УДК 004.4

Д.Р. Яценко, В.М. Леськів, Н.С. Луцик докт. філос.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МЕТОДИ ЗАХИСТУ ЦЕНТРАЛЬНИХ ПРОЦЕСОРІВ КОМП'ЮТЕРІВ ВІД АТАК

D.R. Yatsenko, V.M. Leskiv, N.S. Lutsyk Ph.D.

METHODS OF COMPUTER CENTRAL PROCESSORS PROTECTION AGAINST ATTACKS

Одним з основних складових комп'ютера є процесор, від якого залежить програмне керування всіма складовими системи, що впливає на ефективну роботу комп'ютера. При роботі процесор оперує важливими даними, витік котрих є неприпустимим [1]. Тому безпека процесора є першочерговою задачею захисту. Особливо це актуально для персональних робочих станцій, де можливий витік особистої інформації. Для організації безпеки даних використовуються системи захисту. Вони бувають апаратними, або ж як у випадку з вразливостями Meltdown/Spectre, програмними [2].

Для захисту системи від вразливостей Meltdown/Spectre, виробники BIOS та операційних систем створили програмні версії систем захисту. Варто зазначити, що апаратна система захисту присутня лише в комп'ютерних системах на базі процесорів 2020 лінійного року. Основна проблема програмних систем захисту, це вплив на швидкодію процесора і системи в цілому [3, 4].

Дослідження впливу існуючих програмних засобів захисту центральних процесорів на швидкодію дасть відповідь наскільки критичний вплив цих засобів. Дослідження буде проводитися в ігрових застосунках (для отримання середніх значень та 1%/0.1% fps) та бенчмарках, а саме - Cinebanch r20 (кількість балів) та X 265 (час перекодування відеофайлу) із використанням різних версій BIOS та Windows [5].

Це дозволить визначити які версії програмних засобів захисту типу BIOS та Windows використовувати, щоб зменшити негативний вплив програмних систем захисту на робочу станцію.

Література

1. Tanenbaum A.S., Austin T. Structured Computer Organization. Pearson, 2013. 775p.
2. База даних загальновідомих вразливостей інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: https://cve.mitre.org/.
3. Kocher P., Horn J., Fogh A., Genkin D., Gruss D., Haas W., Hamburg M., Lipp M., Mangard S., Prescher T., Schwarz M., Yarom Y. Spectre Attacks: Exploiting Speculative Execution. San Francisco, California, 2019. 19p.
4. Lipp M., Schwarz M., Gruss D., Prescher T.,Haas W., Fogh A., Horn J., Mangard S.,Kocher P., Genkin D.,, Yarom Y., Hamburg M. Meltdown: Reading Kernel Memory from User Space. San Francisco, California, 2019. 18p.
5. Засоби тестування процесору та системи [Електронний ресурс] – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/computer-stress-test-software/.