УДК 004.056.5 **DOI:10.30837/rt.2025.4.223.06**

П.В. ШУЛІК, канд. техн. наук, Д.С. БАЛАГУРА, канд. техн. наук,
В.В. ПРОСОЛОВ, Д.О. В'ЮХІН

СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ OPEN PORTABLE TRUSTED EXECUTION ENVIRONMENT (OP-TEE), KVM/QEMU ТА INTEL TRUST DOMAIN EXTENSIONS

Вступ

За останні 10–15 років технології захисту інформації в мобільних пристроях та мікроконтролерах дуже просунулись завдяки розвитку бездротового Інтернету та систем Інтернету речей (IoT). Тобто, невеликі малопотужні пристрої стали частиною великої мережі – Інтернет. Але їх низькі обчислювальні потужності привели до неспроможності ефективного захисту несанкціонованого доступу до інформації. Таким чином це призвело до значного поштовху в розробці апаратно-програмних технологій захисту інформації для таких пристроїв.

Переважна більшість таких пристроїв базується на процесорах Advanced RISC Machines (ARM) одноіменної компанії. Тому ARM прийшлось зайнятись розробкою підсистем захисту інформації для своїх архітектур та розробити технологію ARM TustZone [1, 2]. Технологія була представлена ще у 2002 р., але до більш-меньш поширеного використання дійшло тільки після 2009 р. Основна ідея ARM TustZone заключається в розподілі обчислень на звичайні та сек'юрні та ізоляції доступу зі звичайного середовища (операційної системи та звичайних додатків) до сек'юрних даних та обчислень. Це робиться завдяки апаратно-програмним механізмам. На рівні апаратних механизмів периферія поділяється на елементи для роботи з захищеною та звичайною інформацією – наприклад, розподіл оперативної пам'яті та флеш пам'яті. В ARM TrustZone також вводиться захищений режим роботи ARM ядра. У ньому виконується робота з секретною інформацією, яка не повинна бути доступною для основної операційної системи та її додатків.

З боку програмних механізмів існує багато різних підходів ізоляції доступу на рівні окремих додатків та на рівні ізольованих операційних систем. В сучасних операційних системах для захисту інформації існує підхід з використанням двох операційних систем, де система поділяється на два світи: звичайний (non secure world) – де працює звичайне програмне забезпечення, та захищений світ (secure world), в якому ведеться робота з конфіденційною інформацією. Звичайний світ не має доступу до захищеного світу, тоді як останній може з'єднуватись при бажанні з різними пристроями. Цей підхід стосується не тільки процесора, але і пам'яті, транзакції на шинах, переривань, периферійніх пристроїв в рамках системи, в тому числі, програмного забезпечення.

Як приклад програмної підтримки такого підходу можна навести опен соурс фреймфорк OP-TEE (Open Portable Trusted Execution Environment) [3]. Це відкритий фреймворк TEE для платформ ARM, що реалізує захищене середовище виконання на базі TrustZone та сумісний зі специфікаціями GlobalPlatform. Типова архітектура програмного забезпечення OP-TEE показана на рис. 1.

У звичайному світі працює основна операційна система, наприклад Linux або Android та звичайні додатки. Коли потрібно запустити якусь задачу, яка працює з конфіденційними даними, наприклад, аутентифікація, шифрування даних, банківські операції та інше, то йде запит від звичайного до сек'юрного світу. Для цього використовується API, який надається сек'юрним світом. Звернення до API виконується через Kernel module (або драйвер) та Monitor. Monitor розташований в сек'юрному світі та виступає арбітром, який обробляє запити від звичайного світу та повертає відповіді. В сек'юрному світі на рівні User space працюють додатки, які запускаються у відповідь на API запити.

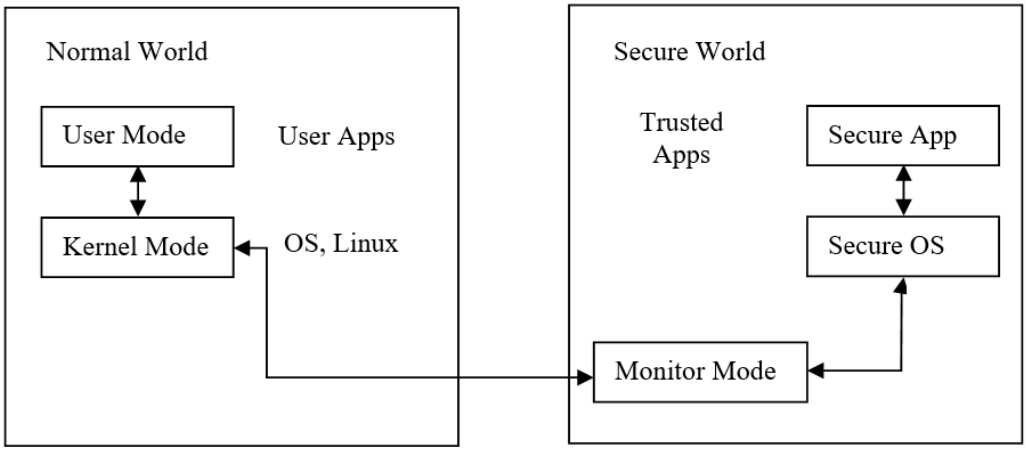

Рис. 1. Типова архітектура поділу світів OP-TEE

Спочатку OP-TEE була створена безпосередньо для підтримки ARM TrustZone для процесорів ARM Cortex A, де використовуються Unix-подібні операційні системи. Але OP-TEE поширюється дуже активно останні декілька років для роботи вбудованих та мобільних пристроїв і набрала популярності. Такий стан справ викликає інтерес до використання OP-TEE з боку виробників серверних рішень, де системи в основному базуються на процесорах Intel-x86. Підтримка такого підходу з боку Intel-x86 платформ є проблематичною, тому що Intel не має подібних ARM TrustZone рішень. Але Intel-x86 має розвинену апаратну підтримку віртуалізацій, де для організації secure world може використовуватися окрема віртуальна машина.

Апаратна віртуалізація Intel-x86 (або VT-d/VT-x) [4, 5] – це технологія, що дозволяє запуск віртуальних машин в ізольованому режимі, де пам’ять, дисковий простір, периферія можуть бути розподілені та ізольовані між віртуальними машинами, тобто одна віртуальна машина не буде мати доступу до ресурсів іншої віртуальної машини.

Intel постійно удосконалює аппаратні механізми для підтримки сек’юрних рішень та реалізаціїї концепції поділу світів. Однією із останніх розробок від Intel є технологія Trust Domain Extensions (Intel TDX), яка додає нові апаратні елементи для ізоляції доступу до ресурсів віртуальних машин.

Метою даного дослідження є створення системи захисту інформації на основі інтеграції OP-TEE фреймворка з Intel-X86 платформами з використанням технології Intel TDX та VT-d/VT-x.

Предметом дослідження є програмні засоби інтеграції OP-TEE фреймворка з Intel-x86 VT-d/VT-x з використанням Intel TDX.

Суть інтеграції OP-TEE складається в заміщенні технологїї TrustZone віртуальними машинами та технологіями процесорів Intel-x86 VT-d/VT-x, де апаратні ресурси розподіляються між віртуальними операційними системами, і забезпечують ізоляцію ресурсів та інформації між операційними системами [6, 7]. В свою чергу Intel TDX додала нові елементи для підтримки ізоляції між віртуальними машинами. Перший елемент називається Total Memory Encryption (Intel TME), він забезпечує можливість шифрування пам’яті кожної віртуальної машини. Другий елемент – це новий режим праці процесора, який називається Secure-Arbitration Mode (SEAM) і в концепції повторює режим роботи non-secure/secure процессора ARM.

Технологія Intel TDX

Intel Trust Domain Extensions [8] була запропонована у травні 2021 р. для реалізації довіреного середовища, в якому віртуальні машини (так звані «довірчі домени» або TD) апаратно ізольовані від монітора віртуальної машини хоста (VMM), гіпервізора та іншого програмного забезпечення на хості. Ця апаратна ізоляція призначена для запобігання загроз суб'єктів

з адміністративним доступом або фізичним доступом до віртуальної машини хоста від шкоди аспектам конфіденційності та цілісності віртуальної машини.

Intel TDX включає апаратне середовище довіреного виконання (TEE), яке полегшує розгортання довірчих доменів (TD), які є апаратно ізольованими віртуальними машинами (VM), призначеними для захисту конфіденційних даних і додатків від несанкціонованого доступу. На рис. 2 показана архітектура Intel TDX, де показано, що все сек'юрне програмне забезбечення розташовано в TD. З хардверного боку основні компоненти підтримки адаптовані для підтримки TD. Так, наприклад, преривання в Advanced Programmable Interrupt Controller (APIC) розподіленні на trusted/untrusted та доданий контроль доступу в State Save Area для блокування доступу до станів, які належать до TD та аналогічного контролю page tables та VM control structures.

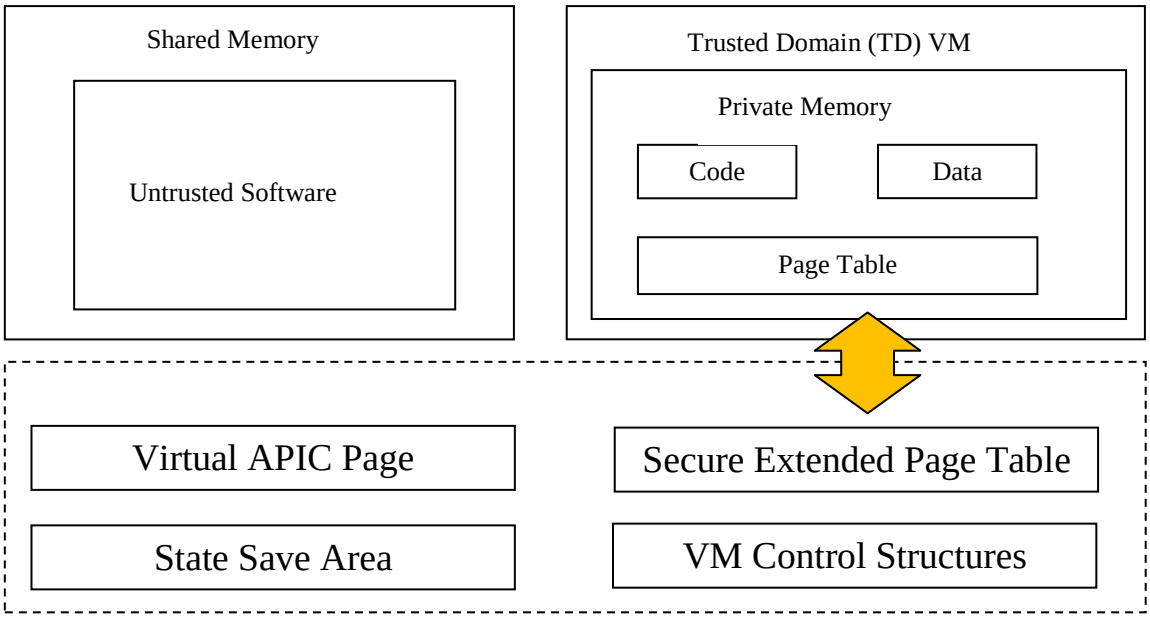

Рис. 2. Архітектура Intel TDX

Intel TDX включає також програмний модуль, який працює в новому режимі CPU, називається Secure Arbitration Mode (SEAM) та за концепцією дуже нагадує режим роботи secure-mode ARM TurstZone. Програмний модуль запускається на кожен менеджер віртуальних машин або virtual machine manager (VMM) і підтримує TD entry на кожну віртуальну машину. Модуль розміщується в зарезервованому просторі пам'яті, визначеному регістром діапазону SEAM (SEAMRR).

На рис. 3 показано обмін запитами між VMM та TD модулем.

Додана нова SEAMCALL інструкція в VMM для переводу CPU в режим операції SEAM-VMX-root та запуску TDX модуля. TDX модуль забезпечення інтерфейс для VMM для створення, видалення та виконання TD. Модуль Intel TDX виступає в якості надійного посередника, який допомагає впроваджувати політику безпеки, дії та необхідній доступ до даних для TD. Як частина створення TD, VMM надає сторінки пам'яті для TD-коду, даних та структур метаданих, пов'язаних з TD, таких як структура керування віртуальною машиною

Модуль Intel TDX призначений для виконання входу VM в SEAM-VMX, некореневої операції з використанням інструкцій VMRESUME і VMLAUNCH-VMX для виконання TD.

Intel TDX використовує шифрування пам'яті за допомогою Intel Total Memory Encryption (TME) [10], який шифрує всю пам'ять платформи одним ключем і надає можливість задати використання конкретного ключа для кожного TD.

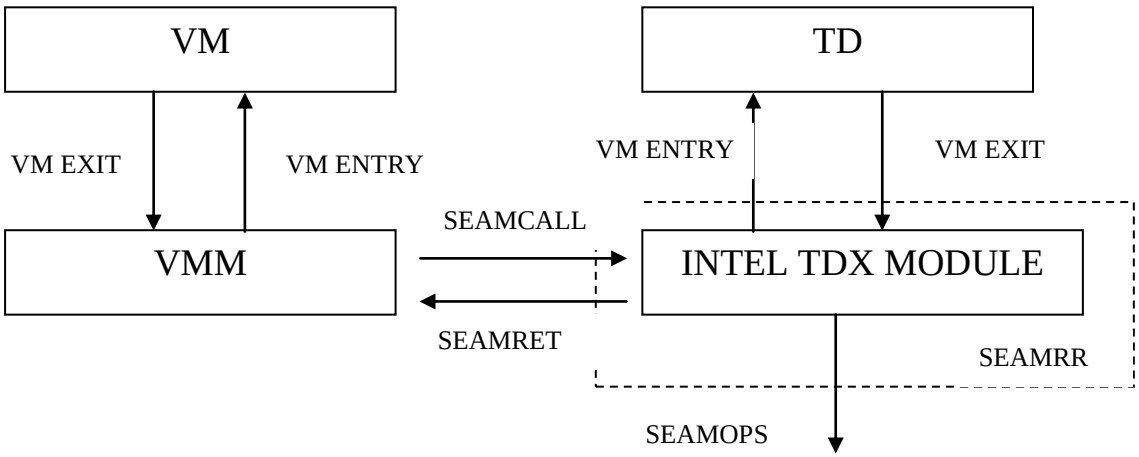

Рис. 3. Потоки в SEAM модулі

Режим Multi-Key TME (MK-TME) розширює TME для підтримки декількох ключів шифрування.

Операційна система (ОС) може використовувати можливості MK-TME в рідному або віртуалізованому середовищі. Якщо MK-TME сконфігуровано належним чином, то MK-TME доступна для кожної гостьової ОС у віртуалізованому середовищі, тому MK-TME може використовуватися як рідною, так і гостьовою ОС, як показано на рис. 4.

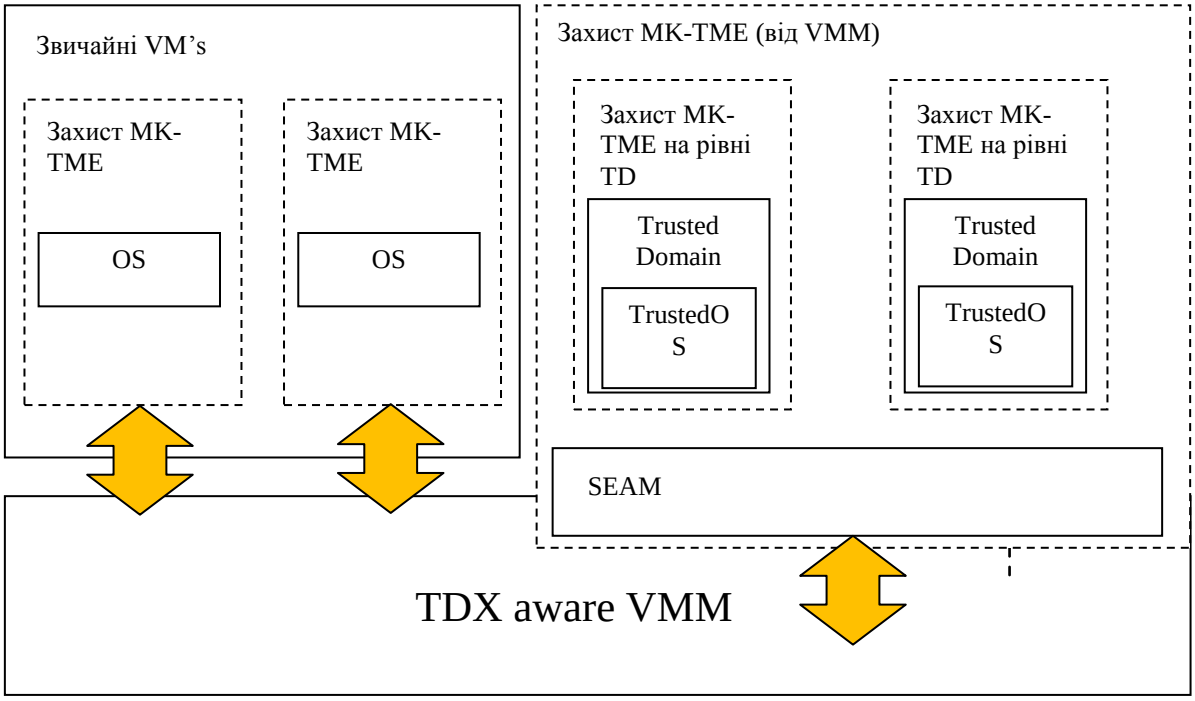

Рис. 4. Архітектура MK-TME

Таким чином, технологія Intel Trust Domain Extensions (Intel TDX) включає описані вище апаратно-програмні розширення до стандартної VT-d/VT-x та MK-TME, які разом утворюють новий вид середовища для віртуальної машини (virtual machine guest), яке називається Trust Domain (TD). TD виконується в CPU у режимі, який захищає конфіденційність змісту пам'яті та стану додатків TD в CPU від іншого програмного забезбечення (інших VM's) та від VMM.

Основні відмінності між стандартною технологією Virtual Machine Extension (VMX) та Intel TDX відмічені в табл. 1.

Таблиця 1

Порівняння технологій Virtual Machine Extension (VMX) та Intel TDX

Технологія	**Доступ до віртуальної машини**	**Переключення між станами CPU. Операції State Save & Restore**	**Управління**
VMX (VT-d/VT)	VMM має повний доступ	VMM SW виконує VMX переключення (наприклад регистри загального призначення)	VMM має багатий набір елементів керування для взаємодії з VM для того, щоб скасувати привілеї VM
TDX	VMM не має повного доступа, TD може надати доступ, якщо забажає	керуються модулем Intel TDX в режимі безпечного арбітражу (SEAM)	VMM має обмежений набір контролю для управління ресурсами

Архітектура на базі Intel TDX з запуском OP-TEE в окремій TD

Запропоноване в роботі рішення (див. рис. 5) базується на ізоляції OP-TEE в окремій TD. Рішення базується тільки на використанні в якості хостової операційної OS Linux або Android. Тому у якості системи віртуалізації використовується Kernel-based Virtual Machine (KVM).

Для стандартної реалізації OP-TEE з відкритим кодом існує реалізація QEMU для платформ ARM TrustZone, яка легко інтегрується і запускається в середовищі KVM. Таким чином ми можемо запустити OP-TEE/QEMU/KVM як TD.

Для комунікації між клієнтськими додатками (Client Application’s) операційної системи хоста в OP-TEE був доданий VIRTIO драйвер. На стороні хоста, оскільки optee-драйвер працює в ядрі Linux, надсилання та отримання повідомлень перекривається модулем vhost-vsock, як показано на рис. 5.

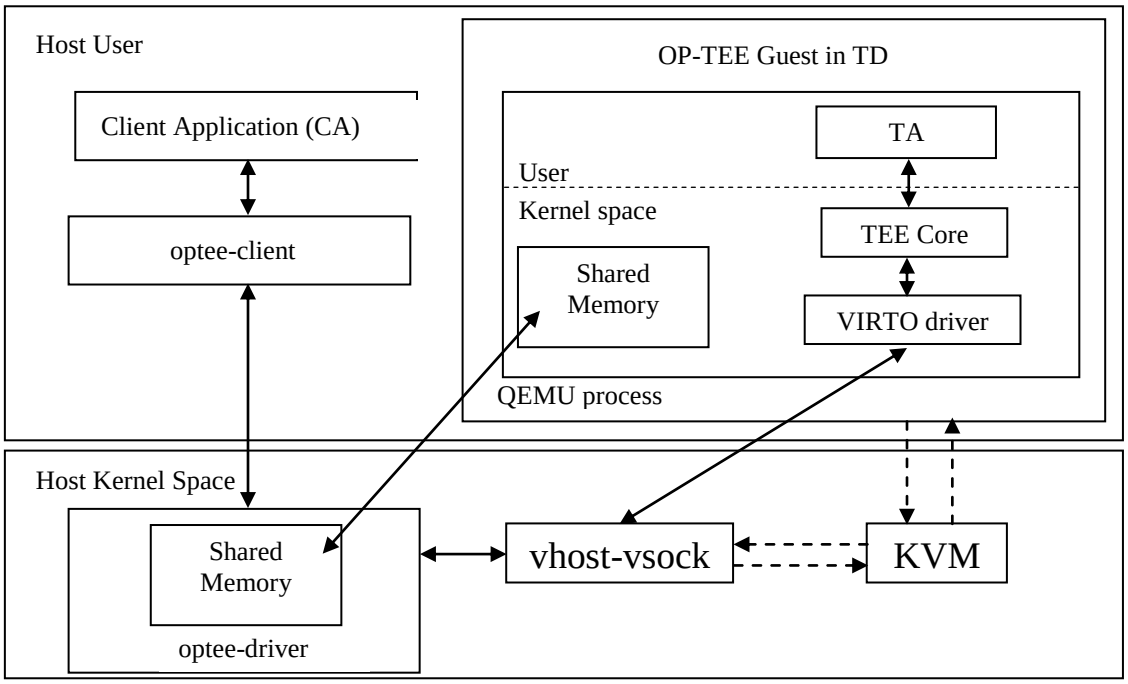

Рис. 5. Архітектура OP-TEE в контексті технології Intel TDX

Для передачі великих обсягів інформаціїї між Normal та Secure World використовується shared memory. У KVM немає спеціальної конфігурації Extended Page Tables (EPT) для забезпечення спільного використання пам'яті між хостом та OP-TEE. Для вирішення цієї проблеми виділяються два блоки пам'яті з однаковим розміром в optee-driver і OP-TEE відповідно. Копія пам'яті на основі повідомлень VIRTIO синхронізується між цими двома блоками «спільної» пам'яті.

Інтеграція OP-TEE для Intel x86 з використанням Intel TDX була виконана з використанням таких компонентів: Intel Xeon Bronze 3508U Processor; Normal World OS: Ubuntu LTS 24.04.1; OP-TEE 4.3.0.

Висновки

Запропонований варіант інтеграції фреймворку OP-TEE на Intel x86 з використанням Intel Trust Domain Extensions. Така архітектура дозволяє будувати системи високого рівня захисту (банківські/фінансові та інші), які повністю захищені від несанкціонованого доступу до даних. OP-TEE фреймворк забезпечує захист на програмному рівні, ізолюючи працю з конфіденційними даними в окрему операційну систему (Secure World OS) з обмеженим доступом. Trust Domain Extensions забезпечує захист даних на апаратному рівні завдяки розміщенню Secure World OS в повністю зашифрованій пам'яті.

OP-TEE фреймворк первинно розроблений для ARM платформ, але запропоноване рішення дозволяє використовувати OP-TEE для захисту конфіденційних даних на Intel x86 платформах без будь-яких змін у коді.

Запропонований варіант дає більше модульності та забезпечує більш легке портування на інші платформи та легке оновлення компонентів. Наприклад, Secure World VM може оновлюватися окремо від Normal World VM.

Список літератури:

1. ARM Security Technology, Building a Secure System using TrustZone, ARM, Technology Copyright © 2005-2009 ARM Limited. All rights reserved. PRD29-GENC-009492C.
2. TrustZone Explained: Architectural Features and Use Cases.
3. GlobalPlatform // TEE System Architecture Version 1.2 (Nov 2018), GPD SPE 009.
4. Intel® Processor and Intel® Core™ i3 N-Series, Datasheet. Vol. 1 of 2. https://edc.intel.com/content/www/us/en/design/products/platforms/processor-and-core-i3-n-series-datasheet-volume-1-of-2/001/intel-virtualization-technology-intel-vt-for-intel-64-and-intel-architecture-int/
5. Intel Virtualization Technology for Directed I/O Architecture Specification, March 2023, Revision 4.1
6. Arshad Nehal, Priyanka Ahlawat Securing IoT applications with OP-TEE from hardware level OS // 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA) 10.1109/ICECA.2019.8822040.
7. Kickstart Embedded. OP-TEE: What a Beginner Needs to Know. Sep. 13, 2022. [Online]. Available: https://kickstartembedded.com/2022/09/13/op-tee-part-1-what-a-beginner-needs-to-know/.
8. Intel Trust Domain Extensions, White Paper, 0720/RR/MESH/PDF 343961-003US, https://cdrdv2.intel.com/v1/dl/getContent/690419
9. Intel, "Intel Supervisor Mode Execution Protection (SMEP) Datasheet," [Online]. Available: https://edc.intel.com/content/www/us/en/design/products/platforms/processor-and-core-i3-n-series-datasheet-volume-1-of-2/001/intel-supervisor-mode-execution-protection-smep/.
10. Intel TDX Virtual Firmware Design Guide, Document Number: 344991-004US, Intel Corp, December 2023
11. Шулік П. В., Федюшин О.І. Організація довіренного середовища виконання з використанням QEMU та TRUST DOMAIN EXTENSIONS від INTEL // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 15-ї міжнар. наук.-техн. конф., 24-25 квітня 2025р., м. Баку, м. Харків, м. Жиліна : [у 3 т.]. Т. 3 . Харків : Impress, 2025. С. 97. Doi: https://doi.org/10.32620/ICT.25.t3.
12. Шулік П. В. Використання віртуальних машин для організації захисту інформації на платформах INTEL // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 15-ї міжнар. наук.-техн. конф., 24-25 квітня 2025р., м. Баку, м. Харків, м. Жиліна : [у 3 т.]. Т. 3. Харків : Impress, 2025. С. 98. Doi:https://doi.org/10.32620/ICT.25.t3.

Надійшла до редколегії 07.10.2025

Відомості про авторів:

Шулік Павло Вікторович – канд. техн. наук, ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки; Україна; e-mail: pavlo.shulik@nure.ua; ORCID: https://orcid.org/0009-0004-6200-2172

Балагура Дмитро Сергійович – канд. техн. наук, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Харківський національний університет радіоелектроніки; Україна; e-mail: dmytro.balahura@nure.ua; ORCID: https://orcid.org/0000-0002-6327-6405

Просолов Владислав Валерійович – аспірант кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Україна; e–mail: vladyslav.prosolov@nure.ua; ORCID: https://orcid.org/0009-0002-1276-4828

В'юхін Даніїл Олександрович – ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Харківський національний університет радіоелектроніки; Україна; e-mail: daniil.viukhin@nure.ua; ORCID: https://orcid.org/0009-0009-8442-9587