ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Національного технічного
університету України
"Київський політехнічний інститут
імені Ігоря Сікорського"
к.т.н., доц.
Тетяна ЖЕЛЯСКОВА

"05" 03 2025 р.

ВИТЯГ

з протоколу № 4/2025 від 05 березня 2025 р. розширеного засідання
кафедри інформаційної безпеки
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"

БУЛИ ПРИСУТНІ:

- з кафедри інформаційної безпеки:

завідувач кафедри д.т.н. професор Ланде Д. В., д.т.н. професор Мачуський Є. А., к.т.н. доцент Стьопочкіна І. В., к.т.н. доцент Демчинський В. В., к.т.н. доцент Гальчинський Л. Ю., к.т.н. доцент Коломицев М. В., д.т.н. професор Качинський А. Б., с.н.с доцент Смирнов С. А., старший викладач Наконечна Ю. В., к.т.н. доцент Луценко В.М., к.т.н. доцент Прогонов Д.О., асистент Кіреєнко О.В., ст.викладач Степаненко В.М, к.т.н. доцент Репа Ф.М, асистент Личик В. В., асистент Полуциганова В.І., к.т.н. доцент Носок С.О., к.т.н. доцент Ільїн М.І., к.ф.-м.н. професор Півень О.Б., к.т.н. доцент Литвинова Т.В.;

- з кафедри математичних методів захисту інформації:

в.о. завідувача кафедри, к.т.н. доцент Яковлєв С. В.;

- з інших кафедр КПІ ім. Ігоря Сікорського:

д.т.н., професор науково-дослідницького центру ІСЗЗІ «КПІ ім. Ігоря Сікорського» Іванченко С. О.

СЛУХАЛИ:

1. Повідомлення аспіранта кафедри інформаційної безпеки Мазурка Валентина Олеговича за матеріалами дисертаційної роботи "Створення засобів захисту оперативної пам'яті від атак типу RowHammer", поданої на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації.

Освітньо-наукова програма Кібербезпека.

Тему дисертаційної роботи "Створення засобів захисту оперативної пам'яті від атак типу RowHammer" затверджено на засіданні Вченої ради Навчально-наукового фізико-технічного інституту КПІ імені Ігоря Сікорського (протокол № 20 від "29" листопада 2021 року) та перезатверджено на засіданні Вченої ради (факультету, інституту) засіданні Вченої ради Навчально-наукового фізико-технічного інституту КПІ імені Ігоря Сікорського (протокол № 10 від "12" вересня 2024 року).

Науковим керівником затверджений доцент, к.т.н. Луценко В. М.

2. Запитання до здобувача.

Запитання по темі дисертації ставили:

Д.т.н. професор Мачуський Є. А., д.т.н. професор Ланде Д. В., д.т.н. професор Качинський А. Б., д.т.н., професор науково-дослідницького центру ІСЗЗІ «КПІ ім. Ігоря Сікорського» Іванченко С. О.

3. Виступи за обговореною роботою.

В обговоренні дисертації взяли участь:

Д.т.н. професор Мачуський Є. А., д.т.н. професор Ланде Д. В., д.т.н. професор Качинський А. Б., к.т.н. доцент Стьопочкіна І. В., с.н.с доцент Смирнов С. А.

УХВАЛИЛИ:

ПРИЙНЯТИ такий висновок про наукову новизну, теоретичне та практичне значення результатів дисертаційного дослідження:

1. Актуальність теми дослідження Пам'ять є ключовим компонентом обчислювальних систем. Вона використовується для зберігання вхідних даних, проміжних змінних і кінцевих результатів будь-якої програми. У 2014 році професор Кім Йонг та його колеги з університету Карнегі-Мелона опублікували першу публічну статтю про помилки та спотворення даних в комірках DRAM, спричинені частими та прицільними активаціями потрібних рядків пам'яті, названу RowHammer. Дослідження, проведене лабораторією Касперського та Університетом Цюріха в кінці 2024 року показало, що на даний момент такий тип атак неможливо відрізнити від штатної роботи сучасних типів пам'яті DDR4 та DDR5, що є серйозною загрозою для обчислювальних систем та даних, що на них зберігаються. Саме тому захист від подібного роду атак є актуальною проблемою сучасних обчислювальних систем і, зважаючи на динаміку і тренди розвитку пам'яті, зокрема DRAM, ставатиме лише актуальнішою в майбутньому.

2. Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконувалась у відповідності до наукової складової освітньо-наукової програми «Кібербезпека». Наукові дослідження виконувались здобувачем на кафедрі інформаційної безпеки КПІ ім. Ігоря Сікорського 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 доцента КПІ ім. Ігоря Сікорського, кандидата технічних наук Луценка В.М. Тематика роботи включена до плану науково-дослідних робіт на кафедрі інформаційної безпеки «КПІ ім. Ігоря Сікорського», узгодженого з центром досліджень та розробок «Самсунг РнД Інститут Україна».

3. Наукова новизна отриманих результатів

У дисертації вперше одержані такі нові наукові результати:

- 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.

4. Теоретичне та практичне значення результатів роботи, впровадження

Отримані в дисертаційній роботі результати можуть бути застосовані в різних областях діяльності для підвищення захищеності пам'яті обчислювальних систем від атак типу RowHammer.

Створена спеціалізована плата тестування пам'яті на основі FPGA для роботи з новими чіпами DDR5 та запропоновано програмний комплекс захисту даних від спотворення під час атак типу RowHammer на основі двох принципів детектування, що здатні захищати обчислювальні системи в реальному часі.

Теоретичні та практичні результати дослідження застосовуються у спільній роботі кафедри інформаційної безпеки НТУУ «КПІ ім. Ігоря Сікорського» та центру досліджень та розробок «Самсунг РнД Інститут Україна».

5. Апробація результатів дисертації

Апробація матеріалів дисертаційного дослідження проведено на 5 науково-практичних конференціях.

6. Дотримання принципів академічної доброчесності

За результатами науково-технічної експертизи (експерт к.т.н. доцент Коломицев М. В.) дисертація Мазурка Валентина Олеговича визнана оригінальною роботою, яка не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача

За результатами досліджень опубліковано 9 наукових публікацій, у тому числі:

- 4 статті у наукових фахових виданнях України за спеціальністю, 125 Кібербезпека та захист інформації
- 5 тез виступів на наукових конференціях;

1. Mazurok, V., & Lutsenko, V. «An analytical overview and trend analysis of RowHummer vulnerabilities for various DRAM vendors.» Social Development and Security, 14(3), P 238-244.
URL: https://doi.org/10.33445/sds.2024.14.3.16 (date of access 26.12.2024)

У роботі здобувачем показано процес створення тестової платформи для тестування чіпів DRAM на предмет вразливості типу RowHammer та показано дані тестування чіпів типу DDR3 та DDR4. Дані сформовано в графіки та показано прогнозовані тренди розвитку вразливості.

2. Mazurok, V., & Lutsenko, V. «Enhancing Row-Sampling-Based RowHammer defense methods with Machine Learning approach» Theoretical and Applied Cyber Security Vol. 6 No. 2 P 31-35 URL: https://doi.org/10.20535/tacs.2664-29132024.2.319008 (date of access: 26.12.2024)

У роботі здобувачем наведено розроблений алгоритм детектування атак типу RowHamtmer за допомогою нейронних мереж. Представлено дані навчання та тестування трьох видів мереж та показано їх недоліки та переваги.

3. Mazurok, V., & Lutsenko, V. «Improving the effectiveness of Row-Sampling methods to protect against Row-Hummer attacks». Social Development and Security, 14(6), P 61-67. URL: https://doi.org/10.33445/sds.2024.14.6.7 (date of access: 26.12.2024)

У роботі здобувачем представлено розроблену математичну модель представлення пам'яті DRAM та показано недоліки методу детектування заснованого на вибірці рядків. Показано доповнення та математичний апарат що покращує даний алгоритм детектування атак типу RowHamtmer за рахунок врахування неоднорідності пам'яті та радіусу дії збурень.

4. Mazurok, V., & Lutsenko, V. «Detecting RowHummer attacks using frequency arrays». Social Development and Security. 2025. 15(1). P. 130-136. https://doi.org/10.33445/sds.2025.15.1.12 (date of access: 05.03.2025)

У роботі здобувачем представлено розроблену математичну модель захисту пам'яті DRAM на основі лічильників доступу та розрахунку частоти активації. Показано математичний апарат для детектування атак типу RowHamtmer без недоліків нерівномірного оновлення лічильників.

5. Мазурок В. Луценко В. «Аналітичний огляд атаки RowHammer на сучасну пам'ять» Міжнародна науково-практична інтернет-конференція «Виклики і загрози для критичної інфраструктури» м. Київ, 8–10 лист. 2022 року, С. 316–317.

У дослідженні здобувачем продемонстровано процес розробки тестової платформи для перевірки чіпів DRAM на наявність вразливості типу RowHammer. Проведено тестування чіпів пам'яті стандартів DDR3 та DDR4, результати якого представлені у вигляді графіків, що ілюструють прогнозовані тенденції у розвитку цієї вразливості.

6. Мазурок В. Луценко В. «Практична ефективність RowSampling для захисту від RowHammer» V Міжнародна науково-практична конференція "Trends of modern science and practice", 8–11 лют. 2022 р., Анкара, Туреччина, С. 97–104.

У дослідженні здобувачем розроблено математичну модель для опису пам'яті DRAM, а також проаналізовано недоліки методу детектування вразливостей, заснованого на вибірці рядків. Зокрема, було відзначено, що цей підхід потребує значної оптимізації для забезпечення більшої точності та ефективності в умовах сучасних високопродуктивних систем.

7. Mazurok, V., & Lutsenko, V. «Mathematical model of DRAM for RowHammer protection» XI Міжнародна науково-практична конференція "Інформаційні технології та безпека", м. Київ, 30 лист. 2023 р. С. 232-234.

У дослідженні здобувачем представлено математичну модель для опису пам'яті DRAM, яка стала основою для розробки математичного апарату. Цей апарат дозволяє враховувати неоднорідність структури пам'яті та радіус дії збурень, що створює базу для створення ефективних алгоритмів детектування атак типу RowHammer.

8. Mazurok, V., & Lutsenko, V. «Discovering DRAM access patterns for machine learning sample finding» XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», м. Київ, 12–13 трав. 2023 р С. 348–352.

У роботі здобувачем показано основні схожості моделі доступу до пам'яті під час атак типу RowHammer. Це грунтовне дослідження показує головні елементи, які можуть допомогти детектувати атаку і які можна використовувати для навчання нейромереж та моделей.

9. Mazurok, V., & Lutsenko, V. «Machine learning methods of RowHammer mitigation» IX Міжнародна науково-практична конференція «Development of innovation systems: trends, challenges, prospects», 04–07 бер. 2025 р., Гамбург, Німеччина С. 342–345.

У роботі здобувачем продемонстровано навчання моделей машинного навчання на даних доступу до пам'яті під час атак типу RowHammer. Показано ефективність детектування кількома моделями та оптимізацію зайнятого ними простору відносно знайдених даних.

Якість та кількість публікацій відповідають «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.

ВВАЖАТИ, що дисертаційна робота Мазурка Валентина Олеговича "Створення засобів захисту оперативної пам'яті від атак типу RowHammer", що подана на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації за своїм науковим рівнем, новизною отриманих результатів, теоретичною та практичною цінністю, змістом та оформленням повністю відповідає вимогам, що пред'являють до дисертацій на здобуття ступеня доктора філософії та відповідає напрямку наукового дослідження освітньо-наукової програми КПІ ім. Ігоря Сікорського Кібербезпека зі спеціальності 125 – Кібербезпека та захист інформації.

РЕКОМЕНДУВАТИ:

1. Дисертаційну роботу "Створення засобів захисту оперативної пам'яті від атак типу RowHammer", подану Мазурком Валентином Олеговичем на здобуття наукового ступеня доктора філософії, до захисту у разовій спеціалізованій вченій раді.

2. Вченій раді КПІ ім. Ігоря Сікорського утворити разову спеціалізовану вчену раду у складі:

Голова:

Д.т.н., доцент кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського **Прогонов Дмитро Олександрович**;

Члени:

Рецензенти:

К.т.н., доцент кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського **Коломицев Михайло Володимирович**;

Д.т.н., професор науково-дослідницького центру ІСЗЗІ КПІ ім. Ігоря Сікорського **Іванченко Сергій Олександрович**;

Офіційні опоненти:

Д.т.н., доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка **Лаптєв Олександр Анатолійович**;

Д.т.н., завідувач кафедри робототехнічних і телекомунікаційних систем та кібербезпеки Черкаського державного технологічного університету **Палагін Володимир Васильович**.

Головуючий на засіданні
д.т.н., професор, завідувач
кафедри інформаційної безпеки
КПІ ім. Ігоря Сікорського _____ Дмитро ЛАНДЕ

Вчений секретар
кафедри інформаційної
безпеки к.т.н., доцент _____ Володимир ДЕМЧИНСЬКИЙ