

РЕЦЕНЗІЯ

на дисертаційну роботу
Мазурка Валентина Олеговича
на тему «Створення засобів захисту оперативної пам'яті від атак типу
RowHammer»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертації.

Зі зменшенням розміру транзисторів і збільшенням щільності запису в мікросхемах пам'яті DRAM, фізичні явища, які раніше вважалися незначущими, починають суттєво впливати на надійність зберігання даних. Одним із таких критичних ефектів є вразливість RowHammer, яка дозволяє змінювати значення бітів у сусідніх комірках пам'яті шляхом багаторазового зчитування певного рядка. Це створює ризики не лише втрати цілісності даних, але й потенційного несанкціонованого доступу до конфіденційної інформації на апаратному рівні.

Актуальність представленої Мазурком Валентином Олеговичем дисертаційної роботи полягає у потребі створенні практичних методів та моделей для виявлення та протидії таким атакам із урахуванням реальних характеристик сучасної пам'яті DDR3–DDR5. Зосереджуючись на побудові універсальної тестової платформи та ефективних методів детектування, зокрема з використанням нейромережевих підходів, автор пропонує ґрунтовне рішення для захисту нових поколінь пам'яті, що зберігає ефективність при обмежених ресурсах системи.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- Вперше розроблено методологію збору даних щодо захисту від атак типу RowHammer нових систем пам'яті DDR5.
- Вперше розроблено модель захисту пам'яті DRAM систем на основі машинного навчання, що працює в реальному часі.

- Вперше розроблено модель захисту пам'яті DRAM систем на основі лічильників доступу, що не має вразливостей нерівномірного оновлення.
- Удосконалено методологію тестування вразливостей чіпів DRAM DDR5 щодо атак типу RowHammer шляхом розробки апаратно-програмного комплексу тестового обладнання.

Дані щодо результатів досить повно представлено в матеріалах дисертаційного дослідження, опубліковано в фахових наукових виданнях та апробовано на науково-практичних конференціях з кібербезпеки.

Наукові дослідження були виконані здобувачем на кафедрі інформаційної безпеки КПІ ім. Ігоря Сікорського в рамках НДР на кафедрі інформаційної безпеки згідно вимог щодо забезпечення захищеності та безперебійного функціонування інформаційних та комунікаційних систем об'єктів критичної інфраструктури, визначених в Концепції забезпечення національної системи стійкості, ухваленої Указом Президента України № 479/2021 від 27.09.2021 року під керівництвом кандидата технічних наук, доцента Луценко Володимира Миколайовича.

В дисертаційній роботі поставлене наукове завдання щодо створення засобів захисту оперативної пам'яті від атак типу RowHammer виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Мазурка Валентина Олеговича повністю відповідає Стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації та напрямам досліджень відповідно до освітньої програми Кібербезпека.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям Інформаційні технології.

Згідно зі звітом подібності за результатами перевірки дисертаційної роботи на текстові співпадиння, дисертаційна робота Мазурка Валентина Олеговича є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело. Порушення принципів академічної доброчесності відсутні.

Мова та стиль викладення результатів.

Дисертаційна робота виконана українською мовою. Стиль написання дисертації відзначається академічною строгістю й логічною послідовністю, що

забезпечує належний рівень наукової культури викладення. Автор вміло володіє встановленою технічною термінологією. Структура та текст дисертації викладені у доступному для сприйняття виді, надають можливість нескладного стеження за ходом досліджень від постановки завдання до отриманих результатів.

Дисертація складається з вступу, 4 розділів, висновків та списку літератури. Загальний обсяг дисертації складає 208 сторінок.

У вступі детально розглядається сучасний стан проблеми атак на оперативну пам'ять та доводиться необхідність пошуку нових підходів до її захисту. Поряд із цим формулюються наукові завдання, визначається мета дослідження, обґрунтовується його новизна та актуальність, а також підкреслюється внесок роботи у розвиток прикладних аспектів кібербезпеки.

Перший розділ дисертації присвячений аналізу існуючих досягнень за темою роботи. Розкрито технічні засади функціонування DRAM, показано її вразливість до атак та аналіз сучасних способів захисту. Особливу увагу приділено побудові кеш-пам'яті, механізмам обробки запитів і ключовій ролі кеш-влучань/промахів у визначенні характеру доступу до пам'яті, що є важливим в контексті RowHammer. Проведено класифікацію атак на оперативну пам'ять і детальний аналіз механізму RowHammer. Здійснено огляд захисних методів і їхню оцінку з точки зору ефективності й практичності. Підкреслено потребу у створенні нових рішень, які дозволять виявляти загрозу до того, як вона завдаватиме шкоди. Все це є основою та утворенням подальшого вектору досліджень в рамках дисертаційної роботи.

У другому розділі розглядається практична реалізація експериментальної системи для оцінки вразливості DRAM до RowHammer-атак. Описано процес створення спеціалізованої платформи на FPGA, яка дозволяє відходити від жорстко визначених інтерфейсних стандартів пам'яті та надає змогу експериментального виявлення слабких місць мікросхем. Представлено результати масштабного дослідження чіпів DRAM різних виробників і поколінь, а також аналізу ефективності поширених механізмів захисту.

У третьому розділі дисертації описано підходи до детектування RowHammer-атак, якими є вибірка рядків, використання машинного навчання та частотний масив. Представлено модифікований підхід до вибірки активованих рядків, який дозволяє підвищувати ймовірність виявлення небезпечного доступу. Запропоновано новий параметр – радіус дії атаки, що враховує фізичні характеристики щільності DRAM та потенціал неочевидного впливу на сусідні рядки. Представлено систему детектування на базі трьох типів нейронних мереж, де найефективнішою виявилась модель MLP з точністю 99,7%. Проведено аналіз частотного методу, що використовує лічильники активації для ідентифікації атакуючих рядків. Цей підхід досягає до

99,8% точності, однак вимагає точного налаштування для кожного чіпу та частотної синхронізації. Усі запропоновані стратегії мають свої переваги та недоліки, а їх розгляд дозволяє сформулювати комплексне бачення шляхів ефективного захисту пам'яті.

У четвертому розділі дисертації детально описано імплементацію механізмів захисту від RowHammer-атак у реальну апаратну систему. Першочергово підкреслено важливість використання потужного процесора для моделювання високочастотного доступу до пам'яті. Окрему увагу приділено технічним деталям реалізації частотного масиву, зокрема питанням перетворення часових параметрів у дискретні значення для лічильників. Це дозволяє адаптувати захист під конкретну DRAM-конфігурацію. Тестування в реальному середовищі охоплює як нейромережеві моделі, так і метод частотного масиву.

У висновках дисертаційної роботи описано сутність вирішення актуального наукового завдання щодо створення засобів захисту оперативної пам'яті від атак типу RowHammer. Продемонстровано способи детектування, що здатні виявляти до 99.8% атак на сучасні типи пам'яті DDR4 та DDR5. Також описано наукові та практичні результати роботи.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи.

Наукові результати дисертації висвітлені у 4 наукових публікаціях здобувача, серед яких 4 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України, апробовані на 5 науково-практичних фахових конференціях.

Публікації здобувача відзначаються належним рівнем наукової аргументації, актуальністю тематики та структурною цілісністю. Усі роботи відповідають вимогам до фахових видань і засвідчують дотримання принципів академічної доброчесності, зокрема коректного цитування джерел, аналізу та відсутність запозичень без посилань. Наукові результати, що отримані в дисертаційній роботі, повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

В роботі виявлені наступні недоліки та зауваження:

1. При аналізі існуючих платформ основна увага приділена FPGA-платформі тестування. Мало приділено уваги іншим платформам, наприклад, на процесорах архітектур ARM, RISC-V тощо.

2. Нечітко виконано обґрунтування важливості вхідних ознак у побудованих ML-моделях. Це ускладнює інтерпретацію результатів і знижує довіру до їх застосування в системах критичної інфраструктури.

3. Не повною мірою розкрито питання масштабування системи детектування в великих мережевих комплексах. Не вказано, як вплине імплементація моделей захисту на затримки в роботі при розширенні систем до промислового рівня.

4. Не наведено повного переліку відомостей щодо роботи системи в реальних умовах. Тестування проводилось у переважно контрольованому середовищі, без належної кількості реалістичних багатфакторних сценаріїв. Можуть з'явитись додаткові питання щодо виявлення атак в умовах значних зовнішніх шумів.

5. Не проведено оцінювання впливу температурного режиму на результати тестування. Це питання не було передбачено експериментом як одного з ключових факторів, що впливає на стабільність DRAM і ефективність RowHammer-атак.

6. Запропонована методологія детектування атак RowHammer на основі частотних масивів не передбачає програмного модулю для автоматичної адаптації до нових чіпів DRAM в частотних масивах. Вона вимагає повторного навчання чи ручної корекції порогу виявлення атаки A_{RH} відповідно до кожного чипа пам'яті.

7. Використані моделі машинного навчання, наприклад, MLP, CNN, LSTM в методах виявлення атак є базовими та не є на сьогоднішній день найефективнішими. Адже мають місце і інші, новітні моделі, які можуть дати кращі результати.

Вважаю, що висловлені зауваження та недоліки не зменшують значущості отриманих наукових результатів та практичної цінності дисертаційної роботи в цілому.

Висновок про дисертаційну роботу.

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Мазурка Валентина Олеговича на тему «Створення засобів захисту оперативної пам'яті від атак типу RowHammer» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням. Сукупність отриманих наукових та практичних результатів є вирішенням наукового завдання, що має істотне значення для галузі знань Інформаційні технології. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п. 6 – 9 «Порядку присудження

ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач Мазурок Валентин Олегович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Рецензент:

Професор Спеціальної кафедри №1 ІСЗЗІ КПІ ім. Ігоря Сікорського

д.т.н., професор

«05» 06 2025 року

Сергій ІВАНЧЕНКО

Підпис д.т.н., професора Іванченка С.О. засвідчую.

Заступник начальника Інституту

(з наукової роботи)

Сергій КОНЮШОК

