні бути захищені таким чином, щоб був доказ про втручання.

Г.2.6.8 Відповідне середовище

Виробник повинен визначити необхідне апаратне та програмне середовище. Мінімальні ресурси та відповідна конфігурація (наприклад, процесор, пам'ять, засоби зв'язку, версія операційної системи тощо), необхідні для правильної роботи, повинні бути оголошені виробником та зазначені у сертифікаті.

Г.2.6.9 Обмеження експлуатації

У ЗР ПЗ повинні бути передбачені технічні засоби для запобігання роботі, якщо не доступні мінімальні ресурси або відповідна конфігурація. Система повинна працювати лише в середовищі, визначеному виробником для правильної роботи.

Г.2.7 Відповідність виготовлених ЗВТ затвердженому типу

Виробник повинен виробляти ЗВТ та ЗР ПЗ, які відповідають затвердженому типу та поданій документації.

Г.2.8 Обслуговування та переконфігурація

Г.2.8.1 Загальне

Оновлення ЗР частини ЗВТ на місці експлуатації слід розглядати як:

- зміну ЗВТ, коли ПЗ замінюється іншою затвердженою версією,
- ремонт ЗВТ, коли перевстановлюється та ж версія.

Г.2.8.2 Вимоги до оновлення

Дозволяється використання лише версій ЗР частини ПЗ, які відповідають затвердженому типу (див. Г.2.7). Вони повинні бути зазначені у сертифікаті.

Застосовність наступних вимог залежить від виду ЗВТ і повинна бути визначена в відповідній Рекомендації. Наступні пп. Г.2.8.3 та Г.2.8.4 є альтернативами. У випадку, коли йдеться про специфічні для ЗВТ параметри (особливо, калібрувальні параметри), слід робити лише перевірене оновлення. Це питання стосується повірки ЗВТ на місці експлуатації.

Г.2.8.3 Перевірене оновлення (Verified update)

ПЗ для оновлення може бути завантажено локально, тобто безпосередньо на ЗВТ, або віддалено через мережу. Завантаження та встановлення можуть бути двома різними кроками. Потрібно розірвати пломбу, щоб оновлення набрало чинності. На місці встановлення ЗВТ повинна бути присутня особа, яка переконується, що оновлене ПЗ було встановлено успішно. Після оновлення ЗР частини ПЗ ЗВТ (заміна іншою затвердженою версією або повторне встановлення) ЗВТ не повинен використовуватися для ЗР цілей до того, до перевірки та оновлення та активації засобів захисту.

Г.2.8.4 Відстежене оновлення (Traced update)

Г.2.8.4.1 ПЗ повинно бути завантажене у ЗВТ згідно з вимогами для відстеженого оновлення (пп. Г.2.8.4.2 - Г.2.8.4.8). Відстежене оновлення - це процедура зміни ПЗ у повіреному ЗВТ або компоненті, після якої подальша перевірка непотрібна. Це означає, що відстежене оновлення не повинно впливати на існуючі параметри. ПЗ для оновлення може бути завантажено локально, тобто безпосередньо на ЗВТ, або віддалено через мережу. Оновлення ПЗ записується в журнал аудиту. Процедура відстеженого оновлення включає кілька кроків: завантаження, перевірку цілісності, перевірку походження (аутентифікацію), встановлення, ведення журналу та активацію.

Г.2.8.4.2 Відстежене оновлення ПЗ повинно бути автоматичним.

Г.2.8.4.3 ПЗ повинно забезпечити доказ будь-якого втручання. Під час оновлення будь-яка інформація про журнал аудиту та значення лічильника подій, повинна бути збережена.

Г.2.8.4.4 Технічні засоби повинні бути використані для гарантування автентичності завантаженого ПЗ.

Г.2.8.4.5 Передбачені технічні засоби для забезпечення цілісності завантаженого ПЗ (ПЗ не було недопустимо змінено перед завантаженням). Це може бути досягнуто додаванням контрольної суми або хеш-коду завантаженого ПЗ та його перевіркою під час процедури завантаження.

Г.2.8.4.6 Для забезпечення належного відстеження оновлень з ЗР частини ПЗ ЗВТ повинен використовуватися журнал аудиту, який забезпечує можливість подальшої перевірки та контролю або інспекції. Журнал аудиту має містити, як мінімум, наступну інформацію: успішність/невдача процедури оновлення; ідентифікація ПЗ встановленої версії; ідентифікація ПЗ попередньої встановленої версії; мітка часу події; ідентифікація завантаженої сторони, якщо це доступно.

Г.2.8.4.7 Може бути необхідним, щоб користувач або власник ЗВТ надав свою згоду на відстежене оновлення. ЗВТ повинен мати можливість для користувача або власника висловити свою згоду, наприклад, натисканням кнопки перед початком оновлення.

6.2.8.4.8 Якщо завантажене ПЗ не пройшло випробування на цілісність (Г.2.8.4.5) або на автентичність (Г.2.8.4.4), прилад повинен відкинути нову версію і використовувати попередню версію ПЗ або перейти в неробочий режим. У цьому режимі функції вимірювання повинні бути заборонені. Якщо журнал аудиту більше недоступний (Г.2.8.4.6), або користувач або власник відмовився від згоди (Г.2.8.4.7), процедура оновлення не повинна запускатися.

Г.2.8.5 Якщо необхідний доступ користувача для налаштування параметрів, що специфічні для ЗВТ, реєстрування будь-якої корекції параметра повинно бути автоматичне та нескасовуване.

Г.2.8.6 Під час оновлення ПЗ запис в журналі не повинен бути стертий або перезаписаний.

Г.3 Рекомендації щодо комбінацій методів оцінювання відповідно до рівнів випробування наведено в таблиці Г.1

Таблиця Г.1 - Рекомендації щодо комбінацій методів оцінювання та випробувань

Вимога		Методи при низькому рівні випробувань	Методи при високому рівні випробувань	Примітка
1		2	3	4
Загальні вимоги				
Г.1.1	Ідентифікація ПЗ	AD + VFTSw	AD + VFTSw + CIWT	Високий рівень випробувань обирається, за необхідності високого ступеню відповідності
Г.1.2	Відповідність алгоритмів та функцій	AD + VFTM	AD + VFTM + CIWT/SMT	
Захист ПЗ				
Г.1.3.1	Запобігання втручанням	AD + VFTSw	AD + VFTSw	
Г.1.3.2	Докази втручання	AD + VFTSw	AD + VFTSw + DFA/CIWT/SMT	Високий рівень випробувань обирається, за високого ризику шахрайства
Підтримка апаратних функцій				
Г.1.4.1	Виявлення значних дефектів	AD + VFTSw	AD + VFTSw + CIWT + SMT	Високий рівень випробувань обирається, за необхідності високої надійності
Г.1.4.2	Захист довговічності (Durability protection)	AD + VFTSw	AD + VFTSw + CIWT + SMT	Високий рівень випробувань обирається, за необхідності високої надійності

1		2	3	4
Г.1.5	Мітки часу	AD + VFTSw	AD + VFTSw + SMT	
Вимоги для спеціальних конфігурацій				
Г.2.2.1	Розділення	AD	AD + DFA/CIWT	
Г.2.2.2	Специфікація та розділення частин ПЗ	AD	AD + DFA/CIWT	
Г.2.3	Загальнодоступна індикація	AD + VFTM/ VFTSw	AD + VFTM/ VFTSw + DFA/CIWT	
Г.2.4	Зберігання даних	AD + VFTSw	AD + VFTSw + CIWT/SMT	Високий рівень випробувань обирається у разі передбаченого незахищеного зберігання даних
Г.2.4.2	Повнота збережених даних	AD + VFTSw	AD + VFTSw + CIWT/SMT	Високий рівень випробувань обирається, за високого ризику шахрайства
Г.2.4.3	Захист збережених даних	AD + VFTSw	AD + VFTSw + SMT	
Г.2.4.4	Автоматичне зберігання	AD + VFTSw	AD + VFTSw + SMT	
Г.2.5	Передача даних	AD + VFTSw	AD + VFTSw + CIWT/SMT	Високий рівень випробувань обирається у разі передбаченої передачі даних через відкриті мережі
Г.2.5.1	Повнота переданих даних	AD + VFTSw	AD + VFTSw + CIWT/SMT	Високий рівень випробувань обирається, за високого ризику шахрайства
Г.2.5.2	Захист переданих даних	AD + VFTSw	AD + VFTSw + SMT	
Г.2.5.3	Затримка або переривання передачі	AD + VFTSw	AD + VFTSw + SMT	Високий рівень випробувань обирається за високого

1		2	3	4
				ризику шахрайства, напр. - передача даних через відкриті мережі
Г.2.6	Сумісність операційних систем та апаратного забезпечення	AD + VFTSw	AD + VFTSw + SMT	
Г.2.6.2	Апаратні інтерфейси	AD + VFTSw	AD + VFTSw + SMT	
Г.2.6.3	Процеси завантаження	AD + VFTSw	AD + VFTSw + SMT	
Г.2.6.4	Ресурси системи	AD + VFTSw	AD + VFTSw + SMT	
Г.2.6.5	Захист під час використання	AD + VFTSw	AD + VFTM/ VFTSw + DFA	
Г.2.6.6	Комунікація з ЗР частиною ПЗ	AD + VFTSw	AD + VFTM/ VFTSw + DFA	
Г.2.6.7	Ідентифікація та простежуваність	AD + VFTSw	AD + VFTSw + SMT	
Г.2.6.8	Відповідне середовище	AD + VFTSw	AD + VFTSw + SMT	
Г.2.6.9	Обмеження експлуатації	AD + VFTSw	AD + VFTSw + SMT	
Обслуговування та переконфігурація				
Г.2.8.3	Перевірене оновлення	AD	AD	
Г.2.8.4	Відстежене оновлення	AD + VFTSw	AD + VFTSw + CIWT/SMT	Високий рівень випробувань обирається за високого ризику шахрайства

ДОДАТОК Д

Форма протоколу випробувань ПЗ

ПРОТОКОЛ

випробувань програмного забезпечення

Реєстраційний номер _____ **Дата реєстрації** _____

Видається _____

_____

_____

Об'єкт випробувань _____

_____

Вимоги до випробувань _____

_____

Додаткові вимоги _____

Місце випробувань _____

_____

Період випробувань _____

Кількість сторінок протоколу _____

Затвердив

_____ _____

(підпис)

М.П.

Перевірив

_____ _____

(підпис)

Випробування провів

_____ _____

(підпис)

Позначення _____ **Версія** _____

Розробник ПЗ _____

_____

_____

Назва, тип ЗВТ _____

_____

Виробник ЗВТ _____

_____

Призначення ЗВТ _____

Надане програмне забезпечення

Назва файлу	*Об'єм, байти*	*Тип файлу*	*Дата та час*

Надана документація

Позначення в протоколі	*Позначення, назва*

Надані файли вихідного коду

Назва файлу	*Об'єм файлу*	*Дата запису файлу*

Рівень жорстокості випробувань _____

Результати випробувань

Перевірка відповідності ПЗ основним вимогам до ЗВТ

Позначення, назва та зміст вимоги	*Результат перевірки та висновок*
Висновок	

Перевірка відповідності ПЗ додатковим вимогам до ЗВТ

Позначення, назва та зміст вимоги	*Результат перевірки та висновок*
Висновок	

Висновок