Section: Information Technology, Cyber Security and Computer Engineering

DOI 10.70286/EOSS-12.01.2026.001.76-84

МЕТОДИ АПАРАТНОГО ТА ПРОГРАМНОГО ЗАХИСТУ МІКРОКОНТРОЛЕРНИХ СИСТЕМ В УМОВАХ ЗРОСТАННЯ КІБЕРЗАГРОЗ

Слободяник Костянтин
аспірант
Карасюк Анастасія
здобувач вищої освіти
Кафедра інформаційних технологій проєктування та дизайну
НУ «Одеська політехніка», Україна

Анотація. У статті проаналізовано сучасні загрози інформаційній безпеці мікроконтролерних систем та систематизовано апаратні й програмні методи їхнього захисту з урахуванням обмежених ресурсів вбудованих платформ і можливості фізичного доступу до пристроїв. Показано, що мікроконтролерні системи, які широко застосовуються у вбудованих, кіберфізичних та IoT-рішеннях, формують специфічний ландшафт загроз, у якому програмні атаки поєднуються з апаратними втручаннями та атаками на канали обміну даними. Розглянуто основні класи загроз, включаючи модифікацію прошивки, експлуатацію вразливостей криптографічних реалізацій, атаки через інтерфейси налагодження, аналіз побічних каналів і перехоплення або підміну даних під час передавання. Обґрунтовано роль апаратних механізмів захисту, таких як безпечне завантаження, апаратна ізоляція пам’яті, захист інтерфейсів налагодження та вбудовані криптографічні модулі, у формуванні базового рівня довіри до платформи. Показано, що програмні засоби — контроль цілісності прошивки, криптографічний захист даних, безпечне оновлення програмного забезпечення та керування доступом — доповнюють апаратні механізми, забезпечуючи гнучкість і адаптивність системи безпеки. Зроблено висновок про доцільність комбінованого застосування апаратних і програмних підходів у межах багаторівневої моделі захисту, заснованої на принципах security by design та defense in depth, для підвищення стійкості мікроконтролерних систем до сучасних кіберзагроз.

Ключові слова: мікроконтролерні системи, інформаційна безпека, апаратний захист, програмний захист, Secure Boot, IoT, defense in depth.

Введення. Мікроконтролерні системи є базовими компонентами сучасних вбудованих, кіберфізичних та IoT-рішень і широко застосовуються в промисловій

автоматизації, медичних пристроях, транспортних системах, побутовій електроніці та системах «розумного дому». З огляду на стрімке зростання кількості підключених пристроїв, мікроконтролери дедалі частіше стають об'єктами цілеспрямованих кіберзагроз, спрямованих на порушення конфіденційності, цілісності та доступності оброблюваних даних [1, 2].

На відміну від класичних обчислювальних систем, мікроконтролерні платформи мають суттєві обмеження за обчислювальними ресурсами, обсягом пам'яті та енергоспоживанням. Ці обмеження ускладнюють застосування традиційних механізмів захисту, характерних для серверних або настільних систем, і вимагають спеціалізованих підходів до забезпечення безпеки [3]. Водночас фізична доступність багатьох вбудованих пристроїв створює додаткові ризики, пов'язані з апаратними атаками, зчитуванням прошивки, втручанням у канали обміну даними та експлуатацією інтерфейсів налагодження.

Зростання складності атак на мікроконтролерні системи зумовлює необхідність поєднання апаратних і програмних методів захисту. Апаратні механізми — такі як безпечне завантаження, ізоляція пам'яті та апаратні модулі криптографії — забезпечують базовий рівень довіри до платформи. Програмні засоби, своєю чергою, дозволяють реалізувати контроль цілісності, захист прошивки, криптографічний захист даних і механізми безпечного оновлення програмного забезпечення [4, 5].

У сучасних умовах мікроконтролерні системи дедалі частіше розглядаються як частина розподілених інформаційних систем, де компрометація одного пристрою може призвести до каскадних наслідків для всієї інфраструктури. Це зумовлює потребу в комплексному підході до безпеки, який охоплює як апаратний рівень, так і програмну реалізацію, з урахуванням специфіки експлуатації вбудованих пристроїв [6].

Таким чином, актуальним є аналіз методів апаратного та програмного захисту мікроконтролерних систем, а також визначення їхніх переваг, обмежень і можливостей комбінованого застосування для підвищення загального рівня інформаційної безпеки.

Мета та завдання дослідження. Метою дослідження є аналіз та систематизація методів апаратного й програмного захисту мікроконтролерних систем з урахуванням обмежених ресурсів вбудованих платформ і зростання складності сучасних кіберзагроз.

Досягнення поставленої мети передбачає розгляд мікроконтролерної системи як багаторівневої структури, у межах якої безпека формується сукупністю апаратних механізмів довіри, програмних засобів захисту та організаційних підходів до розроблення й експлуатації. На відміну від традиційних обчислювальних систем, у вбудованих пристроях апаратний рівень відіграє ключову роль у забезпеченні базової довіри, тоді як програмні механізми доповнюють його, реалізуючи гнучкі та адаптивні засоби протидії загрозам [3, 4].

Особливістю мікроконтролерних платформ є поєднання кіберзагроз із фізичним доступом до пристроїв, що потребує одночасного врахування атак програмного характеру та апаратних атак, зокрема аналізу побічних каналів і втручання в інтерфейси налагодження. У цьому контексті дослідження орієнтоване на визначення ефективності комбінованого застосування апаратних і програмних методів захисту [2, 6].

Для досягнення поставленої мети в роботі визначено такі завдання дослідження:

1. Проаналізувати архітектурні особливості мікроконтролерних систем, що впливають на реалізацію механізмів інформаційної безпеки, зокрема організацію пам’яті, режими виконання та інтерфейси взаємодії.

2. Класифікувати основні загрози безпеці мікроконтролерних систем, включаючи програмні атаки, апаратні втручання та атаки на канали зв’язку.

3. Дослідити апаратні методи захисту, такі як безпечне завантаження, апаратна ізоляція пам’яті, захист інтерфейсів налагодження та використання вбудованих криптографічних модулів.

4. Проаналізувати програмні механізми захисту, зокрема контроль цілісності прошивки, криптографічний захист даних, безпечне оновлення програмного забезпечення та керування доступом.

5. Оцінити доцільність комбінованого застосування апаратних і програмних підходів для підвищення рівня захищеності мікроконтролерних систем у практичних сценаріях експлуатації.

Виконання зазначених завдань дозволяє сформувати цілісне уявлення про сучасні підходи до захисту мікроконтролерних систем і визначити напрями підвищення їхньої стійкості до кіберзагроз. Отримані результати можуть бути використані при проєктуванні вбудованих пристроїв, а також у процесі оцінювання безпеки існуючих рішень.

Результати дослідження і їх обговорення.

Загрози безпеці мікроконтролерних систем. Мікроконтролерні системи функціонують у середовищі, де поєднуються обмежені обчислювальні ресурси, тривалий життєвий цикл пристроїв і часто відсутній фізичний контроль доступу. Це формує специфічний ландшафт загроз, у якому програмні атаки тісно переплітаються з апаратними втручаннями та атаками на канали обміну даними. Для коректного вибору методів захисту доцільно розглядати загрози за їхньою природою та рівнем впливу на систему.

Програмні загрози. Програмні загрози є найбільш поширеним класом атак на мікроконтролерні системи, особливо в пристроях, підключених до мереж або інтегрованих у розподілені інформаційні системи. До цієї категорії належать уразливості прошивки, помилки реалізації протоколів обміну даними та недостатній контроль доступу до функціональних модулів.

Однією з типових загроз є модифікація або підміна прошивки пристрою. У разі відсутності механізмів перевірки цілісності зловмисник може завантажити

змінену версію програмного забезпечення, яка виконує приховані функції або порушує штатну логіку роботи системи. Подібні атаки особливо небезпечні для пристроїв з можливістю віддаленого оновлення прошивки.

Іншою поширеною проблемою є некоректна реалізація криптографічних алгоритмів або використання слабких ключів і застарілих протоколів. В умовах обмежених ресурсів розробники інколи відмовляються від повноцінних механізмів захисту, що призводить до зниження криптостійкості та відкриває можливості для перехоплення або підміни даних.

Апаратні загрози та фізичний доступ. На відміну від серверних або настільних систем, мікроконтролерні пристрої часто експлуатуються в умовах, де зловмисник може отримати фізичний доступ до обладнання. Це створює передумови для апаратних атак, спрямованих на зчитування конфіденційної інформації або втручання в роботу пристрою.

До таких загроз належать атаки через інтерфейси налагодження та програмування, які в багатьох випадках залишаються активними після введення пристрою в експлуатацію. За їх допомогою можливе зчитування пам’яті, модифікація прошивки або отримання ключових матеріалів. Окрему групу становлять атаки на побічні канали, зокрема аналіз споживання електроенергії або електромагнітного випромінювання, які дозволяють відновлювати криптографічні ключі без прямого втручання в програмний код.

Фізичне втручання також може включати спроби порушення цілісності апаратних компонентів, зміну конфігурації пам’яті або використання спеціалізованого обладнання для обходу захисних механізмів. Такі атаки потребують значних технічних ресурсів, проте в критичних системах їхня ймовірність не може бути проігнорована.

Загрози через канали обміну даними. Мікроконтролерні системи часто взаємодіють із зовнішніми компонентами через бездротові або дротові канали зв’язку, що створює додатковий вектор атак. Перехоплення, підміна або повторне відтворення переданих даних можуть призвести до порушення функціонування пристрою або компрометації всієї системи.

Особливо небезпечними є атаки типу повторної передачі повідомлень, коли зловмисник використовує перехоплені пакети для відтворення легітимних команд. За відсутності механізмів автентифікації та захисту від повторів такі атаки можуть бути реалізовані навіть без знання внутрішньої логіки пристрою. У бездротових мережах додаткові ризики пов’язані з можливістю глушіння сигналу або нав’язування хибних вузлів зв’язку.

Таким чином, загрози безпеці мікроконтролерних систем мають комплексний характер і охоплюють програмний, апаратний та комунікаційний рівні. Це обумовлює необхідність багаторівневого підходу до захисту, у межах якого апаратні та програмні методи доповнюють один одного. У наступному розділі буде розглянуто апаратні методи захисту, що формують базовий рівень довіри до мікроконтролерних платформ.

Апаратні методи захисту мікроконтролерних систем. Апаратні методи захисту формують базовий рівень довіри до мікроконтролерної системи та є критично важливими в умовах обмежених ресурсів і можливого фізичного доступу до пристрою. На відміну від програмних механізмів, апаратні засоби складніше обійти або модифікувати без спеціалізованого обладнання, що робить їх фундаментом безпеки вбудованих систем [4, 6].

Безпечне завантаження (Secure Boot). Одним із ключових апаратних механізмів захисту є безпечне завантаження, яке забезпечує перевірку автентичності та цілісності прошивки перед її виконанням. Принцип роботи Secure Boot полягає у формуванні ланцюга довіри, де кожен етап завантаження перевіряє цифровий підпис наступного компонента. У разі невідповідності підпису або виявлення модифікацій виконання коду блокується.

Реалізація Secure Boot дозволяє ефективно протидіяти атакам, спрямованим на підміну або модифікацію прошивки, навіть за наявності фізичного доступу до пристрою. Такий підхід є особливо важливим для мікроконтролерів, що використовуються в критичних системах, де компрометація програмного забезпечення може мати значні наслідки [3, 5].

Апаратна ізоляція та захист пам’яті. Значну роль у забезпеченні безпеки відіграють механізми апаратної ізоляції пам’яті та виконуваного коду. Сучасні мікроконтролери підтримують розмежування доступу до різних областей пам’яті, що дозволяє відокремити критичні компоненти системи від менш довірених частин програмного забезпечення.

Такі механізми запобігають несанкціонованому доступу до конфіденційних даних і ускладнюють реалізацію атак, спрямованих на ескалацію привілеїв. Апаратна ізоляція особливо ефективна у поєднанні з багаторежимною моделлю виконання, де окремі функції працюють у привілейованому або захищеному режимі, недоступному для звичайного прикладного коду.

Захист інтерфейсів налагодження та програмування. Інтерфейси налагодження та програмування є важливими для розроблення й тестування мікроконтролерних систем, проте після введення пристрою в експлуатацію вони можуть стати серйозним джерелом ризику. Через такі інтерфейси можливе зчитування вмісту пам’яті, модифікація прошивки або отримання доступу до внутрішніх регістрів системи.

Апаратні методи захисту передбачають повне або часткове відключення інтерфейсів налагодження, їхнє блокування після першого програмування або захист за допомогою апаратних паролів і ф’юзів. Застосування таких заходів значно ускладнює фізичні атаки та зменшує ризик несанкціонованого доступу до внутрішньої структури пристрою [6].

Апаратні криптографічні модулі. Вбудовані криптографічні модулі дозволяють виконувати криптографічні операції без залучення основного процесора, що підвищує продуктивність і знижує енергоспоживання. Крім того, апаратна реалізація криптографії зменшує ризик атак на побічні канали, оскільки

такі модулі часто мають додаткові засоби захисту від аналізу споживаної потужності та електромагнітного випромінювання [3, 4].

Апаратні криптографічні модулі використовуються для зберігання ключів, генерації випадкових чисел і виконання операцій шифрування, хешування та цифрового підпису. Їх застосування підвищує загальний рівень безпеки системи та дозволяє реалізувати надійний захист даних навіть у ресурсно обмежених мікроконтролерних платформах.

Таким чином, апаратні методи захисту створюють основу безпеки мікроконтролерних систем, забезпечуючи початковий рівень довіри та захист від широкого спектра атак. Водночас вони не можуть повністю замінити програмні механізми, а потребують їхнього доповнення для реалізації гнучких і адаптивних засобів захисту. У наступному розділі буде розглянуто програмні методи забезпечення безпеки мікроконтролерних систем.

Програмні методи захисту мікроконтролерних систем. Програмні методи захисту доповнюють апаратні механізми та забезпечують гнучкість і адаптивність системи безпеки мікроконтролерних платформ. Вони дозволяють реалізувати контроль цілісності програмного забезпечення, захист даних у процесі зберігання й передавання, а також механізми безпечного оновлення прошивки без фізичного доступу до пристрою [2, 5].

Контроль цілісності та автентичності прошивки. Одним із базових програмних механізмів захисту є контроль цілісності прошивки, який забезпечує виявлення несанкціонованих змін у коді. Такий контроль зазвичай реалізується шляхом обчислення криптографічних хешів або перевірки цифрових підписів програмного забезпечення під час запуску або в процесі роботи системи.

Поєднання програмного контролю цілісності з апаратним Secure Boot дозволяє сформувати надійний ланцюг довіри, у якому навіть за компрометації окремих компонентів атака може бути виявлена на ранньому етапі. Це особливо актуально для пристроїв із тривалим життєвим циклом, які експлуатуються протягом багатьох років без фізичного обслуговування [4].

Криптографічний захист даних. Програмні криптографічні механізми забезпечують конфіденційність і цілісність даних, що зберігаються в пам’яті мікроконтролера або передаються через канали зв’язку. У практичних реалізаціях застосовуються симетричні алгоритми шифрування для захисту даних і асиметричні алгоритми для автентифікації та обміну ключами.

З огляду на обмежені ресурси мікроконтролерів, особливого значення набуває вибір ефективних алгоритмів і режимів роботи. Неправильна реалізація криптографії або використання слабких параметрів може нівелювати переваги навіть наявних апаратних засобів захисту. Тому програмні криптографічні модулі повинні розроблятися з урахуванням вимог до продуктивності, енергоспоживання та стійкості до атак [3, 5].

Безпечне оновлення програмного забезпечення. Механізми безпечного оновлення прошивки є критично важливими для підтримання актуального рівня

безпеки мікроконтролерних систем. Вони дозволяють усувати виявлені вразливості та додавати нові функції без фізичного втручання в пристрій.

Програмні засоби захисту в цьому контексті передбачають автентифікацію джерела оновлення, перевірку цілісності завантажених даних і захист від атак повторного відтворення. За відсутності таких механізмів оновлення прошивки може стати вектором атаки, що дозволяє зловмиснику впровадити шкідливий код у систему [2, 6].

Керування доступом і логіка безпеки. Додатковим рівнем захисту є реалізація програмних механізмів керування доступом до функціональних можливостей мікроконтролерної системи. Обмеження доступу до критичних операцій, перевірка прав користувачів і контроль виконання команд дозволяють зменшити наслідки потенційної компрометації окремих компонентів.

У поєднанні з журналюванням подій безпеки такі механізми створюють основу для виявлення аномальної поведінки та реагування на інциденти. Хоча можливості моніторингу в мікроконтролерних системах обмежені, навіть базові засоби реєстрації подій можуть істотно підвищити рівень захищеності системи в реальних умовах експлуатації. На рис. 1 подано узагальнену модель безпеки мікроконтролерної системи, що поєднує апаратні та програмні методи захисту. Апаратний рівень формує початкову довіру до платформи за рахунок механізмів безпечного завантаження, апаратної ізоляції пам’яті, захисту інтерфейсів налагодження та використання вбудованих криптографічних модулів. Ці засоби ускладнюють фізичні атаки та забезпечують захист критичних ресурсів пристрою.

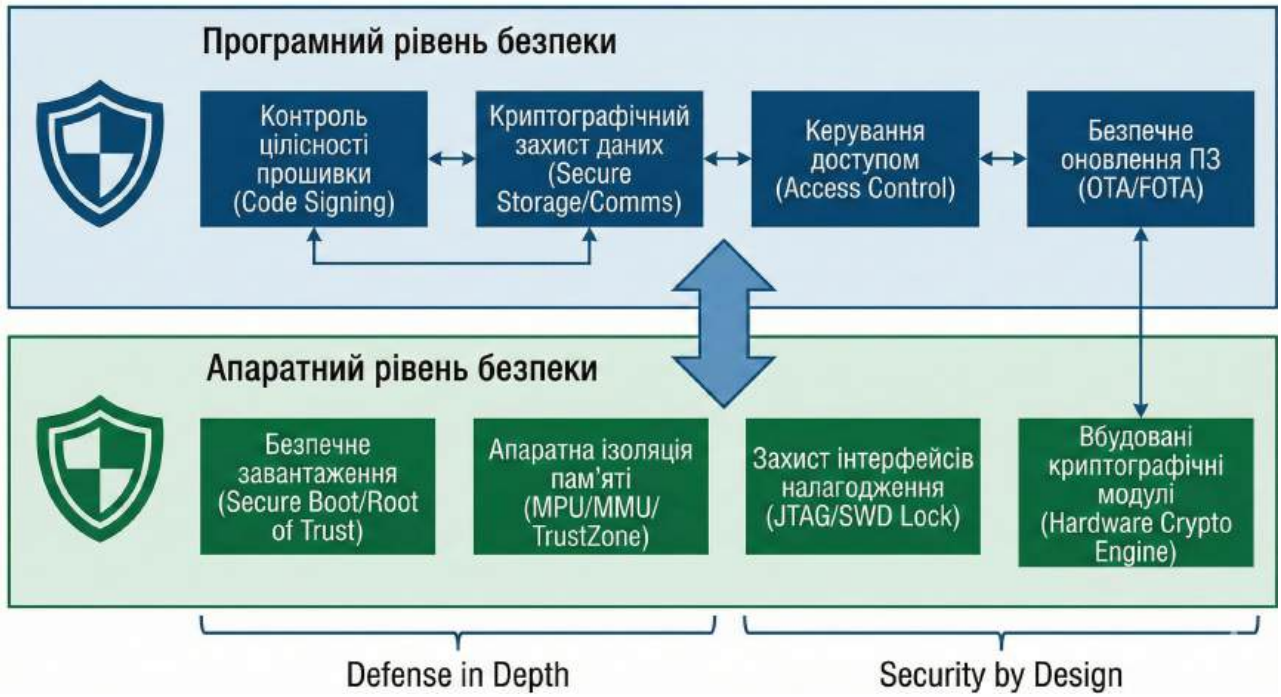

Рисунок 1. Багаторівнева модель безпеки мікроконтролерної системи

Програмний рівень доповнює апаратні механізми, реалізуючи контроль цілісності прошивки, криптографічний захист даних, керування доступом і безпечне оновлення програмного забезпечення. Взаємодія між рівнями дозволяє створити комплексну систему безпеки, стійку до програмних, апаратних та комунікаційних загроз, що відповідає принципам defense in depth і security by design.

Розглянуті програмні методи захисту демонструють, що безпека мікроконтролерних систем не може бути досягнута виключно апаратними засобами. Лише поєднання апаратних механізмів довіри з програмними засобами контролю й захисту даних дозволяє створити стійку до сучасних кіберзагроз вбудовану систему.

Висновки. У межах роботи проаналізовано сучасні загрози безпеці мікроконтролерних систем та розглянуто апаратні й програмні методи протидії, що застосовуються у вбудованих і IoT-пристроях. Показано, що специфіка мікроконтролерних платформ — обмежені обчислювальні ресурси, тривалий життєвий цикл і можливість фізичного доступу — суттєво ускладнює використання традиційних підходів до інформаційної безпеки та потребує спеціалізованих рішень.

У роботі систематизовано основні класи загроз, зокрема програмні атаки на прошивку, апаратні втручання та атаки через канали обміну даними. Встановлено, що ізольоване застосування окремих механізмів захисту не забезпечує належного рівня стійкості системи. Апаратні засоби, такі як безпечне завантаження, ізоляція пам’яті, захист інтерфейсів налагодження та вбудовані криптографічні модулі, формують початковий рівень довіри до платформи, однак потребують доповнення програмними механізмами.

Програмні методи захисту — контроль цілісності прошивки, криптографічний захист даних, безпечне оновлення програмного забезпечення та керування доступом — забезпечують гнучкість і адаптивність системи безпеки. Їх поєднання з апаратними механізмами дозволяє реалізувати багаторівневу модель захисту, стійку до широкого спектра атак як програмного, так і апаратного характеру.

Отримані результати свідчать про доцільність комплексного підходу до безпеки мікроконтролерних систем, заснованого на принципах security by design та defense in depth. Такий підхід може бути використаний при проєктуванні нових вбудованих пристроїв, а також для оцінювання рівня захищеності вже впроваджених систем. Подальші дослідження доцільно спрямувати на аналіз автоматизованих засобів виявлення атак на мікроконтролерні платформи та інтеграцію механізмів безпеки з системами централізованого моніторингу.

Список використаних джерел

1. Wolf M. Security in Automotive Bus Systems / M. Wolf, A. Weimerskirch, C. Paar // Proceedings of the Workshop on Embedded Security in Cars. – 2004.

2. Roman R. Securing the Internet of Things / R. Roman, P. Najera, J. Lopez // Computer. – 2011. – Vol. 44, № 9.
3. Kocher P. Introduction to Differential Power Analysis / P. Kocher et al. // Journal of Cryptographic Engineering. – 2011.
4. ARM Ltd. Platform Security Architecture (PSA) : Technical White Paper. – 2022.
5. Stallings W. Cryptography and Network Security. – 8th ed. – Harlow : Pearson, 2023.
6. Garcia F. D. Hardware Attacks on Embedded Systems / F. D. Garcia, D. Oswald, T. Kasper, P. Pavlidès // IEEE Security & Privacy. – 2019.
7. Mangard S. Power Analysis Attacks: Revealing the Secrets of Smart Cards / S. Mangard, E. Oswald, T. Popp. – Berlin : Springer, 2007.

ФУНКЦІОНАЛЬНІ ВИМОГИ БЕЗПЕКИ ISO/IEC 15408-2:2022

Гріненко Т.О.
к.т.н., доцент
Рой Є.О.
здобувач вищої освіти бакалаврського рівня
Олефіренко І.І.
здобувач вищої освіти бакалаврського рівня
Кафедра безпеки інформаційних технологій
Харківський національний університет радіоелектроніки, Україна

Анотація. У роботі надані результати аналізу та дослідження функціональних вимог безпеки стандарту ISO/IEC 15408-2:2022. Проаналізовані нові сімейства вимог (FDP_SDC, FPT_INI, FIA_API), що спрямовані на захист даних у стані спокою, ініціалізацію та автентифікацію в розподілених системах. Визначено роль стандарту як інструменту інтеграції українських IT-продуктів у глобальний безпековий простір.

Ключові слова: Common Criteria, ISO/IEC 15408, CCRA, кібербезпека, сертифікація, функціональна вимога безпеки.

Вступ. В жовтні 2025 року Україна офіційно приєдналася до угоди про визнання загальних критеріїв (Common Criteria Recognition Arrangement, CCRA). CCRA – міжнародна угода, яка забезпечує взаємне визнання сертифікатів безпеки IT-продуктів, виданих у країнах-учасницях. Вона ґрунтується на стандартах ISO/IEC 15408 та ISO/IEC 18045 і має на меті підвищення довіри до безпеки інформаційних технологій, а також спрощення виходу IT-продуктів на міжнародні ринки. Відтепер українські сертифікати визнаються у понад 30 країнах-учасницях угоди, що відкриває експортні можливості для вітчизняного бізнесу [1].

ISO/IEC 15408 встановлює єдину, чітку методологію для формулювання вимог з безпеки IT-продуктів та оцінювання рівня довіри до них. Його головна