Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем та мереж
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: Методи захисту центральних процесорів комп'ютерів від атак

Виконав: студент 6 курсу, групи Сім-61
спеціальності 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

(підпис) (прізвище та ініціали)

Керівник (підпис) Луцик Н.С. (прізвище та ініціали)
Нормоконтроль (підпис) Тиш Є.В. (прізвище та ініціали)
Завідувач кафедри (підпис) Осухівська Г.М. (прізвище та ініціали)
Рецензент (підпис) Михалик Д.М. (прізвище та ініціали)

Тернопіль
2020

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет Факультет комп'ютерно-інформаційних систем та мереж
(повна назва факультету)

Кафедра Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Осухівська Г.М.
(підпис) (прізвище та ініціали)
« 01 » 10 2020 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

студенту Яценку Дмитру Романовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи захисту центральних процесорів комп'ютерів від атак

Керівник роботи Луцик Надія Степанівна, доктор філю.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « *28* » *вересня* 2020 року № *4/7-687*

2. Термін подання студентом завершеної роботи 15 грудня 2020

3. Вихідні дані до роботи
Затверджена тема кваліфікаційної роботи магістра. Наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Було розглянуто саму суть вразливостей, дослідженовразливості процесорів Intel та AMD, проведено аналіз існуючих систем захисту. Докладно розглянуто вразливості Spectre та Meltdown та способи їх виявлення. Проведено тестування продуктивності системи з вимкненими та увімкненими заплатками вразливостей Spectr та Meltdown, та в залежності від версій BIOS та Windows.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Слайди до доповіді за темою кваліфікаційної роботи магістра

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека в надзвичайних	Стадник І. Я., проф.		
Охорона праці	Осухівська Г.М., доц.		

7. Дата видачі завдання 01.10.2020

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Затвердження теми кваліфікаційної роботи магістра	28.09.2020	виконав
2	Аналіз літературних джерел	29.09.20.-15.10.20	виконав
3	Обґрунтування актуальності досліджень	15.10.-21.10.20	виконав
4	Аналіз предмета дослідження та предметної області	21.10.-30.10.20	виконав
5	Проведення дослідження методів та засобів аналітичного опрацювання даних	30.10.-05.11.20	виконав
6	Оформлення розділу «Аналіз існуючих методів та засобів захисту центральних процесорів від атак»	05.11.-12.11.20	виконав
7	Оформлення розділу «Вибір оптимальних методів та засобів захисту центральних процесорів від атак»	12.11.-22.11.20	виконав
8	Оформлення розділу «Результати дослідження впливу процесорних заплаток на швидкодію компютера»	22.11.-10.12.20	виконав
9	Оформлення розділу «Охорона праці та безпека в надзвичайних ситуаціях»	26.11.-12.12.20	виконав
10	Нормоконтроль	13.12.2020	виконав
11	Попередній захист роботи	15.12.2020	виконав
12	Захист кваліфікаційної роботи магістра	24.12.2020	

Студент _____ Яценко Д.Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Луцик Н.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи захисту центральних процесорів комп’ютерів від атак // Кваліфікаційна робота // Яценко Дмитро Романович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, група СІм-61 // Тернопіль, 2020 // с. –70, рис. – 32, табл. -12, аркушів А1 - 8, додат. –1, бібліогр. –17.

Ключові слова: системи захисту, заплатки, вразливості.

Мета роботи полягає у дослідженню методів захисту центральних процесорів комп’ютерів від атак.

Було розглянуто сама суть вразливостей, досліджено вразливості процесорів Intel та AMD. Проведено аналіз існуючих методів захисту та їх вплив на продуктивність комп’ютерної системи.

У роботі розглянуто детально вразливості Meltdown та Spectre та, показано механізм виявлення вразливостей в системі. Розглянуто програми для тестування швидкодії системи.

Проведено тестування продуктивності комп’ютерної системи з вимкненими та увімкненими системами захисту від процесорних вразливостей в три етапи. Перший система без змін, другий оновлена система, третій система без оновлень. Це дало змогу обрати найкращий варіант захисту центральних процесорів комп’ютерів від атак.

ANNOTATION

Methods of computer central processors protection against attacks // Master thesis // Yatsenko Dmytro Romanovich // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information System and Software Engineering, СІм-61 group // Ternopil, 2020 // p. – 70, fig. - 32, tab. - 12, sheets A1 - 8, add. - 1, bibliography. - 17.

Key words: protection systems, security patches, vulnerability.

The purpose of the work is to investigate methods of computer central processors protection against attacks.

In the thesis was considered vulnerability concept, investigated Intel and AMD vulnerabilities. Conducted an analysis of existing methods of protection and their impact on the performance of a computer system. Defined the tasks of qualification research.

Meltdown and Specter vulnerabilities are considered in detail and the mechanism of detecting vulnerabilities in the system is shown. Programs for testing system performance are considered.

Performance testing of a computer system with disabled and enabled systems for protection against processor vulnerabilities was performed in three stages. The first system without changes, the second updated system, the third system without updates. Investigation let us know, which specification of protection systems, are better for protecting computer processor against attacks.

ЗМІСТ

ВСТУП

Актуальність теми роботи. Методи захисту центральних процесорів комп'ютерів від атак є актуальною та дуже важливою темою, так як вразливості центральних процесорів є вкрай поширеною проблемою.

Процесор є основною складовою комп'ютерної системи, тому що він виконує більшість критичних обчислень, які потрібні для роботи комп'ютера. Він проводить програмне керування всіма складовими системи. Варто зазначити, що всі важливі данні проходять через процесор, що робить його можливим місцем витоку інформації [1].

Раніше вразливості процесорів типу Meltdown/Spectre вважалися лише міфом, але дослідники проекту Google Project Zero показали, що ці недоліки архітектури центральних процесорів є реальними. Перелік атак на центральний процесор є величезним. Вразливості, які розглядаються в даній роботі працюють за принципом витоком інформації через бічний канал [2].

Звичайно вендори та монополізуючі виробники операційних систем випустили програмні заплатки, які вирішують проблему безпеки в процесорах, але з'явилась нова проблема - втрата швидкодії. Самі програмні заплатки захищають систему від атак на процесор, але в певних задачах можуть викликати сповільнення його роботи.

Тому дослідження впливу різних програмних заплаток на швидкодію комп'ютера є актуальною та потрібною роботою на сьогоднішній день, адже більшість користувачів використовують моделі процесорів із програмними заплатками, а не архітектурними, як в нових моделях. Таким чином одержані результати дадуть відповідь, який з засобів захисту процесора від вразливостей типу Meltdown/ Spectre чи версія системи на робочій машині завдає найменші втрати в швидкодії.

Мета і задачі дослідження. Метою роботи є дослідження існуючих методів та засобів захисту центральних процесорів комп'ютерів від атак та їх безпосередній вплив на швидкодію системи. Дослідити особливості сторонніх

каналів витоку інформації у сучасних процесора при різних версія засобів захисту. Опрацювати способи захисту процесора від витоку інформації. Порівняти вплив на швидкодію комп’ютера із різними версіями способів захисту запропонованих виробником. Виокремити найкращий набір із системних засобів, які даватимуть захист комп’ютерного процесора від атак та не впливатимуть на продуктивність робочої системи.

Для досягнення вказаної мети в роботі поставлено наступні задачі:

- аналіз наукових публікацій щодо виявлення існуючих методів та засобів захисту центральних процесорів від атак;
- дослідження способів нівелювання вразливостей процесора;
- отримання значень швидкодії системи без застосованих засобів захисту;
- проведення досліджень в ігрових застосунках та бенчмарках, а саме - Cinebanch r20 та X 265 із використанням різних версій BIOS та Windows;
- опрацювання результатів тестування для вибору кращого набору засобів захисту процесора із найменшим впливом на швидкодію системи.

Об'єкт дослідження - процес захисту комп'ютерних процесорів від атак

Предмет дослідження - методи та засоби захисту комп'ютерних процесорів від атак

Методи дослідження. Для вирішення поставлених задач використано наступні методи: аналіз та узагальнення - при проведенні аналізу існуючих методів та засобів захисту комп'ютерних процесорів від атак; порівняння - при виборі методів і засобів захисту процесорів; експеримент та візуалізація - для апробації запропонованих методів та засобів.

Практичне значення одержаних результатів. Отримані результати дають відповідь на питання, чи спричиняють заплатки втрату швидкодії процесора та в яких саме сферах, що дає змогу вибрати набір версій програмних засобів типу BIOS та Windows, які забезпечують високий захист комп'ютерних процесорів та найменший спад продуктивності комп'ютерних систем.

Публікації. Результати дослідження апробовано на IX Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі

сучасних технологій» м. Тернопіль 25-26 листопада 2020 року та VIII науково-технічна конференція «Інформаційні моделі, системи та технології м. Тернопіль 9-10 грудня 2020 року.

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається із вступу, чотирьох розділів, висновків, списку використаних джерел та додатку. Обсяг роботи: пояснювальна записка – 69 аркуші формату А4, графічна частина – 8 аркушів формату А1.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ЦЕНТРАЛЬНИХ ПРОЦЕСОРІВ КОМП’ЮТЕРІВ ВІД АТАК

1.1. Загальні особливості вразливостей

Все більше можна побачити повідомлення про виявлення вразливостей в системах безпеки комп’ютерів. Для початку що таке вразливість, вразливість це відсутність засобів у системи протистояти реалізації конкретної загрози або ж набору загроз. Тобто, це певні недоліки в комп'ютерній системі, завдяки яким можна навмисно порушити її цілісність і викликати невідповідну роботу, або ж збій. Існує обширна класифікація вразливостей, тобто це не тільки вразливості центральних процесорів, які ми розглядаємо, а й інші:

- апаратні вразливості:
  а) вразливість до вологості;
  б) вразливість до пилу;
  в) вразливість до забруднення;
  г) вразливість до незахищеного зберігання.
- вразливості програмного забезпечення:
  а) критично мале тестування;
  б) відсутність або недостатня аудиторська перевірка;
  в) недолік проектування.
- мережеві вразливості:
  а) незахищені, відкриті лінії зв'язку;
  б) небезпечна архітектура мережі.
- вразливості людського фактору:
  а) неадекватний процес підбору персоналу;
  б) недостатнє поінформованість щодо безпеки.
- організаційні вразливості:
  а) відсутність планових перевірок;
  б) відсутність планів безперервності.

Як ми говорили раніше і бачимо на рис. 1.1 , є безліч причин, з яких може з’явитися вразливість, від людського фактору до недоліку системи.

Рис. 1.1. Аспекти вразливостей

Зазвичай вразливість дозволяє зловмиснику, тобто атакуючому «обдурити» застосунок — змусити його виконати певну дію, на яку у додатка не повинно бути прав чи дозволів. Це виконується шляхом впровадження довільно доступним чином в програму шкідливих даних або програмного коду в такі місця, що застосунок сприйме їх як «свої», тобто корінні. Деякі вразливості з'являються через недостатню або ж халатну перевірку даних, що застосовуються користувачем, і дозволяють інтегрувати в інтерпретований програмний код довільні команди (SQL-ін'єкції, XSS). Інші вразливості викликані значно більшими проблемами, такими як записом даних в буфер без необхідної перевірки його меж (переповнення буфера).

Отже, основними першопричинами вразливостей є:

- складність: об’ємні, складні системи примножують ймовірність можливих дефектів і ненавмисних точок доступу;
- публічність: використання загальнодоступного, відомого програмного коду, програмного забезпечення, операційних систем і/або апаратних комплектуючих збільшує можливість того, що зловмисник може дізнатись інформацію та інструменти, щоб використати прогалину в безпеці;

- зв'язок: фізичні з'єднання в системах, привілейовані дозволи, порти, протоколи, служби та час, на який вони є вільно доступними, збільшує можливу вразливість;
- слабкий контроль засобів входу, паролів: користувач використовує ненадійні, прості паролі, які можуть бути підібрані за допомогою простих засобів; користувач зберігає логін та пароль на комп'ютері, який і використовує для входу, на якому програма зловмисника може отримати доступ до даних; користувач незмінно використовує ті ж паролі між різними застосунками і веб-сайтами;
- фундаментальні проблеми дизайну операційної системи: дизайнер операційної системи для забезпечення роботи використовує неоптимальні політики керування «користувач — програма». Наприклад, операційні системи з можливостями щодо дозволу на отримання абсолютного доступу до системи комп'ютера для вибраної програми чи користувача. Дані недоліки операційної системи дають змогу вірусам і шкідливим застосункам виконувати команди з дозволами адміністратора;
- веб серфінг: декотрі сайти можуть містити в собі шкідливі шпигунські або рекламні застосунки, які можуть бути автоматично, без отримання дозволів, встановлені на комп'ютерну систему. Після відвідування цих веб-сайтів, комп'ютер може бути уражений і конфіденційна інформація буде збиратися без відома користувача і передаватися до сторонніх осіб;
- необмежений, все дозволений вхід користувача: застосунок припускає, що все, що вводить користувач є безпечним. Програми, які не виконують перевірки введення користувача, інколи спричиняють випадкове, безпосереднє виконання команд або операторів SQL (переповнення буфера, чи власне ін'єкції SQL) [3,4].

Як ми можемо бачити на рис.1.2 показано більш детально на які підгрупи поділяються можливі вразливості системи, але вже у сфері апаратно програмних вразливостей, не беручи до уваги людський фактор.

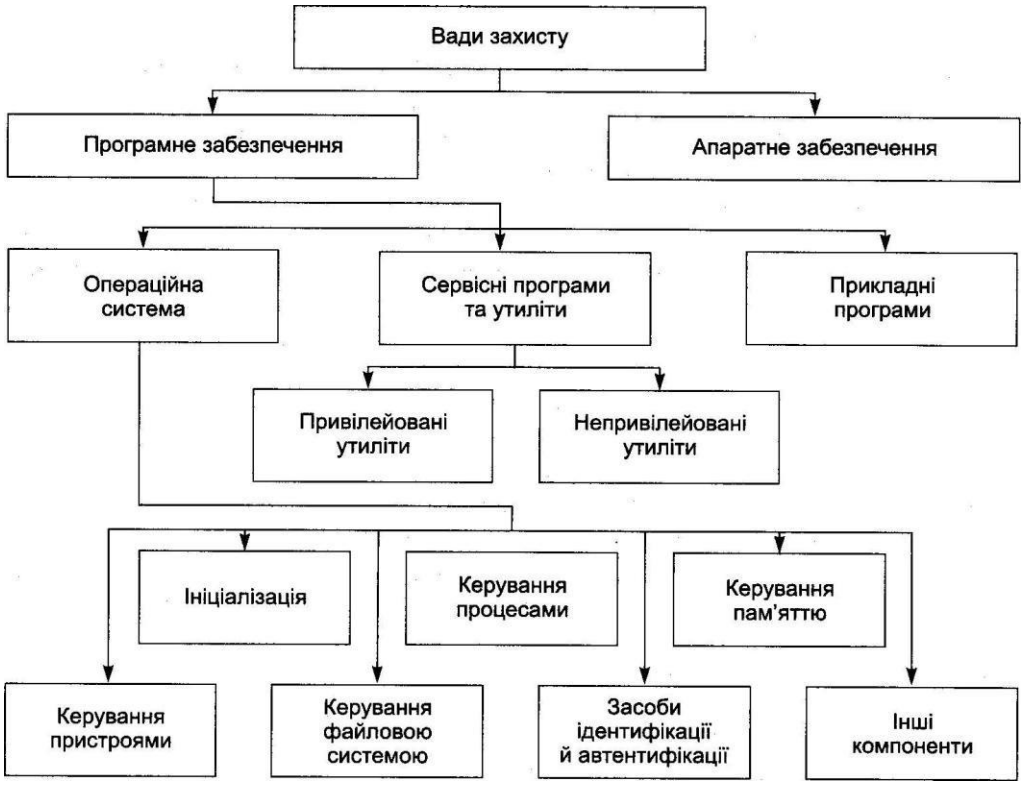

Рис.1.2 Класифікація вад захисту

Вплив від порушення безпеки рано чи пізно буде досить високим. Якщо IT-менеджери чи вище керівництво, або будь який працівник знають, що системи та програми, підпорядковані їм, чи є їх продуктом мають уразливості, і не виправляють нічого, щоб запобігти можливому IT-ризику, то це розглядається як серйозний проступок в багатьох світових законодавствах. Закон про захист персональних даних заставляє менеджерів діяти для зменшення впливу або ймовірності цього ризику безпеки. Тест на можливе проникнення є однією з багатьох форм перевірки слабкості і контрзаходів, які діють в організації: «білий» хакер робить спроби атак на IT-активи організації, для отримання інформації наскільки є надійною безпека даної організації. Правильним способом професійного керування IT-ризиком є використання системи управління інформаційною безпекою за стандартами ISO / IEC 27002 та дотримування цих стандартів, у відповідності зі прийнятою стратегією безпеки, застосованою вищим керівництвом. Однією з основних концепцій IT-безпеки є принцип комплексного, повного, захисту, а саме створення ієрархічної системи захисту, яка може:

- виявити і випередити атаку;
- знайти зловмисників і переслідувати їх.

Система виявлення проникнень є одним з прикладів класу систем, що застосовуються саме для виявлення атак. Приблизні набори критеріїв, яким повинен відповідати комп'ютер, використовувана операційна система і застосунки з метою задоволення достатнього рівня безпеки вже розроблені, прикладами є ITSEC і критерії оцінки IT-безпеки [3,4].

Станом на 2018 рік процесорні вразливості сімейства Spectre наявні практично в усіх сучасних мікропроцесорах, а саме: у настільних комп’ютерах, ноутбуках, планшетах, смартфонах, тощо. Відомо про створення та успішне виконання демонстраційних атак на процесори виробництва Intel, AMD, та більшої частини сімейства ARM [2].

Вразливість також було знайдено і підтверджено практично в процесорах IBM Power: Power7+, Power8 та Power9, Fujitsu SPARC64 XII та SPARC64 X+. Існують відомості, що вразливість Spectre вдалось відтворити в процесорах сімейства Power6, навіть, якщо в них виконання команд конвеєром йде за чергою, але все ж спекулятивно. Вразливість також була виявлена в мікропроцесорах сімейства MIPS P5600 та P6600 [2].

Вразливість процесорів сімейства ARM фактично залежить від наявної версії архітектури та фактичної реалізації ядра кожним конкретним виробником. На разі виявлено та підтверджено наявність вразливості в процесорах з ядрами: Cortex-R7, Cortex-R8, Cortex-A8, Cortex-A9, Cortex-A15, Cortex-A17, Cortex-A57, Cortex-A72, Cortex-A73 та ARM Cortex-A75. Варто зазначити, що деякі смартфони і комп'ютери з простішими (переважно дешевшими) варіантами, в яких немає суперскалярності, відсутня ця вразливість. Для прикладу, всі відомі варіанти Raspberry Pi не уражені ані Meltdown, ані Spectre [2].

Уже станом на початок 2018 року було створено атаки із застосуванням вразливості Spectre між процесами на рівні користувача.

Реалізація вразливості Spectre більш складна ніж Meltdown, але й захист від неї також важчий.

Тим не менш, Spectre становить більшу загрозу хмарним обчисленням, бо в свою чергу, на відміну від Meltdown, може спонукати гіпервізор, тобто передачу даних гостьовій системі.

Проте найбільшою загрозою для звичайних користувачів виявився варіант CVE-2017-5753 (доступ за межі масиву), який досить легко застосовується скриптами JavaScript та спричиняє викрадення даних із веб-браузера користувача. Але є й добра новина, захист від нього є також найпростішим, без помітної втрати швидкодії і потрібно лише оновлення веб-браузера, з яким буде встановлено оновлення систем захисту.

1.2. Вразливості процесорів Intel та AMD

Найбільшу частину ринку комп'ютерних систем займають системи н базі процесорів Intel та AMD. У випадку вразливостей процесори Intel отримують лаври першості. Якщо ж взяти до уваги навіть вищезгадані, так би мовити найбільш відомі вразливості Meltdown та Spectre то процесори Intel уражені обома, а процесори AMD лише Spectre (беручи до уваги лише ці 2 вразливості). Також провівши своєрідний тест (який може бути не надто об'єктивним), якщо в пошуку на сайті CVE спробувати пошукати вразливості Intel їх показує 457, а при проведені повторного пошуку, але уже з AMD то вразливостей всього 40 [5].

Досить недавно було опубліковані дані про чергові вразливості, або ж особливості процесорів Intel. Спеціалісти з безпеки Марк Єрмолов та Максим Горячий із компанії Positive Technologies повідомили про цікаву систему Visualization of Internal Signals Architecture (VISA). Дана система дозволяє без будь-якого спеціального обладнання, тобто лише використовуючи засоби процесора, в реальному часі отримувати свого роду знімки роботи внутрішніх компонентів центрального процесора та отримувати індивідуальні сигнали [6].

Дослідники заспокоїли, що можна не панікувати, так як для використання цієї системи спостереження каналу потрібно використати складнішу вразливість для отримання всіх прав адміністратора.

Цікава користь від VISA для дослідників в тому, що вони тепер зможуть безпосередньо побачити найнижчий рівень роботи мікропроцесорів Intel. За словами науковців, дана технологія дає змогу получити доступ до внутрішньої шини процесора, що в свою чергу дозволить побачити читання та запис пам’яті, Використовуючи цю особливість, кожен може спробувати проаналізувати різні аспекти апаратної кібербезпеки.

Сама система VISA є частиною з декількох наборів прихованих та непублічних інструментів розробників під внутрішньою, загальною назвою Trace Hub. Інженери та відповідальні за проектування процесорів Intel використовують даний набір засобів для аналізу роботи нових, або уже готових чіпів та потоків даних [6].

Якщо ж взяти до уваги зловмисників, то система VISA їм не менш цікава, оскільки дає змогу ефективніше відшукувати вразливості. Дана система дає зловмисникам змогу отримувати інформацію безпосередньо з процесора.

Також стало відомо що процесори Intel стали жертвою нової вразливості Spoiler.

Spoiler - це вразливість безпеки на сучасних центральних процесорах, які використовують спекулятивне виконання. Він використовує побічні ефекти спекулятивного виконання для підвищення ефективності Rowhammer та інших пов'язаних з ними атак пам'яті і кешу. Згідно з повідомленнями, всі сучасні процесори Intel Core вразливі атаці станом на 2019 рік. Компанія AMD заявила, що її процесори не є вразливими.

Zombieload, RIDL & Fallout і Store-to-Leak Forwarding, відому як уразливості MDS. Вони достатньо серйозні, що власники ПК на базі Intel потребують негайного виправлення, що, на жаль, вплине на продуктивність - особливо в режимі багатопоточності. Однак власникам AMD пощастило. На

своєму сайті AMD заявив, що його чіпи захищені від проблем завдяки вбудованим перевіркам апаратного захисту.

Вразливість Spectre та супутня вразливість Meltdown (CVE-2017-5754) чинять свій зловмисний вплив за допомогою реалізації принципів спекулятивного виконання в сучасних процесорах.

Для збільшення швидкодії програм сучасні процесори і мікропроцесори загалом, можуть виконувати частину інструкцій позачергово, спираючись на конкретні припущення. Під час операції спекулятивного виконання процесор робить перевірку на припущення і якщо вони справджуються, то виконання продовжується. Але якщо ці припущення виявилися помилковими, то процес виконання буде зупинено і відбувається повернення до початкової, тобто вірної послідовності інструкцій. Проте, у певних випадках процес спекулятивного виконання має сторонні, не надто приємні ефекти, які не можна усунути під час повернення до звичної черговості інструкцій. Дані ефекти можуть призводити до витоку даних (так звані бічні, або сторонні канали інформації).

Тобто, якщо виконання застосунку залежить від даних у спільній, загальній пам'яті, то процесор може спробувати зробити деякі припущення про наступний перебіг подій і задля економії кількох сотень циклів відправити ці дані в кеш процесора попередньо. Якщо все ж таки припущення були хибними, то загалом швидкість виконання програм не змінюється, тобто вона виявляється такою ж, якби процесор опрацьовував інструкції за їх початковою чергою та залишався очікувати при звертаннях до оперативної пам'яті. Але, якщо ж припущення все таки були правильними, то виконання програм значно пришвидшується, через більш ефективне використання ресурсів системи. Завдяки уникненням простою процесора.

Якщо ж поглянути з сторони інформаційної безпеки, то спекулятивність має ймовірність для виникнення некоректного виконання програми. Розробники вважали раніше що, якщо процесор все ж таки автоматично повертається до початкового, а це є коректним станом, через хибні припущення, то дані помилки не спричиняють жодної загрози.

Вразливість Spectre заснована на примусі процесора до спекулятивного виконання послідовності інструкцій, виконання яких було б неможливим за звичної роботи програми. Розробники назвали ці інструкції посередніми, або ж проміжними (transient instructions). За допомогою вдалого підбору посередніх інструкцій атакуюча сторона здатна спричинити виток із пам'яті комп’ютера жертви завдяки сторонньому каналу.

Вразливість Spectre має кілька можливих алгоритмів реалізації:

- якщо ввести в оману модуль передбачення переходів, щоб він спекулятивно виконав захищений код на комп’ютері жертви із бічним каналом. Дія цього варіанту заключається між процесами навіть більше, між гіперпотоками, в середині одного мікропроцесора та може бути використано для спроби атаки на ядро операційної системи чи навіть гіпервізора віртуальної машини. Ця вразливість за загальною системою класифікації CVE має код CVE-2017-5715;

- змусити мікропроцесор спекулятивно завантажити данні за межами масиву. Даний різновид діє в межах лише одного процесу. Ця вразливість також має код CVE-2017-5753.

Наступний різновид вразливості Spectre є читання за межами масиву (CVE-2017-5753)

Ця вразливість є спрощеною версією Meltdown (або ж навпаки, Meltdown є більш серйозним варіантом цієї вразливості).

Вразливість CVE-2017-5753 заснована на тому, щоб обдурити модуль передбачення переходів, для примусового спекулятивного зчитування даних за межами масиву. Результатом цих дій, зловмисник може зчитати всі дані в межах конкретного процесу (основна відмінність спрощеного варіанту від Meltdown , що даний варіант позбавлений виходу у зони з вищим рівнем захисту). Під час дослідження цей варіант вразливості отримав назву: «Атака із використанням хибного передбачення умовного переходу», що мовою оригіналу Exploiting Conditional Branch Misprediction.

Щоб успішно реалізувати дану вразливість, зловмисник повинен заставити жертву виконати певну послідовність інструкцій, конкретно в просторі процесу, на який здійснюється атака. В такому випадку можуть бути чи вже наявні в коді, процесу інструкції, чи ж атакований процес буде виконувати дані інструкції у JiT-компіляторі.

Дослідження спеціалістів змогло показати приклади успішних атак, в яких використовували цю вразливість проти ядра Linux, через систему eBPF. Також успішні атаки були на сучасні веб-браузери які виконують сценарій JavaScript із використанням JiT-компіляції. Окрім того, було представлено найпростішу програму-демонстратор, яка була написана мовою C. Її суть заключається в зчитуванні «прихованих» даних в межах власного процесу.

Атаку із використанням даної уразливості було показана на основі функції, сторонній канал в якій був створений нижче показаним кодом:

```
if (x < array1_size)
     y = array2[array1[x] * 256];
```

Умовний перехід по суті гарантує, що звернення до array1 буде завжди правильним і не буде виходи за межі конкретного масиву. Але, при спекулятивному виконанні цих команд процесор може виконати дані інструкції в конвеєрі, що призведе до того, що він залишить сторонній канал у вигляді кешованих фрагментів, вищеописаного масиву array2. В даному прикладі значення змінної x визначатиме адресу в пам'яті, яку буде зчитано зловмисником. Саме значення комірки пам'яті, що буде знаходитись за адресою array1 + x буде відновлено за допомогою інформації про кешований фрагмент масиву array2.

Ще одна вразливість із даної групи це маніпуляція модулем передбачення переходів (CVE-2017-5715)

Під час досліджень на тему сімейства цих вразливостей також був представлена інша вразливість, так звана маніпуляція непрямими переходами, або мовою оригіналу це Branch Target Injection. Вразливість знаходиться

безпосередньо в модулі передбачення переходів і її можна використати для атаки між різнорівневими процесами.

Якщо ж порівнювати із прямим переходом, то при непрямому переході потрібна адреса переходу наперед не відома, а повинна отримуватись із регістра, комірки пам'яті, або ж обчислена іншим способом. Якщо процес отримання необхідної адреси для переходу займатиме надто багато часу, то модуль передбачення переходів ймовірно вирішить спекулятивно виконати перехід за хибною адресою. Зловмисник може змусити модуль передбачення переходів виконувати операції по переходу для спекулятивного виконання за завідома хибними адресами, які ж сам і визначатиме. Тобто, за цих умов буде спекулятивно виконано інструкції, виконання яких за нормальних умов ніколи б не було. Дана ситуація спричиняє значну вразливість, при умові, що спекулятивне виконання цих інструкцій залишає помітні побічні ефекти [7,8].

Команда дослідників університету Прінстона, за участі компанії NVIDIA в лютому 2018 отримали нові, раніше не відомі способи атак з використанням вразливостей Meltdown/Spectre. Було отримано назви MeltdownPrime і SpectrePrime відповідно. Якщо ж порівнювати з уже відомими методами, то дані відрізняються способом, за яким інформація відтворюватиметься із процесорного кешу [9].

Що MeltdownPrime, що SpectrePrime, побудовані на основі роботи з двома ядрами багатоядерного процесора. Вони використовують певні особливості роботи протоколу про узгодження вмісту кеша для різних ядер CPU. Якщо ми згадаємо вищеописані атаки, то основною вразливістю їм служило відновлення вмісту кеша на основі принципу FLUSH + RELOAD, але в даних методах застосований принцип «Prime and Probe».

Варто зазначити, що сучасні програмні заплатки від виробників забезпечують захист і від нових атак.

Спеціаліст з Linux-сайту Phoronix провела тести, які показують, що патчі можуть суттєво вплинути на продуктивність. Машини Intel зазнали втрат у вигляді 16 відсотків продуктивності в середньому з встановленими новими

оновленнями і ввімкненим багатопотоком, у порівнянні з 3-відсотковим падінням на чіпах AMD [9].

Що ще гірше, Apple і Google радили користувачам Intel повністю відключити багатопоточність на чіпах Intel, якщо вони дійсно хочуть бути безпечними. Це може призвести до зниження продуктивності на 40-50%, залежно від програми. Знову ж таки, чіпи AMD не повинні бути вразливі для нових помилок, і немає необхідності відключати багатопоточність.

1.3. Системи захисту комп’ютерних процесорів від атак

Існує велика кількість систем та засобів для захисту комп’ютерних процесорів від атак. Загалом системи захисту поділяють на програмні та апаратні системи захисту, як зрозуміло з назви вони діють у своїх конкретних областях, але часто перетинаються. Одною з основних груп таких засобів є превентивні засоби захисту комп’ютерних систем. Дані системи засновані для попередження атаки, для ефективного подальшого захисту від неї. Тобто це певний набір засобів чи порад який повинен підвищити захищеність системи.

Якщо взяти до уваги апаратні засоби захисту то це можуть бути, як використання більш захищених, спеціалізованих комп’ютерних систем, системи шифрування даних, захищені канали зв’язку. Тобто канали зв’язку, доступу до яких не має ніхто окрім авторизованих користувачів системи, дані засоби часто використовують в уряді для зв’язку високопосадовців із доступом до державної таємниці. В більшості своїй апаратні засоби безпеки використовують в галузях, де безпека передачі цілісності і конфіденційності інформації є першочерговою. Як було зазначено вище, дані засоби використовують не тільки в уряді, а й в інших сферах, таких як армія і оборона, авіація чи залізничне сполучення.

Також є програмні засоби захисту комп’ютерних систем і процесорів вцілому, хоч вони також використовуються у різних сферах, але все ж є більш розповсюдженими в користувацьких комп’ютерних системах. Загалом це системні та прикладні застосунки, які призначені для захисту інформації на

пристрої, яка передається чи зберігається безпосередньо на потужностях пристрою. Переважно програмні засоби захисту інформації використовують для контролю і безпосереднього виконання процесів ідентифікації й автентифікації користувачів. Також програмні засоби використовують для розмежування доступу користувачів комп'ютерної системи до інформаційної мережі. Одним з найбільш розповсюджених засобів захисту є парольний захист і перевірка повноважень. Також як програмний засіб можна використовувати шифрування інформації на пристрої. Ще одним важливим напрямком захисту є контроль і захист від несанкціонованих змін інформації, її зчитування та копіювання.

Основна увага розробників і в свою чергу користувачів комп'ютерних систем сьогодні приділена саме програмним засобам захисту від несанкціонованого проникнення в інформаційні ресурси користувача і особливо до проблем мережі Інтернет. Методи захисту бувають різні окрім описаних вище ще й організаційні, технологічні чи ті ж апаратні, але є один нюанс, вони, в більшості випадків, не можуть бути здійснені без застосування програмної складової. Варто зазначити, що основними недоліками програмних засобів захисту інформації є саме використання наявних ресурсів системи, що в свою чергу призводить до втрат її швидкодії, не виключена й можливість обходу такого захисту, тобто методи атаки на систему також розвиваються, як і захисту.

Найбільш розповсюдженими прикладами саме програмних засобів IT-захисту є:

- система моніторингу і керування доступом;
- керування записами;
- брандмауер, або ж мережевий екран;
- система моніторингу та виявлення вторгнень;
- програмні засоби для шифрування;
- пісочниця.

Система моніторингу і керування доступом це комплекс апаратно програмних засобів і покликаний до контролю доступу користувачів до самих

комп’ютерних систем. Тобто це система захисту не від мережевих атак на систему, швидше вона запобігає контактним атакам чи можливим помилкових дій людей, які не мають доступу до системи.

Брандмауер або ж фаєрвол це грубо кажучи стіна, між різними рівнями безпеки середовищ, яка за певними, налаштовуваними правилами може пропускати, або ж відхиляти з’єднання та передачу файлів. Сам брандмауер може бути також як у вигляді окремого приладу (маршрутизатора чи роутера), або ж програмним забезпеченням.

Система моніторингу та виявлення вторгнень відома як Intrusion Detection System, скорочено IDS, це переважно програмний або апаратний засіб, основна ціль якого це виявлення фактів несанкціонованого проникнення в комп'ютерну систему чи мережу. Також дана система виявляє факти несанкціонованого управління комп’ютерною системою. Вся активність шкідливого програмного забезпечення чи відомості про порушення стандартної роботи системи централізовано збирається системою. Система виявлення вторгнень обробляє дані отримані від великої кількості джерел і застосовує методи фільтрації тривоги для ефективного розпізнавання несанкціонованої активності від можливого хибного спрацювання тривоги.

Також існує різновид системи виявлення вторгнень які можуть виявити початковий стан атаки на мережу, що варто зазначити, що деякі з них можуть виявляти нові, раніше не відомі атаки. Даний різновид має назву системи запобігання вторгненням або ж Intrusion Prevention System, скорочено IPS. Дана система IPS не здійснює лише оповіщення, але й має змогу здійснювати різні заходи, які будуть спрямовані на саме блокування атаки, тобто, розрив з'єднання між системою і зловмисником чи виконання певного скрипту, який був заздалегідь створений адміністратором. В прикладних рішеннях переважно програмно-апаратні рішення складаються із обох типів систем. Наглядну різницю між IPS та IDS показано на рис.1.3.

Хоч існує не один, а декілька типів IDS, які за розміром можуть бути від окремих комп'ютерів до повноцінних, великих мереж. Одними із

найпопулярнішими класифікаціями є системи моніторингу вторгнень у мережу тобто network intrusion detection systems, або ж скорочено NIDS. Також поширені системи виявлення вторгнень які засновані на аналізі хостів HIDS. Якщо ж для прикладу, то HIDS буде система відслідковування важливих файлів операційної системи, а прикладом NIDS це вже система аналізу вхідного мережевого трафіку. Загалом, саму IDS також можна класифікувати за методами виявлення загроз: найбільш відомим є виявлення на основі сигнатур (розпізнавання поганих шаблонів, таких як шкідливе ПЗ) та виявлення аномалій (виявлення відхилень від «правильного» трафіку, часто за допомогою машинного навчання).

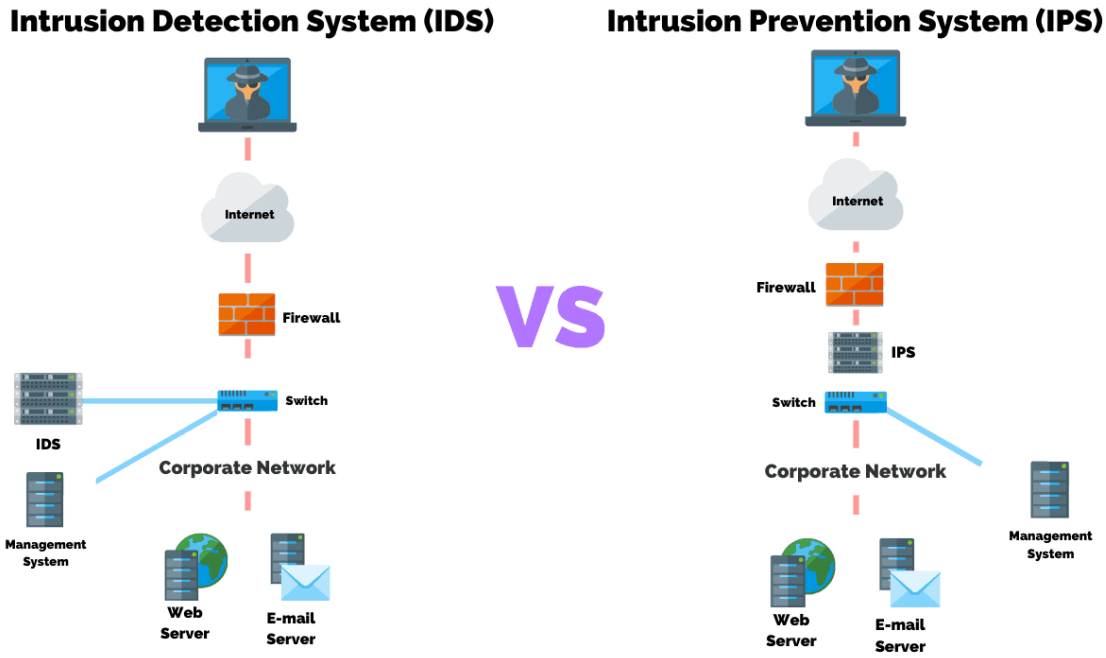

Рис.1.3. Різниця між IPS та IDS

Пісочниця, це переважно жорстко контрольований набір засобів, це місце на жорстокому диску комп'ютера та/або оперативній пам'яті, які використовують не для захисту системи від зовнішніх атак, а для виконання гостьової програми. Доступ до мережі передавання даних, повний чи частковий доступ до системних ресурсів операційної системи, також пряме отримання інформації з засобів введення переважно повністю або частково емулюються,

або сильно ізолюються, обмежуються. Пісочниці є наглядним прикладом віртуалізації.

Підвищена безпека для виконання коду в пісочниці надає захист системи від перевантажень, тому деякі різновиди пісочниць використовують для пробного чи першого запуску не відлагодженого або шкідливого коду. Варто зазначити, що такими засобами як пісочниця користуються розробники в процесі написання продукту, для безпечних пробних запусків програм. Це дозволяє уникнути випадкових пошкоджень системи не готовим продуктом, що дозволить зменшити час на усунення пошкоджень системи.

1.4. Висновки до розділу 1

В першому розділі, даної кваліфікаційної роботи магістра було розглянуто саму суть вразливостей, розібрано, що вони можуть бути не лише як програмна чи апаратна вада комп’ютерної системи, а й люди, котрі обслуговують чи працюють на цих машинах. Було розглянуто вразливості систем на базі процесорів Intel та AMD. Досліджено конкретні вразливості сімейства Meltdown та Spectre. Було висвітлені групи дослідників, котрі відкрили дані прогалини в безпеці, та продовжили працювати над ними. Також було показано всі можливі системи захисту, комп’ютерів розділених по категоріях, від найпростіших до найскладніших. Описано можливий вплив на потужність та швидкодію системи, через наявність тої чи іншої системи захисту.

РОЗДІЛ 2
ВИБІР ОПТИМАЛЬНИХ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ЦЕНТРАЛЬНИХ ПРОЦЕСОРІВ ВІД АТАК

2.1. Виявлення вразливостей у системі

Атаки типу Spectre використовують можливості прогнозування переходів процесора. Сучасні процесори включають функцію, яка називається прогнозування переходів, яка спекулятивно виконує інструкції в місці, яке на думку центрального процесора, буде переходом. Таке спекулятивне виконання допомагає більш повно використовувати частини CPU, мінімізуючи час очікування, і, отже, підвищуючи продуктивність. Коли перехід успішно передбачений, інструкції будуть виконані, що означає, що будуть видані результати інструкцій, таких як регістр і запис пам'яті. Якщо перехід неправильно передбачений, спекулятивні інструкції будуть відкинуті, а прямі побічні ефекти інструкцій буде скасовано. Що не скасовується, це непрямі побічні ефекти, такі як зміни кешу процесора. Вимірюючи затримку операцій доступу до пам'яті, кеш можна використовувати для вилучення значень з умовно виконаних інструкцій.

У варіанті Spectre 1 (CVE-2017-5753) інструкції після умовного передбачення умовно виконуються в результаті неправильного прогнозування. З варіантом 2 Spectre (CVE-2017-5715) ЦП виконує інструкції в місці, визначеному помилково прогнозованим переходом.

В обох варіантах атаки Spectre вплив полягає в тому, що процес може просочити конфіденційні дані в інші процеси в системі. Spectre може також дозволити одній частині програми отримати доступ до інших частин того ж простору пам'яті процесу, що інакше не було б дозволено.

Хоча атака Spectre сама по собі не перетинає границю привілеїв пам'яті користувача / ядра, залежно від конфігурації цільової платформи, атака Spectre може опосередковано дозволити користувацькому простору отримати доступ до пам'яті ядра. Наприклад, у блозі Project Zero описується сценарій, який

використовує eBPF для видалення вмісту пам'яті ядра в коді простору користувача. Це стало можливим завдяки тому, що eBPF JIT дозволяє додаткам простору користувача вводити код, який виконується в просторі ядра. Хоча цей код перевіряється ядром, буде дозволено виконувати eBPF-сумісний код з дозволами ядра. Експлойт, описаний Project Zero, використовує eBPF для виконання атаки Spectre в просторі ядра, а стягувані дані в просторі користувача. Можливо, що інші технології, які дозволяють виконання коду в ядрі, також можуть бути використані для витоку пам'яті ядра за допомогою Spectre [7].

Meltdown пов'язана з атакою Spectre, оскільки вона також використовує бічний канал кешу для доступу до даних, які в іншому випадку не будуть доступні. Основна відмінність полягає в тому, що він використовує можливості виконання в сучасних процесорах. Як і спекулятивне виконання через прогнозування переходів, як це використовує Spectre, виконання поза чергою на CPU є методом, що забезпечує повне використання модулів процесора. Хоча інструкції можуть з'являтися послідовно на машинній мові, процесор, який підтримує виконання поза чергою, може виконувати інструкції не послідовним чином, що може звести до мінімуму час, який CPU витрачає в режимі очікування. Meltdown використовує небезпечну поведінку, яка була продемонстрована в процесорах Intel і може вплинути на процесори інших виробників. Уразливі процесори дозволяють читати пам'ять у виконанні команд поза чергою, а також містити умови гонки між підняттям винятків та виконанням команд поза чергою. Атака Meltdown читає значення пам'яті ядра, яке викликає виняток, тому що код, що виконується з привілеями користувацького простору, не може безпосередньо читати пам'ять ядра. Проте, внаслідок стану перегонів, можуть виконуватися і інструкції з виходу з ладу, що слідують за інструкцією з відмови. Навіть незважаючи на те, що інструкції з'являються після команди з помилкою, виконання поза чергою дозволяє виконувати їх, використовуючи дані, отримані з інструкції, що викликає виняток. До моменту виникнення винятку виконується деяка кількість

інструкцій, що вийшли з ладу (out-of-order). Незважаючи на те, що виняток змушує CPU відкинути інструкції з виключенням, стан кешу не повертається. Це дає змогу зберігати дані з інструкцій, що вийшли з-поза порядку, після того, як було висунуто виняток.

Вплив Meltdown полягає в тому, що процес, що виконується в просторі користувача, може переглядати вміст пам'яті ядра. Meltdown може також дозволити Spectre-подібний витік вмісту пам'яті, що не перетинає межі привілеїв користувача / ядра.

Послаблення ядра Linux для Meltdown називаються KAISER, а згодом KPTI, які спрямовані на поліпшення поділу сторінок ядра та пам'яті користувача. Оскільки атаки Spectre не перетинають межі користувача / ядра, захист, введений з KAISER / KPTI, не додає жодного захисту від них [8].

Для того, щоб виявити наявність вразливостей на вашому комп’ютері, можна скористатись декількома способами.

Перший це напряму виконати PowerShell скрипт, як і радили самі Microsoft. Для цього потрібно для початку налаштувати політику виконання, ExecutionPolicy, на потрібний рівень, а саме Bypass , або Unrestricted. Для початку потрібно взнати, яка політика у вас вже застосована, це можна зробити за допомогою команди:

```
Get-ExecutionPolicy
```

Дана команда виведе нам наявну політику виконання, як видно на рис. 2.1.

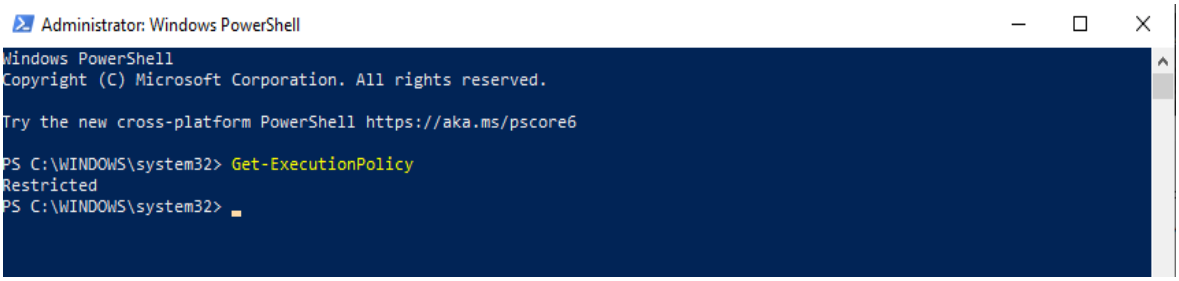

Рис. 2.1. Політика виконання PowerShell

Варто зазначити, що запускати PowerShell потрібно від імені адміністратора. Для зміни політики виконання на потрібну нам потрібно буде виконати наступну команду:

```
Set-ExecutionPolicy Unrestricted
```

Або ж, щоб не отримувати сповіщень і запитів підтверджень від системи, то команду:

```
Set-ExecutionPolicy Unrestricted –Force
```

Далі ми можемо завантажити і виконати PowerShell модуль, це можна зробити за допомогою наступних команд:

```
Install-Module SpeculationControl
```

Відповідаємо на всі питання так, або ж «Y», як у запитанні. Далі виконуємо команду:

```
Import-Module SpeculationControl
```

І для запуску вже безпосередньо перевірки виконуємо команду:

```
Get-SpeculationControlSettings
```

В результаті ви отримаєте список із можливих вразливих чи захищених елементів системи. На рис. 2.2 показано результат повністю захищеної системи.

Для виконання даного способу виявлення вразливостей необхідні деякі знання роботи з Windows PowerShell. Якщо команди для встановлення та запуску даного модуля виявлення всі наявні в цій роботі, то саме налаштування рівня політики виконання, є дещо проблематичним, та вимагатиме професійних

знань. Але з використанням інструкцій, описаних в цій роботі та за допомогою ресурсів інтернет, можна справитись з цією задачею.

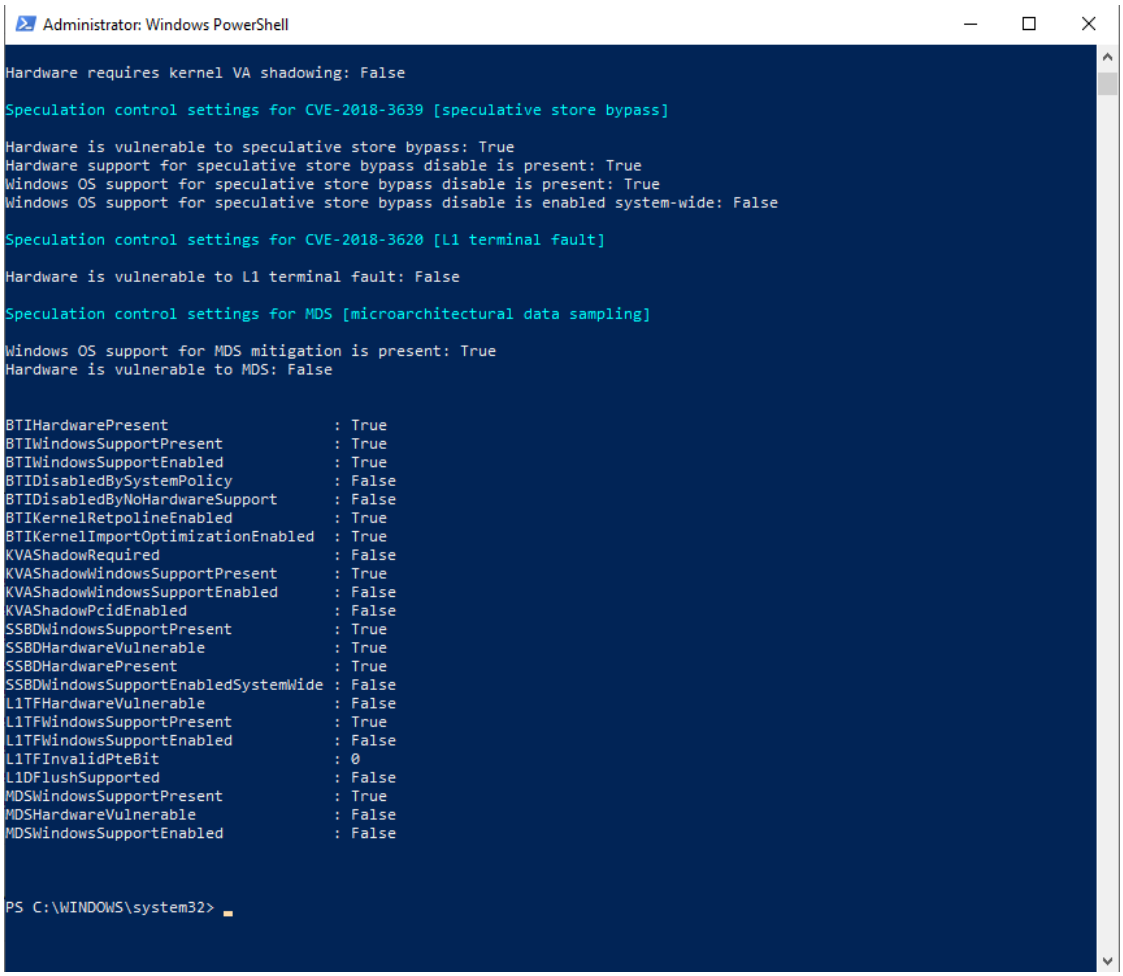

Рис. 2.2. Результат виконання PowerShell модуля із увімкненим захистом

Варто зазначити, що отриманий результат, з наявними результатами «False», є допустимим для комп'ютерів з процесорами компанії AMD, а саме сімейства Ryzen, так як вони не вразливі до атак типу Meltdown. Якщо ж подивитись на результати такого ж тесту, але з уже вимкненими системами захисту від цих вразливостей, то ми отримаємо інший результат, який показано на рис. 2.3.

Як ми бачимо на рис. 2.3, деякі з позицій змінили свій стан з позначення «True» на позначення «False», тобто певні засоби, які раніше були увімкненими стали вимкненими. Зокрема варто зазначити, що BTIWindowsSuportEnabled, тобто даний пункт став вимкненим. У цьому пункті показано, чи ввімкнуто

підтримку Windows для відповідної області для усунення вразливостей. При увімкненому стані, підтримка апаратного забезпечення та підтримка операційної системи для відповідної області, що використовується, для пристрою ввімкнуто, тобто захищаючи її від вразливості сімейства Spectre. Пункт BTIDisabledBySystemPolicy отримав позначку «True», і став вимкненим, так як в назві вказано, що цей параметр відповідає за вимкнення цього пункту. Далі, параметр BTIKernelRetpolineEnabled теж став з позначкою «False», в даному випадку вимкнений, так само, як і параметр BTIKernelImportOptimizationEnabled. Тобто кожен з параметрів відповідає за певну вразливість з сімейства, або пом’якшення вразливості.

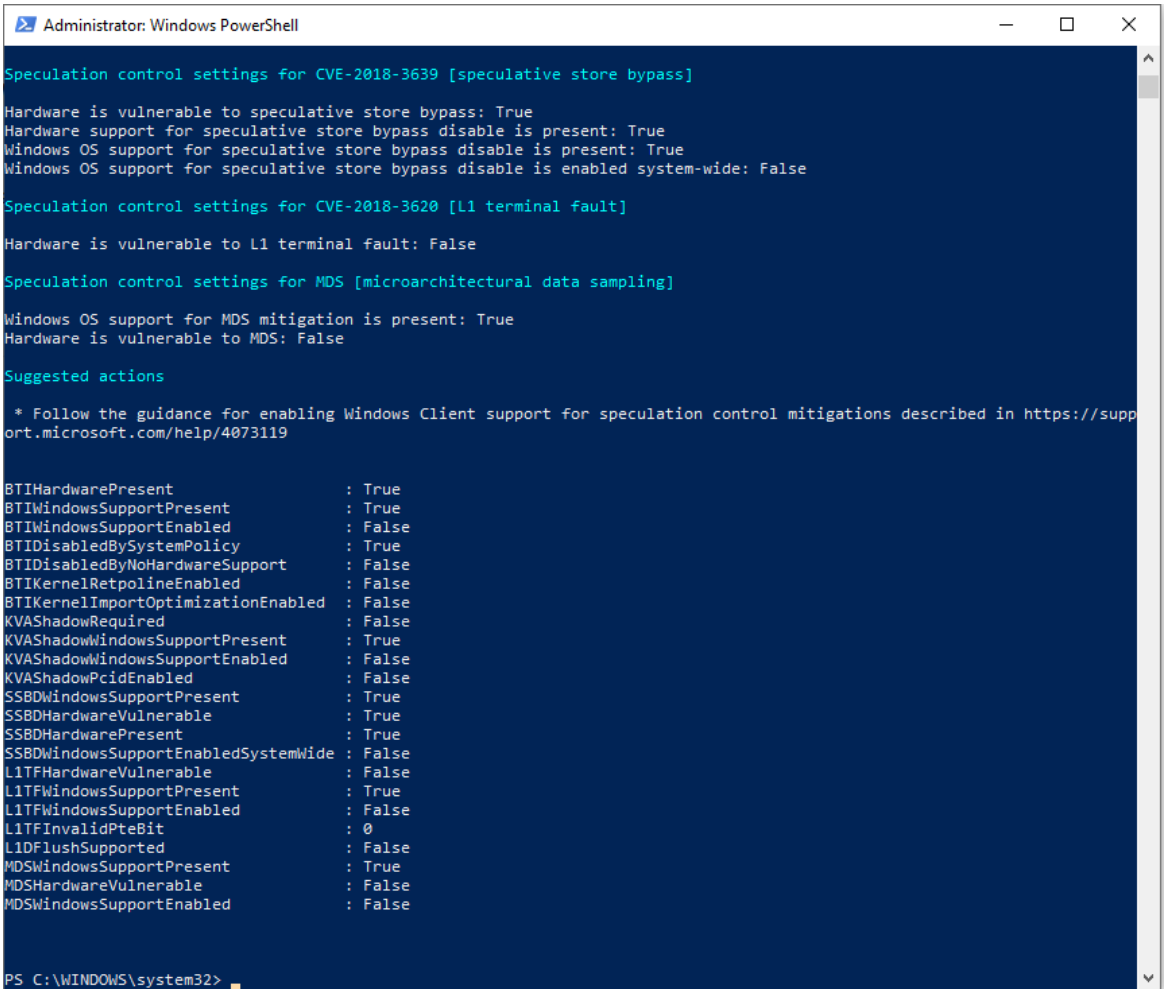

Рис. 2.3. Результат виконання PowerShell модуля із вимкненим захистом

Тобто ми можемо зазначити, що саме зміна цих параметрів в системі, буде означати вразливість чи захищеність від атак типу Spectre, так як атаки

типу Meltdown, через архітектурні вразливості процесорів AMD, не є можливими. Варто зазначити, що в системі, на якій проводились дані тестування, центральним процесором є Ryzen 2600, виробництва AMD.

Проте, якщо дані маніпуляції є занадто складними, а ви все одно бажаєте взнати чи вразлива ваша система, то ви можете скористатись простим, портативним застосунком авторства американського спеціаліста з IT-безпеки Steve Gibson. Тобто вам його не потрібно встановлювати, а лише скачати та запустити на вашому комп'ютері. Дана програмка має назву InSpectre і вона покаже вам чи захищена ваша система від вразливостей, чи ні. Також, як показано на рис. 2.4, ви можете вимкнути захист, тобто заплатки за допомогою цієї програми. Вона це робить шляхом зміни параметрів в реєстрі Windows, що дозволяє вам не робити це самостійно [10].

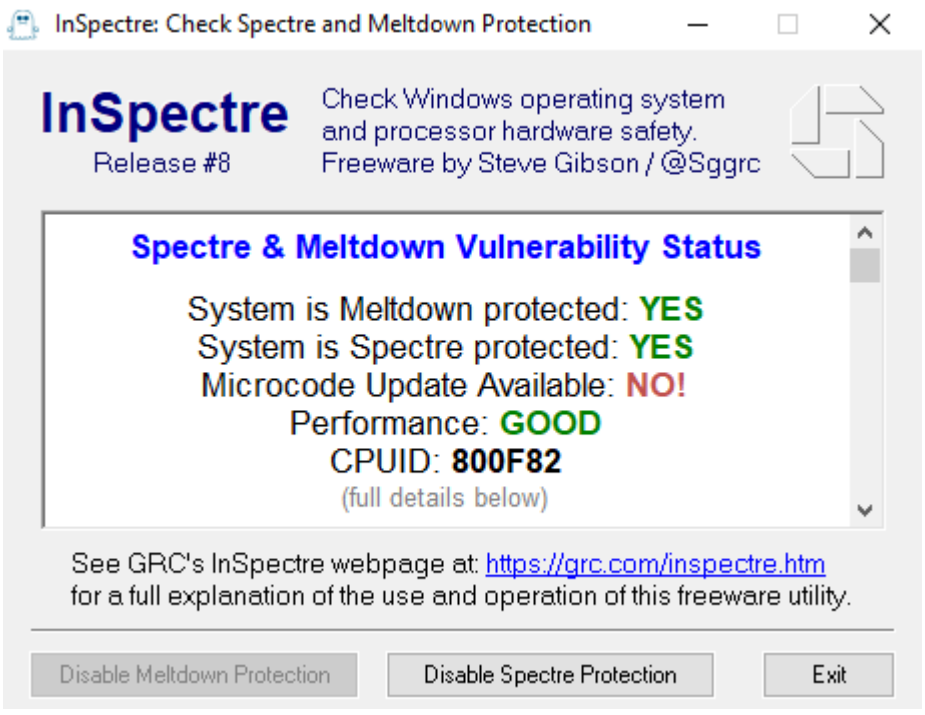

Рис. 2.4. Програма InSpectre

Як ми бачимо на рис. 2.4, кнопка «Disable Meltdown Protection» є неактивною, причини цього було описано вище.

Загалом дана утиліта є вкрай корисною, так як окрім того, що показує нам чи вразлива система, чи ні та безпосередньо дозволяє впливати на параметр

захищеності, може показати чи сповільнена система, чи ні. Саме параметри «System is Meltdown protected», «System is Spectre protected» з подальшими позначеннями типу «YES» чи «NO» і вказує, наявність захисту у нашій системі. Даний параметр не є об'єктивним, так як оперує даними, наявними в системі, та з онлайн баз. Також додаток вказує на наявність оновлень мікрокоду, якщо оновлень немає то все добре, принаймні у випадку для систем на базі Ryzen. Варто добавити, що окрім великого попередження, на головному екрані, присутні також детальніші описи та рекомендації, для безпеки системи. Це можна побачити на рис 2.5, де показано попередження про вразливу систему, яке було отримано, при відкаті системи, до найстаріших версії BIOS та Windows.

Рис. 2.5. Попередження, про вразливість системи у програмі InSpectre

Варто зазначити, що дана утиліта постійно оновлюється, що добре, так як додаються нові і нові функції і можливості, які будуть корисні користувачеві.

2.2. Програми для тестувань швидкодії процесора

Для здійснення аналізу по дослідженню впливу використання процесорних заплаток від вразливостей сімейства Meltdown і Spectre на

швидкодію комп’ютерних систем потрібно використовувати різнопланові тестувальні застосунки. Ці програми повинні бути направленні на тестування системи як в синтетичних застосунках, що будуть подібними до робочих програм, так і на розважальні програми, тобто ігри. Синтетичні тести, це тести, котрі проводяться у спеціалізованих програмах, основна задача котрих і є цей тест. Варто сказати, що синтетичні тести не завжди дозволяють отримати результати, котрі будуть такі ж, як при робочому навантаженні, вони необхідні лише для систематизації отриманих результатів, і порівняння з іншими системами, чи тими ж системами з різними параметрами, що можуть впливати на кінцевий результат. Що в принципі в нашому випадку і використовується, тестування системи, з різними версіями програмного забезпечення, та з ввімкненими та вимкненими заплатками. Різний набір тестів необхідний для різноплановості самих тестів і для отримання задовільних результатів дослідження, як для користувачів комп’ютерної системи для робочих програм, так і для простих ігор.

Отже для тестування було вибрано програми типу бенчмарк: Cinebench R20, X265. Та ігрові застосунки: World of Tanks, FarCry 5.

Компанія Maxon Computer розробила популярний бенчмарк для різних платформ Cinebench R20. Даний застосунок був розроблений для тестування процесорів та визначення рівня їх рівня продуктивності, шляхом отримання певної кількості балів за рендеринг певної фотореалістичної сцени із застосуванням технології Cinema 4D. Варто зазначити, що чим більша кількість балів, тим краще і тим вищий рейтинг у тестованої системи. Сама сцена включає в себе текстури високого розширення, елементи трасування променів, освітлення та відбиттів. Дана версія програми є складнішою ніж попередник, так як обчислювальних потужностей потрібно в 8 разів більше і в 4 рази більше пам’яті. Тому результати даної версії не можна порівнювати із попередніми. Дана версія отримала хорошу оптимізацію під багатопоточні процесори, що пригодиться в цьому дослідженні. На рис. 2.6 показано процес тестування у програмі Cinebench R20. Як видно на цьому ж зображені тест

виконується в 2 етапи. Першим етапом виконується рендеринг сцени всіма ядрами процесора, а в другому етапі ця ж сцена вже опрацьовується лише 1 процесорним ядром. Це конкретно вибраний сценарій тестування, можна використовувати тести, як окремо, так і разом. За це відповідає конкретний пункт в налаштуваннях.

Варто зазначити, що Cinebench R20 не є фінальною версією продукту, так як вже доступна Cinebench R23, проте там зміни не настільки суттєві, для оновлення, основним пунктом в новій версії, є підтримка ARM процесорів, M1 Apple зокрема. А так як тестована система працює на архітектурі X86, то це не є необхідним[11]..

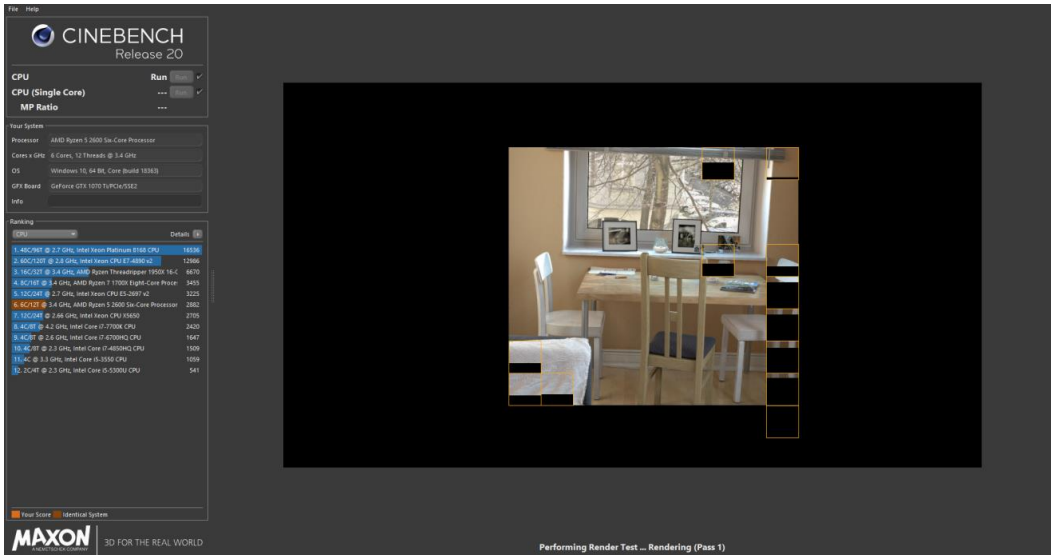

Рис. 2.6. Тестування у програмі Cinebench R20

x265 - це відкрита реалізація нового стандарту кодування відео H.265 (High Efficiency Video Coding (HEVC)). Стандарт H.265 є логічним продовженням H.264 і характеризується більш ефективними алгоритмами стиснення. Стандарт передбачає зменшення розміру файлу приблизно в два рази за однакової візуальної якості у порівнянні з H.264. Стандарт передбачає підтримку високої роздільної здатності до 8K UHD (8192 × 4320). Перша версія стандарту H.265 була опублікована на початку 2013 року. Оскільки стандарт опублікований не так давно, вся приватна реалізація програмного забезпечення для декодування / кодування дуже далека від досконалості (включаючи x265).

А сам спосіб тестування базується на перекодуванні певного тестового відео формату 1080p у формат H.265 у вигляді 4 прогонів із отриманням результату у вигляді часу перекодування відрізку, та середній кількості кадрів у секунду, які було перекодовано. При порівняння результатів, кращий буде той, де час перекодування менший, тобто система швидше виконала поставлену задачу, і середня кількість кадрів у секунду більша, з чого і випливає менший час перекодування. Даний тест використовується в даному дослідженні, так як також добре навантажує процесор [12]. На рис. 2.7 показано перебіг тестування системи.

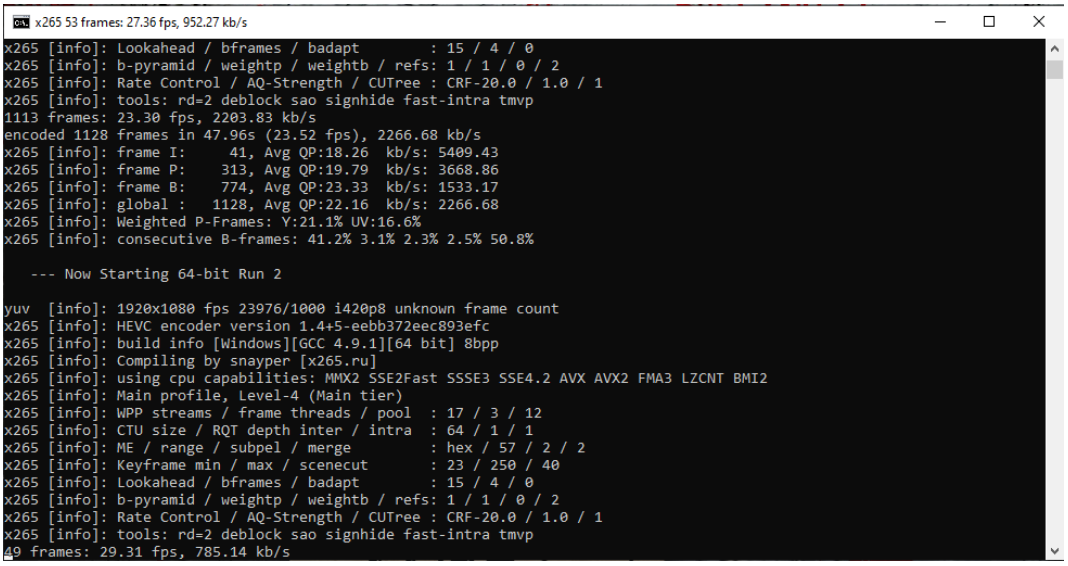

Рис. 2.7. Тестування у програмі X265

Результати отримані при тестуванні даним застосунком записуються у новостворений файл формату Word, в якому вказано час перекодування кожного з прогонів, середня кількість кадрів в секунду під час кожного з прогонів, а також показано загальна інформація, про систему, яка тестується.

Також для тестування було використано вже ігрові застосунки, або ж на їх базі. World of Tanks Encore це свого роду бенчмарк на основі наявної багатокористувацької гри World of Tanks. Даний тест робить прогін на заданій сцені, при налаштовуваних параметрах графіки, з використанням ресурсів близьких, або й навіть більших ніж потрібно для конкретної гри. Цей тест було

вибрано, тому що він добре навантажує всі ядра системи, та що більш важливо він є автоматичним, тобто для тестування не потрібні маніпуляції від людини, що могли б зробити результати не точними. Також тест видає після завершення власний результат, у вигляді рейтингових балів, але в нашому дослідженні вони фігурувати не будуть, ми будемо використовувати середні, максимальні, мінімальні, рідкісні та дуже рідкісні кадри. Варто зазначити, що як звучить з назви, середня кількість кадрів, це відношення кількості кадрів, яка була зафіксована програмою, до всього перебігу тесту. Значення максимальних та мінімальних кадрів, це значення миттєвих кадрів, що були зафіксовані. Якщо ж розглянути що таке 1% та 0.1% кадру, або ж рідкісні та дуже рідкісні, то це грубо кажучи процентиль, або ж в нашому випадку значення, нижче якого находиться певний процент даних із набору, набір в нашому випадку це всі кадри під час нашого тесту. Варто зазначити, що ці дані отримуються за допомогою аналізу і обрахунку часу кадру, або ж «frame time». Тобто тут справа в тому, що під час відтворення зображення, час кадру змінюється в залежності від складності конкретної сцени і тому при середньому значені, всі «довгі» кадри будуть усереднені та втрачені, максимум, якийсь з них буде використаний як мінімальне значення, що не є показником. Але за допомогою цих наших рідкісних і дуже рідкісних кадрів, ми отримуємо вже деяку статистику із кадрів, час яких був довшим за інші, через складність сцени, чи вплив ззовні системи. Ці дані дозволяють краще тестувати систему та порівнювати отримані результати [13]. На рис. 2.8 показано результат після проведення тесту.

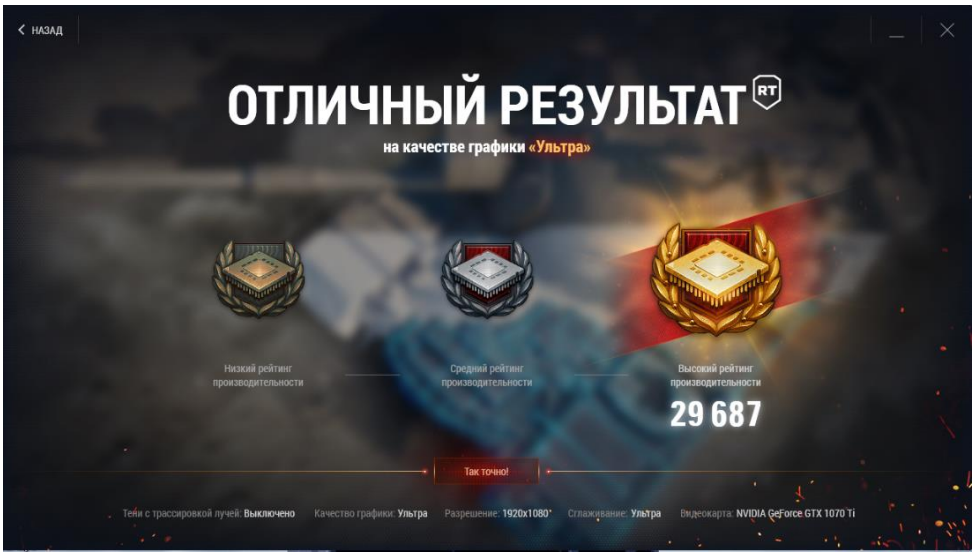

Рис. 2.8. Результат проведення тесту у World of Tanks Encore

Як альтернатива, було використано також ігровий бенчмарк, але вже внутрішній, із гри FarCry 5. Дана гра була вибрана також через наявність автоматичного проведення, хоча варто зазначити, що навантаження на систему також достойне. Тут є відмінність, що гра більше любить високі частоти, й застосовує не всі ядра одночасно. На рис. 2.9 показано статистику після проведення цього тесту. Проте варто зазначити, що в цій грі також використовувались сторонні засоби захоплення та отримання тестових даних [14].

Рис. 2.9. Результат проведення тесту у FarCry 5

На рисунку вище ми бачимо оверлей від сторонньої програми для моніторингу та захоплення тестових даних, ця програма це MSI Afterburner, її первинне призначення було у розгоні та контролі параметрів відеокарт, але її захоплююча складова з моніторингом є також вдалою. На рис. 2.10 показано як виглядає навантаження на систему під час самого тестування, в одному з застосунків.

Проте варто зазначити, що всі необхідні значення, тобто середні, максимальні, мінімальні, рідкісні та дуже рідкісні кадри захоплюються програмою та результати після закінчення тесту записуються у файл типу txt з назвою застосунку, у якому були зібрані та час тестування.

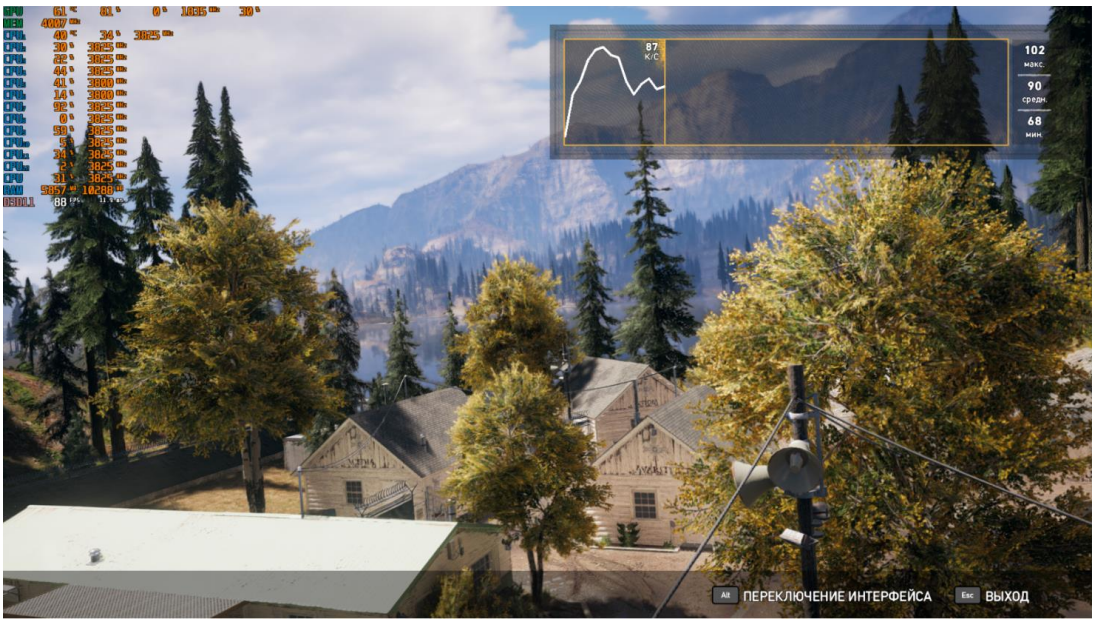

Рис. 2.10. Перебіг тестування у FarCry 5 з оверлеєм MSI Afterburner

MSI Afterburner це застосунок, головна і напевне першочергова задача якого була в моніторингу стану саме відеокарти та можливості розгону частот графічного процесора та пам’яті. Що чудово видно на рис. 2.11.

Тобто головне вікно програми виконано з демонстрацією для початку інформації про встановлену графічну карту в системі та її стан, тобто частота графічного ядра його завантаженість, частота пам’яті та температура. Варто зазначити, що додаток добре справляється із «розгоном», тобто підвищенням частот пам’яті, і що частіше частоти графічного процесора, за допомогою

підняття вольтажу, та як наслідку ефективності системи охолодження. Тому що при збільшені подаваної енергії на графічний чіп, отримується підвищене тепловиділення, яке може спричинити поломку пристрою. Дані дії варто загалом не проводити, а якщо ж вже наважились, то під контролем досвідченої в даних питаннях людини [15].

Проте дана програма використовується саме через те, що вона може виконувати захоплення всіх нам потрібних значень, тобто мінімальне, максимальне, середнє та рідкісне значення кадрів.

Рис. 2.11. MSI Afterburner

Також варто зазначити, що програма дозволяє виводити статистику, та інформацію поверх запущених ігрових додатків, та застосунків, які будуть тестуватись. Там можна виводити необхідні вам параметри, які представлені обширним списком, від тих самих кадрів в секунду, до завантаженості, як графічного так і центрального процесорів, їх температуру, швидкість оберту вентиляторів на системі охолодження. Можна моніторити навіть кількість пам’яті виділеної системою для даного застосунку, не тільки оперативної, але й

графічної. Чи навіть якщо є недостатньо відео пам’яті в відеокарті то показати розмір файлу підкачки, який стягується з оперативної пам’яті, а в свою чергу якщо тієї недостатньо, то з накопичувального пристрою. Всі ці параметри є вкрай важливими, так як дозволяють бачити всю ситуацію в системі під час її тестування, чи навантажена вона, наскільки вона навантажена і т.д.

2.3. Висновки до розділу 2

В другому розділі даної кваліфікаційної роботи магістра було детально розглянуто, що таке витік бічного каналу і яким чином, можна його використати. Було показано способи виявлення наявності даних недоліків в безпеці комп’ютера, як для просунутих, так і для звичайних користувачів. Детально розписано всі програми, які будуть використані у досліджені. Розглянуто синтетичні тести на базі Cinebench R20 та X265, ігрові тести у World of Tanks Encore та FarCry 5, і супутні застосунки, для отримання результатів, а саме MSI Afterburner.

РОЗДІЛ 3
РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ВПЛИВУ ПРОЦЕСОРНИХ ЗАПЛАТОК НА ШВИДКОДІЮ КОМП'ЮТЕРА

3.1. Тестування комп'ютера без змін

Для початку ми проводимо тести не чіпаючи нічого, тобто жодних вимкнень заплаток, чи видалень оновлень безпеки Windows. Наявна версія BIOS E7B79AMS.A30, від 16.11.2018. Єдина маніпуляція, це вимкнення усіх можливих фонових процесів, щоб тести були якомога точнішими. Далі ми робимо просту маніпуляцію, це вимикаємо захист від вразливостей типу Meltdown/Spectre за допомогою утиліти InSpectre, або ж за допомогою коректування певних параметрів у реєстрі. Мною було використано саме утиліту, але команди для зміни реєстру в PowerShell, буде наведено в рис. 3.1.

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 3 /f

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
```

Рис. 3.1. Команди для зміни реєстру в PowerShell

Для визначення, чи все ж таки захист вимкнено, також використовуємо InSpectre, як показано на рис. 3.1.

Рис. 3.2. Утиліта InSpectre

Як було сказано в попередніх розділах, процесори сімейства Ryzen не вразливі до атак типу Meltdown, але це не означає, що не було встановлено уніфікованих заплаток, які б теж могли спричиняти сповільнення системи.

Отже, першим тестом буде Cinebench R20, після двох прогонів, при кожному з станів, увімкненому чи вимкненому систем захисту були вибрані середні значення і занесені у табл. 3.1.

Таблиця 3.1

Тестування Cinebench R20

	Заплатки увімкненні	Заплатки вимкненні
Одноядерний тест, бал.	391	403
Багатоядерний тест, бал.	2911	2930

Також, для наочності дані було подано, як діаграми, тому на рис. 3.3, видно, хоч не значну, але все ж різницю в швидкодії між прогонами.

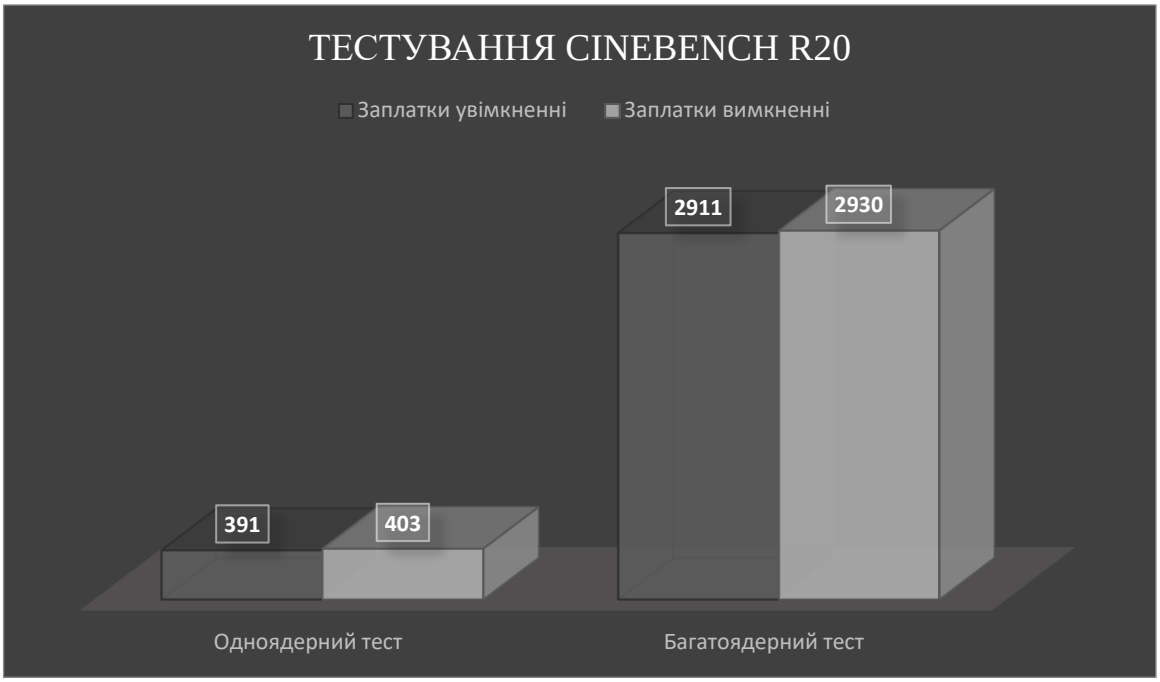

Рис. 3.3. Діаграма результатів тестування Cinebench R20

Наступним тестом буде X265, тут та ж методика, спочатку тестування при увімкнених заплатках, потім у вимкнених, результати показано у табл. 3.2, та рис. 3.4.

Таблиця 3.2

Перекодування відео у x265

	Заплатки увімкненні	Заплатки вимкненні
Час перекодування, с.	47.84	47.62
Середня кількість кадрів, fps	23.58	23.69

Варто зазначити на рахунок результатів тестування. Отриманні результати слід розуміти так:

- час перекодування, чим менше значення, тим краще, і продуктивність системи є вища;
- середня кількість кадрів, чим більше значення, тим краще, тобто це кількість кадрів, перекодованих у секунду.

Рис. 3.4. Діаграма результатів перекодування відео у X265

Далі було проведено тестування у World of Tanks Encore, методика тестування незмінна, дані внесено у табл. 3.3 та у рис. 3.5.

Таблиця 3.3

Тестування у World of Tanks Encore

	Заплатки увімкненні	Заплатки вимкненні
Середня частота кадрів, fps	174.5	175.7
Мінімальна кількість кадрів, fps	113.8	113.1
Максимальна кількість кадрів, fps	412.2	468.9
Рідкісні кадри 1%, fps	110.3	113
Дуже рідкісні кадри 0.1%, fps	89.7	103.8

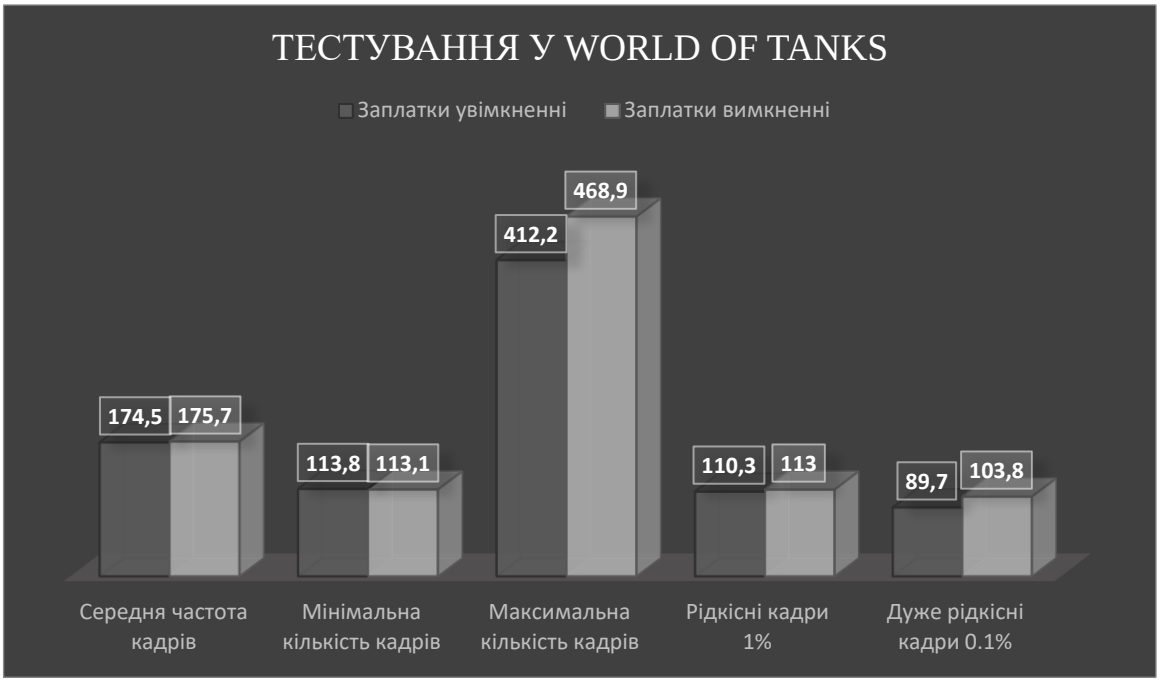

Рис. 3.5. Діаграма результатів тестування у World of Tanks Encore

І останньою програмою для тестування в цьому прогоні буде FarCry 5, методика така ж, як і у попередніх, дані занесено у табл. 3.4 та у рис. 3.6.

Таблиця 3.4

Тестування у FarCry 5

	Заплатки увімкненні	Заплатки вимкненні
Середня частота кадрів, fps	92.8	93.4
Мінімальна кількість кадрів, fps	26.3	65.5
Максимальна кількість кадрів, fps	117.5	116.8
Рідкісні кадри 1%, fps	41.6	64.1
Дуже рідкісні кадри 0.1%, fps	7.2	9.1

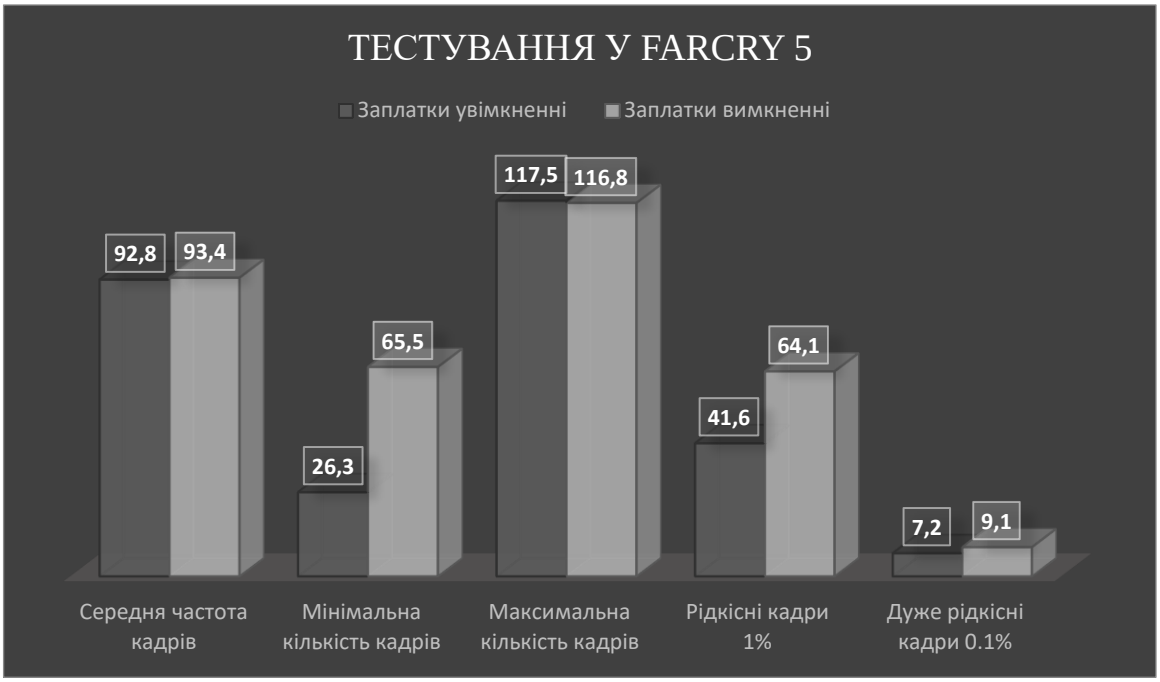

Рис. 3.6. Діаграма результатів тестування у FarCry 5

Як ми бачимо із першого ж прогону, при вимкнені заплаток, різниця є. Якщо ми беремо до уваги синтетичні тести, то там вона мізерна і суттєво не вплине на продуктивність. Але якщо звернути увагу на тести у ігрових застосунках, то ми бачимо, що у обох випадках суттєво підросли показники рідкісних та дуже рідкісних кадрів, більше того у FarCry 5 видно значний приріст по мінімальному значенню кадра. Дані показники є вкрай важливими для такого роду застосунків, так як показують можливі лаги картинки у грі.

3.2. Тестування з оновленою системою

Наступним ж прогоном буде виконання усіх вищепоказаних тестів, але у системі із останньою версією BIOS, та з встановленими всіма можливими оновленнями Windows. Оновлена версія BIOS E7B79vAH.

Отже, після проведення всіх тестів повторно, з такою ж методикою, спочатку із увімкненими заплатками, а потім із вимкненими, було отримано дані, які були внесені в табл. 3.5 і рис. 3.7, для Cinebench R20, табл. 3.6 та рис. 3.8 для x265, табл. 3.7 та рис. 3.9 для World of Tanks Encore і табл. 3.8 та рис. 3.10 для FarCry 5.

Таблиця 3.5

Тестування Cinebench R20

	Заплатки увімкненні	Заплатки вимкненні
Одноядерний тест, бал.	404	402
Багатоядерний тест, бал.	2935	2944

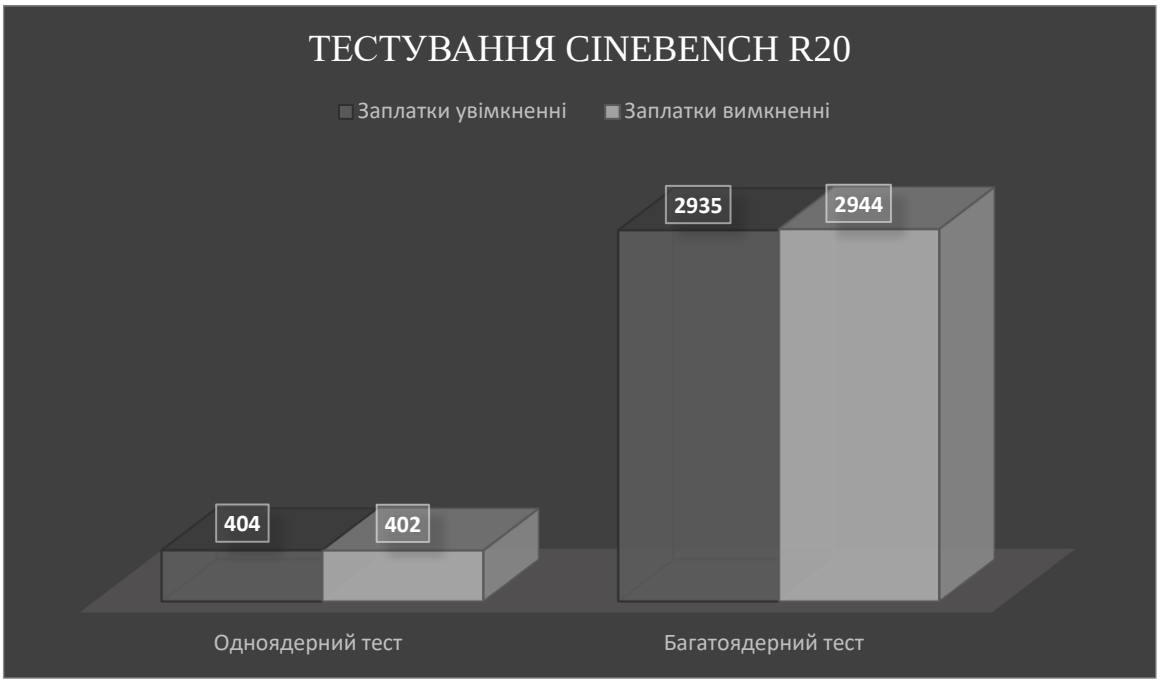

Рис. 3.7. Діаграма результатів тестування Cinebench R20

Видно, що результати у тестах з вимкненими заплатками різняться на рівні статистичних похибок. В одноядерному тесті виграє система захищена, а у багатоядерному навпаки, з вимкненим захистом.

Таблиця 3.6

Перекодування відео у x265

	Заплатки увімкненні	Заплатки вимкненні
Час перекодування, с.	48.62	48.33
Середня кількість кадрів, fps	23.2	23.34

Рис. 3.8. Діаграма результатів перекодування відео у X265

В даному тесті видно, що результати подібні до попереднього тесту, тобто у вигляді похибки, але все ж в сторону системи з вимкненим захистом.

Таблиця 3.7

Тестування у World of Tanks Encore

	Заплатки увімкненні	Заплатки вимкненні
Середня частота кадрів, fps	176.3	176.7
Мінімальна кількість кадрів, fps	113.6	112.5
Максимальна кількість кадрів, fps	475.5	479.9
Рідкісні кадри 1%, fps	113.3	112.5
Дуже рідкісні кадри 0.1%, fps	60.6	77.7

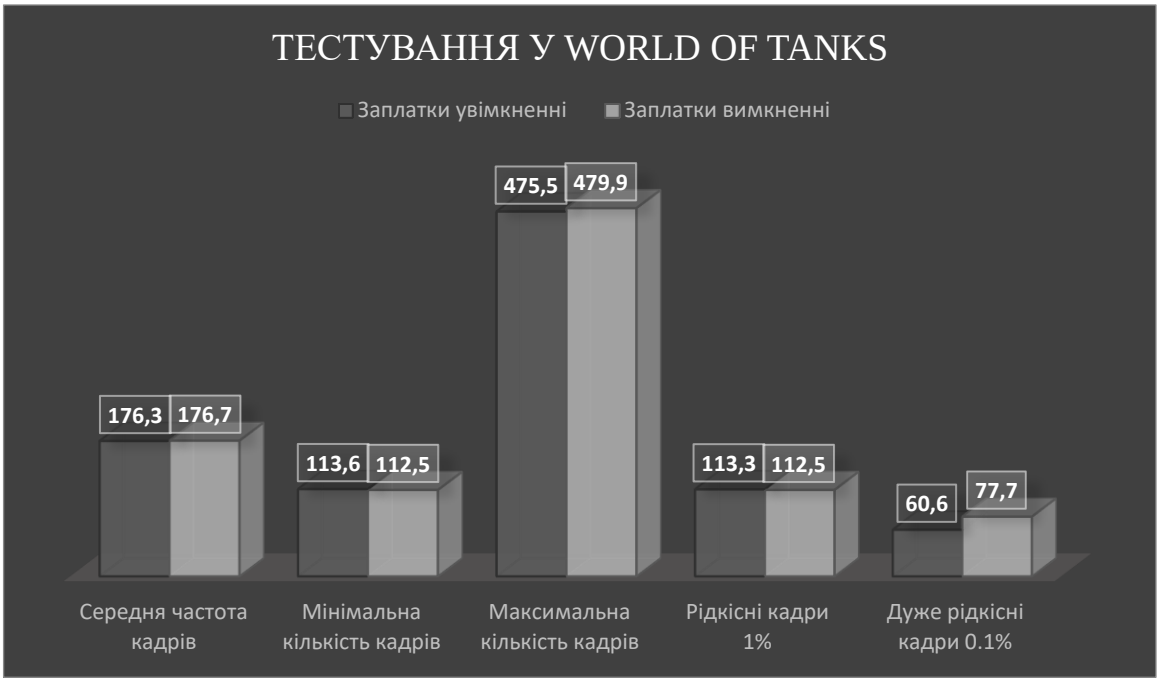

Рис. 3.9. Діаграма результатів тестування у World of Tanks Encore

Отримані результати в даному тестуванні є схожими, відрізняються вони не більше ніж на 1%, але й виключення, у вигляді приросту у дуже рідкісних кадрах на 28.2% на користь вимкненого захисту.

Таблиця 3.8

Тестування у FarCry 5

	Заплатки увімкненні	Заплатки вимкненні
Середня частота кадрів, fps	94.6	95
Мінімальна кількість кадрів, fps	35.1	51.6
Максимальна кількість кадрів, fps	117.5	117.7
Рідкісні кадри 1%, fps	50.9	65.5
Дуже рідкісні кадри 0.1%, fps	8.9	24.3

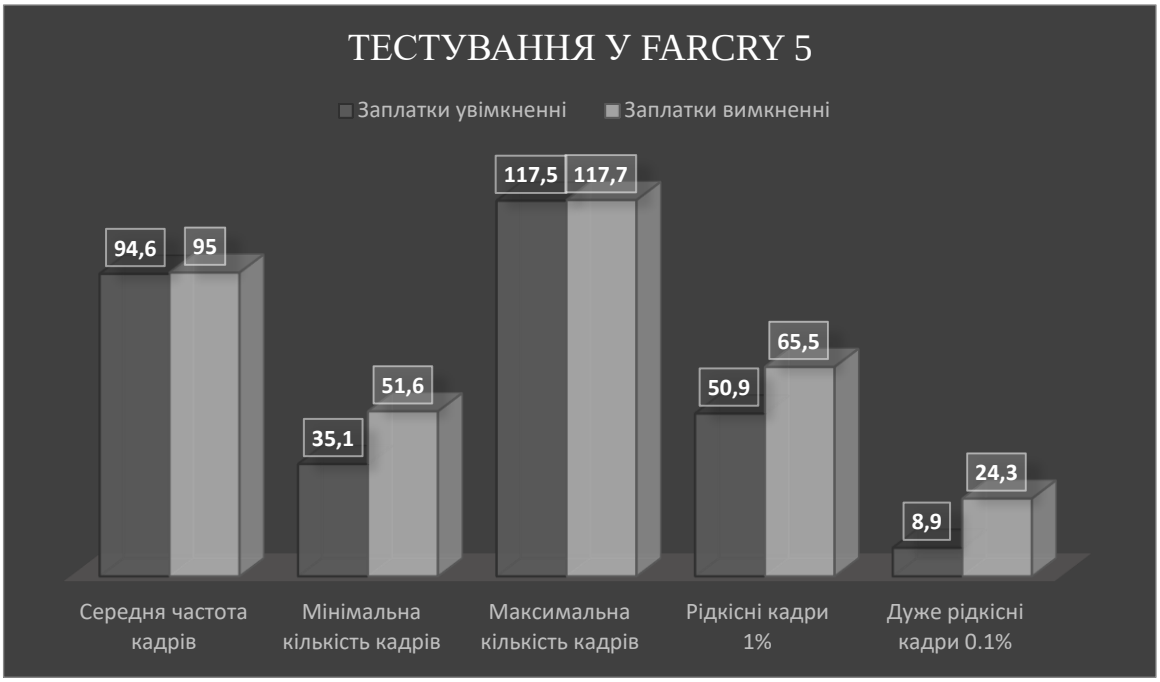

Рис. 3.10. Діаграма результатів тестування у FarCry 5

Таким чином, після отримання всіх даних, ми бачимо схожу картину, тобто результати у робочих програмах залишились з результатами на рівні похибки, але знову ж якщо звертаємо увагу на ігрові застосунки, ми бачимо різницю. Як і в першому випадку різниця проявляється у 0.1% кадру для World of Tanks Encore, але для FarCry 5, знову ж результати кращі як в 1% і 0.1%, так і в мінімальній кількості кадрів.

3.3. Порівняння отриманих результатів тестування

Останнім етапом тестування було проведено ще тест із встановлення найстарішої версії BIOS E7B79vA0, і з видаленням всіх оновлень безпеки у Windows. Прогін буде лише 1, так як систем захисту від Meltdown/Spectre немає. Після цього дані були внесені у збірні таблиці, табл. 3.9 та рис. 3.11 і рис. 3.12 для Cinebench R20, табл. 3.10 та рис. 3.13 і рис. 3.14 для X265, табл. 3.11 та рис.3.15 і рис. 3.16 для World of Tanks Encore, табл. 3.12 та рис. 3.17 і рис. 3.18 для FarCry 5, де їх можна порівняти із даними отриманими в попередніх прогонах. Це дасть нам змогу скласти повноцінну картину, про ефективність виконаних змін, та оновлень.

Таблиця 3.9

Порівняння результатів тестування в залежності від версій у Cinebench R20

	Заплатки увімкненні		Заплатки вимкненні		
	Початковий прогін	Прогін після оновлення	Початковий прогін	Прогін після оновлення	Прогін на старих версіях
Одноядерний тест, бал.	391	404	403	402	404
Багатоядерний тест, бал.	2911	2935	2930	2944	2910

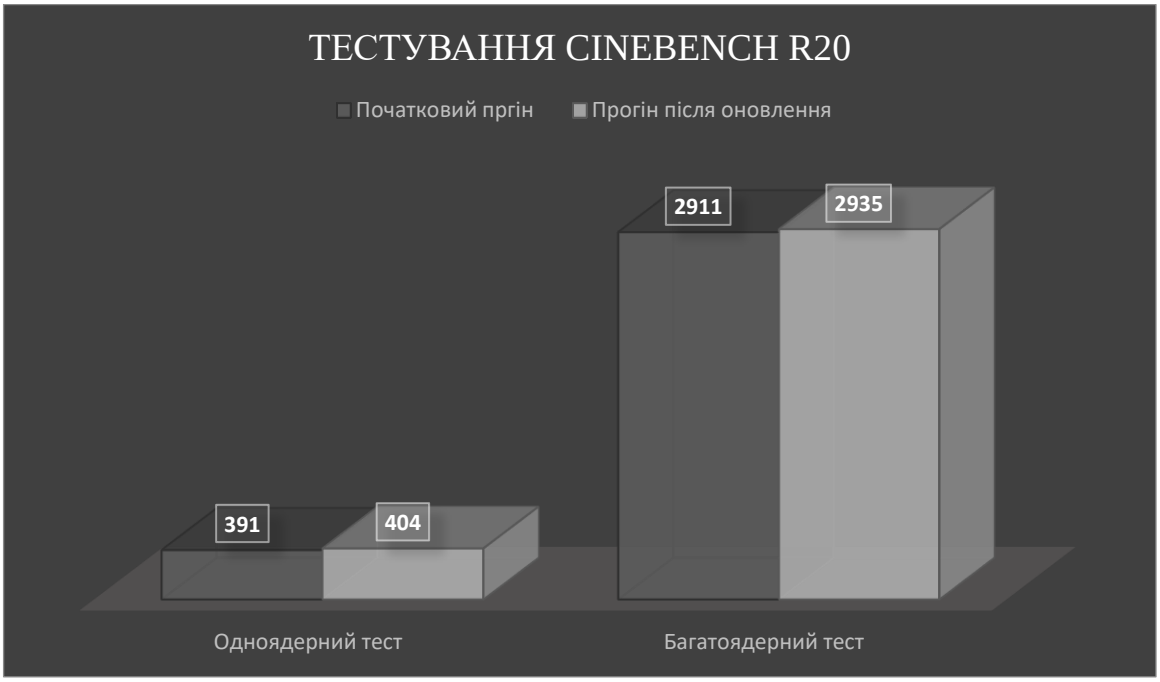

Рис. 3.11. Діаграма порівняння результатів тестування із увімкнутими заплатками у Cinebench R20

Отримані результати показують нам, що результати все ще різняться не більше ніж на 1%, але тим не менш, оновлена система показує кращі результати з увімкненим захистом, та в багатоядерному тесті з вимкненим захистом.

Рис. 3.12. Діаграма порівняння результатів тестування із вимкнутими заплатками у Cinebench R20

Таблиця 3.10

Порівняння результатів тестування в залежності від версій у X265

	Заплатки увімкненні		Заплатки вимкненні		
	Початковий прогін	Прогін після оновлення	Початковий прогін	Прогін після оновлення	Прогін на старих версіях
Час перекодування, с.	47.84	48.62	47.62	48.33	48.28
Середня кількість кадрів, fps	23.58	23.2	23.69	23.34	23.37

Рис. 3.13. Діаграма порівняння результатів тестування із увімкнутими заплатками у X265

Рис. 3.14. Діаграма порівняння результатів тестування із вимкнутими заплатками у X265

По отриманих результатах видно, що різниця в отриманих даних є мінімально, але варто зазначити, що вона все ж переважає на користь системи

із початкового прогону, як з вимкненим захистом, так і з увімкненим захистом, хоч і мінімально.

Таблиця 3.11

Порівняння результатів тестування в залежності від версій у World of Tanks Encore

	Заплатки увімкненні		Заплатки вимкненні		
	Початковий прогін	Прогін після оновлення	Початковий прогін	Прогін після оновлення	Прогін на старих версіях
Середня частота кадрів, fps	174.5	176.3	175.7	176.7	173.6
Мінімальна кількість кадрів, fps	113.8	113.6	113.1	112.5	112.7
Максимальна кількість кадрів, fps	412.2	475.5	468.9	479.9	445
Рідкісні кадри 1%, fps	110.3	113.3	113	112.5	112.1
Дуже рідкісні кадри 0.1%, fps	89.7	60.6	103.8	77.7	49.6

Варто сказати, що параметр середня частота кадрів, є по суті однаковим на всіх прогонах, різниця складає лише похибку. Точно так само, як і параметр мінімальної кількості кадрів. Тобто він також залишився незмінним. Основну увагу слід звернути на показники рідкісних та дуже рідкісних кадрів, там видно основну різницю в значеннях, краще цю різницю буде видно на рис. 3.15 та рис. 3.16.

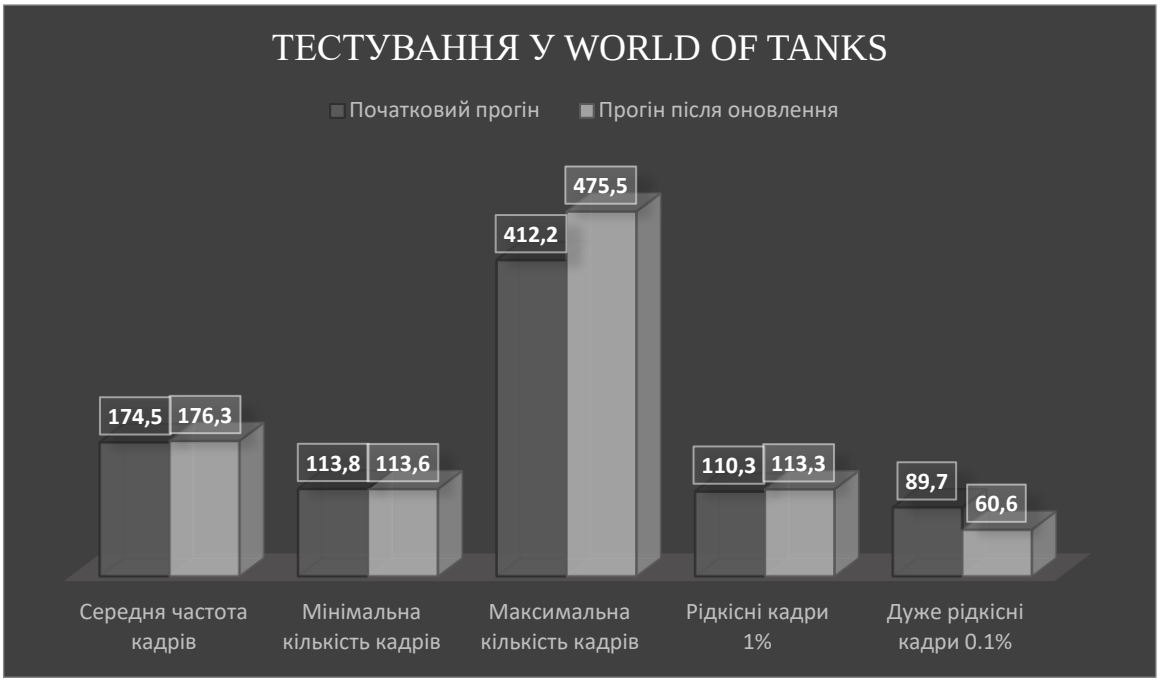

Рис. 3.15. Діаграма порівняння результатів тестування із увімкнутими заплатками у World of Tanks Encore

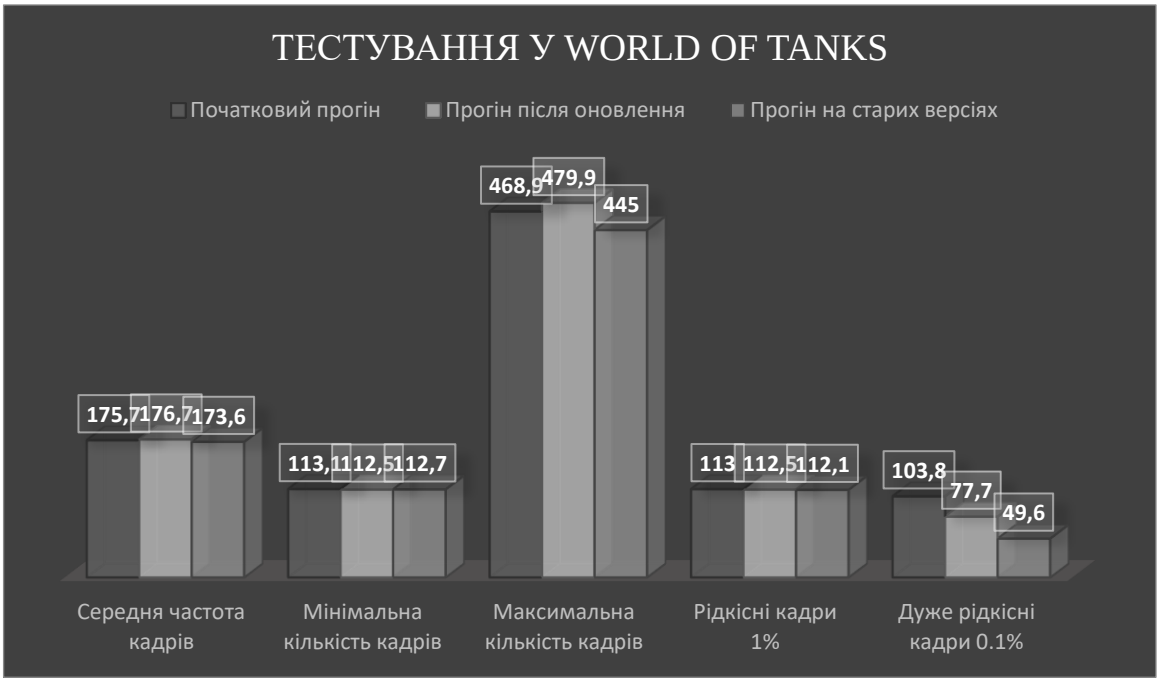

Рис. 3.16. Діаграма порівняння результатів тестування із вимкнутими заплатками у World of Tanks Encore

У випадку з тестуванням у World of Tanks Encore ми бачимо також не значну різницю у всіх параметрах окрім дуже рідкісних кадрів з більшим значенням у початкової системи, та максимальним fps у оновленій системі.

Таблиця 3.12

Порівняння результатів тестування в залежності від версій у FarCry 5

	Заплатки увімкненні		Заплатки вимкненні		
	Початковий прогін	Прогін після оновлення	Початковий прогін	Прогін після оновлення	Прогін на старих версіях
Середня частота кадрів, fps	92.8	94.6	93.4	95	87.6
Мінімальна кількість кадрів, fps	26.3	35.1	65.5	51.6	28.3
Максимальна кількість кадрів, fps	117.5	117.5	116.8	117.7	115
Рідкісні кадри 1%, fps	41.6	50.9	64.1	65.5	47.6
Дуже рідкісні кадри 0.1%, fps	7.2	8.9	9.1	24.3	7

З табл. 3.12 можна побачити різницю в отриманих значеннях. Якщо згадати наприклад результати із тестування у World of Tanks Encore, табл. 3.11, то в даному тесті результат відрізняються навіть у параметрі середньої кількості кадрів. З даних значень видно, що оновлення BIOS дало непоганий приріст до цього параметру, так як найменший показник у тесті із старими версіями. Мінімальна кількість кадрів значно зросла при оновлені, а ще більше зросла при вимкнених заплатках.

Якщо спробувати вибрати найкращий прогін, з проведених саме в FarCry5, то як видно з значень це буде оновлена система із вимкненим захистом, там приріст практично у всіх пунктах.

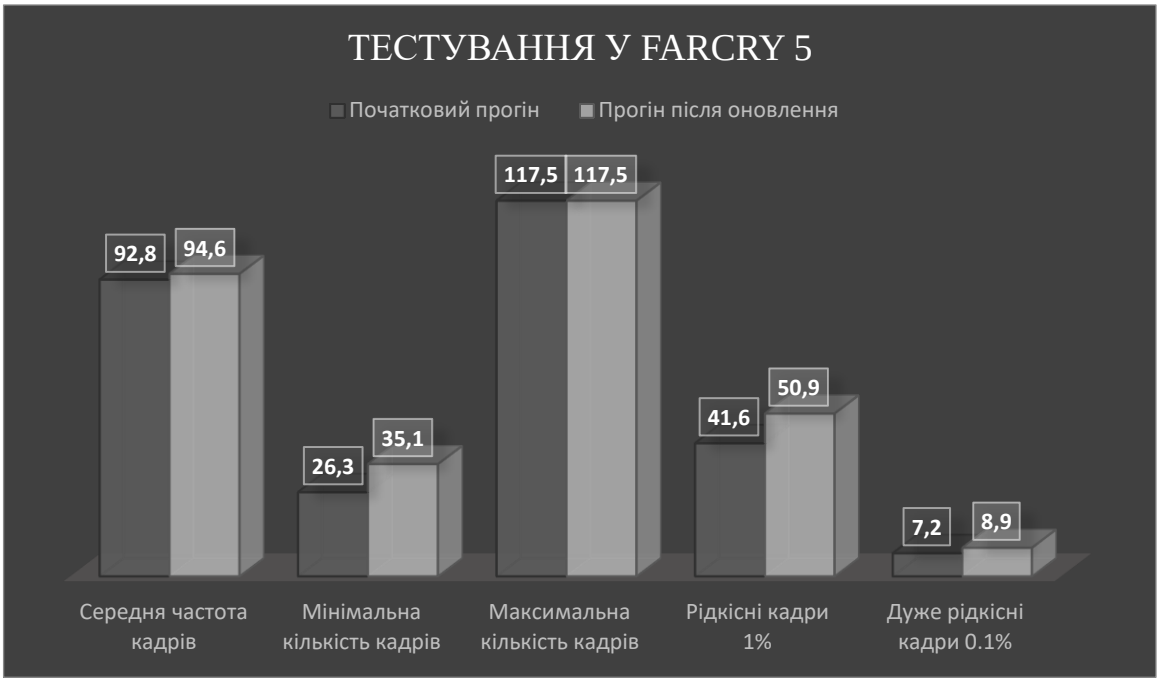

Рис. 3.17. Діаграма порівняння результатів тестування із увімкнутими заплатками у FarCry 5

Рис. 3.18. Діаграма порівняння результатів тестування із вимкнутими заплатками у FarCry 5

Отже після дослідження усіх необхідних даних, можна побачити наступне, що робочі програми, які у даному дослідженні представлено синтетичними тестами, майже не отримують ніяких змін, при оновлені чи

відкаті до старих версій. Також результати у межі похибки у тестах із вимкненими та увімкненими заплатками. Але є цікавий результат, у ігрових застосунках, якщо порівнювати із старими версіями BIOS, та без оновлень Windows, то видно значний приріст продуктивності, у версіях де уже наявні процесорні заплатки. Тобто ясно одне, оновлюватись потрібно. Якщо ж взяти до уваги отримані результати у початковому прогоні, та після оновлення, то можна зауважити суттєвий приріст продуктивності у тестах FarCry 5, а саме в рідкісних, дуже рідкісних і мінімальних значення при увімкнених заплатках та рідкісних і дуже рідкісних при вимкнених заплатках. Саме значення мінімальної кількості кадрів є гіршим, але в межах комфортних. Хоча у тестах в World of Tanks Encore, параметри дуже рідкісних кадрів і є менші, ніж при початкових тестах, але вони все ще в межах комфортних 60.

Таким чином, якщо потрібно вибрати, які версії BIOS чи Windows, із вимкненими чи увімкненими заплатками для робочих програм, то напевне різниці немає, але якщо ж подивитись із сторони ігрових застосунків, то це звичайно останні оновлення, і все таки увімкнені заплатки. Так як не значна втрата в продуктивності, дозволяє отримати повний захист від вразливостей сімейства Meltdown/Spectre.

3.4. Висновки до розділу 3

В третьому розділі кваліфікаційної роботи магістра було проведено практичне дослідження для отримання даних, щодо впливу використання різних версій, засобів захисту в BIOS чи Windows, та їх вплив, при вимкнених та увімкнених заплатках. Це було виконано за допомогою 3 етапів тестування, в якому 1 етап був в ролі чистового, тобто чи потрібно з нього оновлюватись, чи навпаки відкатувати оновлення. Він був проведений, в свою чергу у 2 етапи, з увімкненими та вимкненими заплатками. Наступний етап був проведений на комп’ютерній системі з уже оновленим BIOS, та з всіма оновленнями безпеки Windows, також у 2 етапи, як і попередній. Третім етапом було провести всі ті ж тести, але уже на системі з відкатом всіх оновлень, до моменту виходу

оновлень безпеки, в свою чергу, він був проведений в один етап, так як заплаток ще не було. І фінальним етапом, було проведення висновків на основі отриманих результатів.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Мета кваліфікаційної роботи магістра полягає у методах захисту центральних процесорів комп'ютерів від атак . Під час проведення даної роботи необхідно дотримуватись вимог з охорони праці при роботі з комп'ютерною системою, а також техніки безпеки та протипожежної безпеки при використанні ЕОМ та комп'ютерної техніки. Так як все дослідження проводиться на комп'ютері. І використання отриманих результатів, може бути лише на комп'ютерних системах.

До основних нормативних документів щодо охорони праці користувачів комп'ютерів відносяться НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями», ДСанПіН 3.3-2.007- 98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» та НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні». Згідно із [16, 17], розглянемо вимоги до приміщень, в яких буде розміщуватись робоче місце. У відповідності до НПАОП 0.00-7.15-18, приміщення повинні мати змішане освітлення, тобто природне та штучне. Природне освітлення має здійснюватися через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%. Штучне освітлення мають забезпечувати люмінесцентні лампи. Площа на одне робоче місце повинна становити мінімум 6,0 м2 , при цьому об'єм – мінімум 20,0 м3. Розміщення робочих місць у підвальних приміщеннях, а також на цокольних поверхах заборонено. Приміщення не повинні межувати з іншими приміщеннями, в яких рівні шуму і вібрації перевищують допустимі значення. Покриття підлоги повинне бути матовим з коефіцієнтом відбиття 0,3-0,5. Для внутрішнього оздоблення приміщень слід використовувати спеціальні дифузно-

відбивні матеріали з коефіцієнтами відбиття для стелі 0,7-0,8, для стін 0,5-0,6 [17]. Саме робоче місце теж повинно відповідати вимогам, що описані в вимогах [16,17]. Конструкція робочого місця повинна забезпечити підтримання оптимальної робочої пози. У відповідності до НПАОП 0.00-7.15-18, обладнання і організація робочого місця працюючих з ЕОМ мають забезпечувати відповідність конструкції всіх елементів робочого місця та їх взаємного, розташування ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності. Висота робочого столу, на якому розміщений ПК має знаходитися в межах 680...800 мм, а ширина і глибина – 600...1400 мм і 800..1000 мм відповідно. Стіл також повинен мати достатній простір для ніг, що забезпечить зручну осанку користувача. Конструкція робочого столу повинна відповідати сучасним вимогам ергономіки і забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів. Грубо кажучи робота за комп'ютером не повинна приносити дискомфорт організму користувача. Робочий стілець повинен бути рухомим, регульованим за висотою, за кутом і за нахилом сидіння та спинки. Висота поверхні сидіння стільця має регулюватися в межах 400...500 мм, а ширина і глибина становити не менше ніж 400 мм. Кут нахилу сидіння – до 15 град. вперед і до 5 град. назад. Висота спинки стільця має становити 300..320 мм, ширина – не менше ніж 380 мм, радіус кривизни горизонтальної площини - 400 мм. Кут нахилу спинки має регулюватися в межах 1...30 град. від вертикального положення. Відстань від спинки до переднього краю сидіння має регулюватися в межах 260...400 мм [16]. Монітор ПК має розташовуватися на відстані 600...700 мм від очей користувача. Розташування монітору має забезпечувати зручність зорового спостереження у вертикальній площині під кутом +30 град. до нормальної лінії погляду працівника [16] не заставляючи користувача прихилятись до екрана. Вимоги безпеки при роботі з ПК визначено в НПАОП 0.00-7.15-18. Приміщення повинні бути оснащені аптечками першої медичної допомоги, а також обов’язковим є щоденне вологе прибирання приміщень. Згідно вимог

електробезпеки, ПК повинні підключатися до електромережі тільки за допомогою справних з'єднань. Не допускається підключати ПК до звичайної двопровідної електромережі, в тому числі з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення ПК потрібно виконувати за магістральною схемою. При організації робочих місць електромережу штепсельних розеток для живлення ПК у центрі приміщення прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах [17]. Після закінчення роботи з ПК, він та периферійні пристрої повинні бути відключені від електричної мережі. У разі виникнення певної аварійної ситуації необхідно негайно відключити ПК від електричної мережі. Не допускається виконувати обслуговування, ремонт та налагодження ПК безпосередньо на робочому місці [17]. Основні вимоги до пожежної безпеки вказані в НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні». Згідно з [16], на та під приміщеннями, в яких розміщені ЕОМ, а також у суміжних із ними приміщеннях не дозволяється розташування приміщень категорій А та Б за вибухопожежною небезпекою. Подвійна підлога у приміщеннях з ЕОМ має бути з негорючих матеріалів або матеріалів груп горючості Г1, Г2 з межею вогнестійкості не менше 0,5 години. Простір під нею слід розділяти негорючими діафрагмами на відсіки площею не більше 250 м 2 . Діафрагми повинні мати межу вогнестійкості не менше 0,75 год. Звукопоглинаюче облицювання стін та стель цих приміщень слід виготовляти з негорючих матеріалів або матеріалів груп горючості Г1, Г2. Персональні комп'ютери після закінчення роботи повинні відключатися від мережі. Не рідше одного разу на квартал необхідно очищати від пилу агрегати та вузли, кабельні канали та простір між підлогами [17]. Приміщення повинні бути забезпечені первинними засобами пожежогасіння, а саме вогнегасниками, що використовуються для локалізації і ліквідації пожеж у їх початковій стадії розвитку. Вогнегасники слід встановлювати у легкодоступних та помітних місцях (коридорах, біля входів або виходів з приміщень тощо), а також у пожежонебезпечних місцях, де найбільш вірогідна поява осередків пожежі.

4.2. Джерела, зони дії та рівні забруднень навколишнього середовища у разі аварій на АЕС і хімічно небезпечних об'єктах

Особливе місце у забрудненні оточуючого середовища займає радіоактивне забруднення.

Чорнобильська катастрофа стала наслідком радіоактивного забруднення території України, Білорусі та Росії. Загальна площа радіоактивного забруднення становить понад 30 тис. кв. км.

Слід зазначити, що атомна енергетика в даний час є екологічно чистіша і дешевша, ніж теплова. У розвинутих країнах вона забезпечує від 15 до 70 відсотків усієї електроенергії, що виробляється (Франція — 70 відсотків, США — 17, Швеція — 50, Канада — 15 відсотків). Однак у разі аварії атомні станції становлять дуже серйозну небезпеку для людей і оточуючого середовища. За час експлуатації АЕС у світі сталися три значні аварії: 1961 рік — в Айдахо-Фолсі (США); 1979 рік — на АЕС «Тримайл-Айленд» у Гарисберзі (США), 1986 рік — Чорнобильська АЕС, 2011 префектура Фокусіма, Японія.

Аварії на АЕС мають значні відмінності від ядерних вибухів. Вони відрізняються від ядерних вибухів більшою тривалістю викидів, що змінює напрямок потоків повітряних мас. Тому практично не має можливості прогнозувати розміри зон ураженості. Радіоактивне забруднення оточуючого середовища діє на людину шляхом зовнішнього та внутрішнього опромінення.

Нині спостерігається тенденція до збільшення онкологічних захворювань, захворювань ендокринної системи, систем кровообігу, травлення, а також захворювань, пов'язаних з імунною системою. В зв'язку з тим, що в продуктах викиду перевагу мають довго живучі радіонукліди — цезій-137 (30 років), стронцій-90 (28 років), плутоній-239 (20000 років), зараження буде тривалим. Верховна Рада України ухвалила Закон, який визначає чотири зони радіоактивного забруднення:

- зона періодичного радіоактивного контролю (низьке забруднення, 0,5 — 1 Кі/км2). Дозволено збирання грибів, ягід, лікарських рослин, а також

заготівлю деревини без обмежень. Полювання, рибальство у природних водоймах і річках дозволяється відповідно до правил, що діють на території України, з обов'язковою перевіркою м'яса і риби на вміст у них радіоактивних речовин. У підсобних господарствах ніяких обмежень щодо годівлі та утримання сільськогосподарських тварин і птиці не запроваджується;

- зона посиленого радіоактивного контролю (середнє забруднення, 1—5 Кі/км2). Дозволено збирання, заготівлю грибів, ягід, лікарських рослин і сіна з обов'язковим попереднім дозиметричним контролем. Заготівля деревини і використання продуктів її переробки проводиться без обмежень. У підсобних господарствах рекомендується періодичний вибірковий контроль м'ясних і молочних продуктів, кормів;

- зона гарантованого добровільного відселення (високе забруднення, 5—15 Кі/км2). У цій зоні заготівлю грибів, ягід, хвойної лапини і виробництво хвойно-вітамінного борошна заборонено. Необхідний особливий режим сільського господарства: обмежене землекористування (скорочення рільництва, зменшення обробітку земель), переспеціалізація товарного сільського господарства та насінництва, вирощування технічних культур (льон і інше), розвиток тваринництва, інтенсивне конярство тощо;

- зона відчуження (надзвичайно високе забруднення). Це дослідницький полігон для боротьби із наслідками ядерних катастроф.

Аварії на ХНО – порушення технологічного процесу виробництва, що призводить до викиду в навколишнє середовище токсичних речовин, які можуть викликати ураження людей, тварин, рослин.

Аварії на ХНО можуть бути:

- без руйнування ємностей, цехів, виробництва;
- з руйнуванням ємностей, цехів, виробництва.

За ступенем важкості аварії на ХНО можуть бути:

- без ураження людей (тварин);
- одиничні (кількість потерпілих 1-2 чоловік;
- малі (кількість потерпілих 3-10 чоловік;

- середні (кількість потерпілих 11-50 чоловік;
- великі (кількість потерпілих 51-100 чоловік;
- гігантські (кількість потерпілих >1000 чоловік.

Аварії на ХНО поділяються на категорії:

I. Хімічно заражена тільки територія об’єкту.

II. Хімічно заражена територія об’єкту , а також навколишнє середовище.

III. Регіональні аварії.

IV. Аварії державного масштабу.

V. Аварії з міжнаціональними наслідками.

Під час аварій на ХНО виникають зони хімічного зараження (ЗХЗ). Це територія зараження СДОР у небезпечних для життя людей межах. ЗХЗ включає місце безпосереднього виливу СДОР внаслідок аварії (зона розливу) і територію, на яку поширилися пари СДОР в уражаючих концентраціях (зона заносу). Розміри ЗХЗ визначаються кількістю викиду СДОР внаслідок аварії, їхніми фізико-хімічними властивостями, метеорологічними чинниками та ін. На території ЗХЗ можуть утворитись один чи кілька осередків хімічного ураження.

Було розглянуто зони дії та рівні забруднень навколишнього середовища у разі аварій на АЕС і хімічно небезпечних об'єктах. Одним з найважливішим пунктів, при аваріях на небезпечних об’єктах, це своєчасне повідомлення населення, задля уникнення жертв та спеціалізований комплекс дій для усунення наслідків аварії.

4.3. Висновки до розділу 4

В даному розділі роботи було розглянуто основні нормативні документи та положення з охорони праці, які регулюють умови праці, використання комп’ютерних систем. Також було розглянуто зони дії та рівні забруднень навколишнього середовища у разі аварій на АЕС і хімічно небезпечних об'єктах, що дасть змогу бути більш поінформованим на рахунок цих аварій, та дати уявлення, про можливі дії при виникненні цих небезпечних умов.

ВИСНОВКИ

При написанні кваліфікаційної роботи магістра, у вступі було розписано про актуальність вибраної теми, а саме важливість методів захисту центральних процесорів комп’ютерів від атак. Вказано мету, предмет роботи та практичне застосування її результатів.

В першому розділі, даної було розглянуто саму суть вразливостей, розібрано, що вони можуть бути не лише як програмна чи апаратна вада комп’ютерної системи, а й люди, котрі обслуговують чи працюють на цих машинах. Було розглянуто вразливості систем на базі процесорів Intel та AMD. Досліджено конкретні вразливості сімейства Meltdown та Spectre. Було висвітлені групи дослідників, котрі відкрили дані прогалини в безпеці, та продовжили працювати над ними. Також було показано всі можливі системи захисту, комп’ютерів розділених по категоріях, від найпростіших до найскладніших. Описано можливий вплив на потужність та швидкодію системи, через наявність тої чи іншої системи захисту.

В другому розділі детально розглянуто, що таке витік бічного каналу і яким чином, можна його використати. Було показано способи виявлення наявності даних недоліків в безпеці комп’ютера, як для просунутих, так і для звичайних користувачів. Детально розписано всі програми, які були використані у досліджені. Розглянуто синтетичні тести на базі Cinebench R20 та X265, ігрові тести у World of Tanks Encore та FarCry 5, і супутні застосунки, для отримання результатів, а саме MSI Afterburner.

В третьому розділі було проведено практичне дослідження для отримання даних, щодо впливу використання різних версій, засобів захисту в BIOS чи Windows, та їх вплив, при вимкнених та увімкнених заплатках. Це було виконано за допомогою 3 етапів тестування, в якому 1 етап був в ролі чистового, тобто чи потрібно з нього оновлюватись, чи навпаки відкатувати оновлення. Він був проведений, в свою чергу у 2 етапи, з увімкненими та вимкненими заплатками. Наступний етап був проведений на комп’ютерній

системі з уже оновленим BIOS, та з всіма оновленнями безпеки Windows, також у 2 етапи, як і попередній. Третім етапом було провести всі ті ж тести, але уже на системі з відкатом всіх оновлень, до моменту виходу оновлень безпеки, в свою чергу, він був проведений в один етап, так як заплаток ще не було. І фінальним етапом, було проведення висновків на основі отриманих результатів.

В роботі було розглянуто вразливості сімейства Meltdown та Spectre, системи захисту від них, на базі стандартних засобів BIOS та Windows. Був досліджений вплив на продуктивність системи, в залежності від версій даних засобі та саме використання, чи вимкнення цих заплаток. Як показали дослідження, якщо потрібно вибрати, які версії BIOS чи Windows, із вимкненими чи увімкненими заплатками для робочих програм, то напевне різниці немає, але якщо ж подивитись із сторони ігрових застосунків, то це звичайно останні оновлення, і все таки увімкнені заплатки. Так як не значна втрата в продуктивності, дозволяє отримати повний захист від вразливостей сімейства Meltdown/Spectre.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tanenbaum A.S., Austin T. Structured Computer Organization. Pearson, 2013. 775p.

2. Виявлення вразливостей Spectre/Meltdown. USA, 2018. URL: https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html (дата звернення: 05.11.2020).

3. Pfitzmann B., Waidner M. A General Framework for Formal Notions of «Secure» Systems. Hildesheim, 1994. 24p.

4. Richardson R. CSI Computer Crime & Security Survey. 2008. 30 p.

5. База даних загальновідомих вразливостей інформаційної безпеки. USA, 1999-2020. URL: https://cve.mitre.org/ (дата звернення 06.11.2020).

6. Ermolov M., Goryachy M. How to Hack a Turned-Off Computer, or Running Unsigned Code in Intel Management Engine. Excel, London, 2017. 73 p.

7. 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.

8. 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.

9. Сповільнення системи через Spectre. 2018. URL: https://www.phoronix.com/scan.php?page=article&item=power9-spectre-benchmarks&num=3 (дата звернення: 11.11.2020).

10.Утиліта InSpectre. Laguna Hills, 2018 URL: https://www.grc.com/inspectre.htm (дата звернення: 10.11.2020).

11.Програма для тестування швидкодії системи Cinebench R20. USA, 2020. URL: https://www.maxon.net/en/cinebench (дата звернення: 10.11.2020).

12. Програма для тестування швидкодії системи X265. 2014-2020. URL: https://x265.ru/en/x265-hd-benchmark/ (дата звернення: 10.11.2020).

13.Застосунок для тестування продуктивності системи World of Tanks enCore. Мінськ, 2019. URL: https://worldoftanks.ru/ru/soft/programs/encore/ (дата звернення: 10.11.2020).

14.Застосунок для тестування продуктивності системи FarCry 5. Montreal, 2018. URL: https://store.ubi.com/ru/game?pid=591567f6ca1a6460388b4568&dwvar_591567f6ca1a6460388b4568_Platform=pcdl&edition=Standard%20Edition&source=detail (дата звернення: 10.11.2020).

15. Програма для моніторингу системи MSI Afterburner. URL: https://ua.msi.com/Landing/afterburner (дата звернення: 10.10.2020).

16. Жидецький В.Ц. Охорона праці користувачів комп’ютерів. Львів: Афіша, 2000. 176с.

17. ДСанПіН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин.

Додаток А.

Опубліковані тези конференції за темою дипломної роботи магістра

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Національна академія наук України
Університет імені П'єра і Марії Кюрі (Франція)
Маріборский університет (Словения)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Шяуляйська державна колегія (Литва)
Жешувський політехнічний університет ім. Лукасевича (Польща)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Національний університет біоресурсів і природокористування України (Україна)
Наукове товариство ім. Шевченка
ГО «Асоціація випускників Тернопільського національного технічного університету імені Івана Пулюя»

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том II

IX Міжнародної науково-технічної конференції молодих учених та студентів

25-26 листопада 2020 року

УКРАЇНА
ТЕРНОПІЛЬ – 2020

Матеріали IX Міжнародної науково-технічної конференції молодих учених та студентів.
Актуальні задачі сучасних технологій – Тернопіль 25-26 листопада 2020.

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/.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

9–10 грудня 2020 року

ТЕРНОПІЛЬ
2020

UDC УДК 004.4
Д.Р. Яценко, Н.С. Луцик докт. філос.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ВПЛИВУ ПРОЦЕСОРНИХ ЗАПЛАТОК НА ШВИДКОДІЮ КОМП'ЮТЕРА

UDC 004.4
D.R. Yatsenko, N.S. Lutsyk Ph.D.

RESEARCH OF INFLUENCE OF PROCESSOR SECURITY PATCH ON COMPUTER SPEED

Дослідження впливу використання різних версій систем захисту, вбудованих у BIOS і Windows, та загалом залежність від їх ввімкнення чи примусового вимкнення проводилось за допомогою набору тестових програм. Цей набір порівну складається із засобів синтетичного, тобто робочого тестування, а саме: Cinebench R20 та X265. Також були присутні ігрові застосунки, з вбудованими тестами, на основі гри, а саме: World of Tanks Encore та FarCry 5.

Тести проводились у 2 етапи кожен, за виключенням тестування старих версій, так як там не було засобів захисту від тестованих вразливостей типу Meltdown та Spectre. Тестування проходило спочатку із увімкненими заплатками на конкретній системі, без змін, із вимкненими всіма можливими фоновими процесами, потім із вимкненими заплатками. Наступним етапом було таке ж тестування, але в оновленій системі, з найновішими версіями та оновленнями. Тому під кінець тестування було 3 набори даних, перший прогін із початковими значеннями, другий прогін із оновленою системо, та третій прогін із системою з старими версіями.

Отже після отримання усіх необхідних даних, можна побачити наступне, що синтетичні тестові програми, які у даному дослідженні представлено Cinebench R20 та X265, майже не отримують ніяких змін, при оновлені чи відкаті до старих версій. Тобто беручи до уваги наприклад результат у Cinebench R20 при багатоядерному тесті, ми отримуємо результати у першому прогоні 2930 тестових балів, другому 2944, а у третьому 2910, то ми отримуємо коливання приблизно у 1 відсоток. Також результати у X265 у тестах із вимкненими та увімкненими заплатками не мають явного виграшу, в жодну із сторін. Але є цікавий результат, у ігрових застосунках, якщо порівнювати із старими версіями BIOS, та без оновлень Windows, то видно значний приріст продуктивності, у версіях де уже наявні процесорні заплатки. Якщо ж взяти до уваги отримані результати у початковому прогоні, та після оновлення, то можна зауважити суттєвий приріст продуктивності у тестах FarCry 5, а саме в рідкісних, дуже рідкісних і мінімальних значеннях при увімкнених заплатках та рідкісних і дуже рідкісних при вимкнених заплатках. Саме значення мінімальної кількості кадрів є гіршим, але в межах комфортних 60 кадрів. Хоча у тестах в World of Tanks Encore, параметри дуже рідкісних кадрів і є менші, ніж при початкових тестах, але вони все ще в межах комфортних 60.

Тому, якщо потрібно вибрати, які версії BIOS чи Windows, із вимкненими чи увімкненими заплатками для робочих програм, то напевне різниці немає, але якщо ж подивитись із сторони ігрових застосунків, то це звичайно останні оновлення та увімкнені заплатки. Так як не значна втрата продуктивності, дозволяє отримати повний захист від вразливостей сімейства Meltdown/Spectre. Варто зазначити, що оновлення дають свого роду зменшення втрат швидкодії при застосованих засобах захисту, завдяки пришвидшенню системи в деяких випадках в цілому.