Голові разової спеціалізованої
вченої ради PhD 11440
Хмельницького національного університету
доктору технічних наук, професору
Сергію ЛИСЕНКО
29016, м. Хмельницький,
вул. Інститутська, 11

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

кандидата технічних наук, доцента **Волокити Артема Миколайовича**
на дисертаційну роботу **Стецюка Юрія Васильовича**
на тему: «Методи та засоби забезпечення безпеки спеціалізованих мережних операційних систем», подану до захисту на здобуття наукового ступеня
доктора філософії з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

1. Актуальність теми дисертаційної роботи

Інформаційні технології сьогодні використовуються практично у всіх сферах діяльності організацій, забезпечуючи автоматизацію рутинних операцій. Це також стосується і корпоративних мереж, в яких ведеться обробка, накопичення та передача інформації, яка постійно знаходиться в прицілі кіберзловмисників. Розробники зловмисного ПЗ активно досліджують вразливості апаратного та програмного забезпечення, в тому числі вразливості операційних систем (ОС) з метою отримання доступу до конфіденційної інформації, при цьому постійно удосконалюються способи використання зловмисного програмного забезпечення (ЗПЗ).

В той же час успішне забезпечення захисту інформації в комп'ютерних системах (КС) в першу чергу залежить від стійкості основного програмного компонента - операційної системи, особливо якщо це ОС мережного типу. Незважаючи на великий обсяг наукових досліджень в частині розроблення методів побудови захисних механізмів ОС і, відповідно, отриманих наукових результатів, ця наукова задача і на сьогодні залишається надзвичайно актуальною.

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

Дисертаційне дослідження виконувалось у рамках науково-дослідної тематики Хмельницького національного університету, зокрема держбюджетної науково-дослідної теми № 2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (номер державної реєстрації: 0124U000980), в якій автор дисертації був виконавцем.

3. Наукова новизна отриманих результатів.

Даючи оцінку головним здобуткам дисертаційної роботи, слід зробити акцент на таких основних наукових результатах:

- уперше запропоновано нову модель частково-централізованої системи безпеки ОС, яка, на відміну від наявних рішень, для контролю переміщення інформації використовує механізм маркування конфіденційних даних. Цей механізм є базовим елементом архітектури мережної ОС та забезпечує можливість динамічної передачі керування між її вузлами.

- уперше розроблено метод низькорівневого маркування конфіденційної інформації для захищених спеціалізованих ОС, який, на відміну від відомих підходів, реалізується на межі програмно-апаратної взаємодії засобів комп'ютерної системи. Це дає змогу підвищити стійкість КС до витоку

конфіденційної інформації через оперативну пам'ять під впливом ЗПЗ та комп'ютерних атак, забезпечити контроль руху конфіденційних даних каналами КС та блокувати несанкціоновані операції з ними.

- уперше розроблено метод випадкової динамічної передачі керування між центральними керівними модулями вузлів мережної ОС, який, на відміну від відомих методів, передбачає постійну наявність резервного керівного вузла, зберігання кожним вузлом локальної бази привілеїв і актуалізацію основної бази привілеїв та активних процесів мережі шляхом реплікації локальних баз під час виконання ним керівної ролі. Такий підхід скорочує час передачі керування, зменшує ризик втрати актуальних даних про привілеї й активні процеси та, відповідно, знижує ризик втрати конфіденційної інформації в умовах впливу ЗПЗ і комп'ютерних атак.

- уперше розроблено новий метод кількісної оцінки стійкості ОС до витоку інформації, який, на відміну від існуючих методів, ґрунтується на спільній для всіх досліджуваних об'єктів множині параметрів як аргументах інтегрального показника стійкості. При цьому кожна множина локальних параметрів у межах ОС пов'язується з власною системою вагових коефіцієнтів, що підвищує чутливість оцінювання до змін у системах і точність урахування впливу кожного локального параметра на інтегральний показник.

В дисертаційній роботі повністю виконано поставлене завдання щодо розробки засобів забезпечення безпеки спеціалізованих мережних операційних систем. Результати дисертаційного дослідження свідчать про те, що здобувач повною мірою оволодів методологією наукової діяльності.

4. Короткий аналіз основного змісту дисертації

Науковий рівень викладення дисертації відповідає вимогам МОН України. Назва дисертації адекватно і в повній мірі відображає її зміст.

У *вступі* обґрунтовано актуальність теми дисертації, визначено мету, предмет та об'єкт дослідження, визначені основні завдання, відображено наукову новизну і окреслено практичне значення роботи, підтверджено впровадження результатів, та надано інформацію про особистий внесок здобувача, апробацію та публікацію.

У *першому розділі* здійснено аналіз предметної області дослідження, особливо, що стосується існуючих вразливостей мережних ОС та ситуацій, які часто використовуються зловмисниками для проникнення в комп'ютерні системи. Також проведено аналіз захисних механізмів, реалізованих в сучасних комерційних та некомерційних мережних ОС.

Здійснено критичний огляд наукової літератури та існуючих рішень протидії використанню вразливостей в ПЗ та апаратних засобах КС. На основі проведеного аналізу сформульовано науково-технічну задачу дисертаційного дослідження та визначено комплекс конкретних завдань, розв'язання яких спрямоване на забезпечення безпеки спеціалізованих мережних операційних систем.

У другому розділі представлено метод низькорівневого маркування конфіденційної інформації, в якому контроль конфіденційності винесений на межу апаратно-програмної взаємодії в комп'ютерній системі, що дає можливість ефективно перекривати більшість каналів витоку конфіденційної інформації через оперативну пам'ять (ОП). Приведено приклад реалізації даного методу з використанням принципів роботи сучасних процесорів.

Також представлено модель частково-централізованої системи безпеки з імплементованим методом маркування. Показано підхід до побудови архітектури спеціалізованої мережної ОС з підвищеними параметрами стійкості до витоку конфіденційної інформації.

У третьому розділі описано розробку методу випадкової динамічної передачі керування між вузлами комп'ютерної системи на основі моделі

частково-централізованої системи безпеки КС. Метод включає 6 кроків, виконання яких призводить до періодичної міграції керівного центру між вузлами системи, ускладнюючи атаки на поточний керівний вузол. Детально показано передачу керування між вузлами КС під час штатного режиму роботи та під час збоїв, виконано розрахунок ефективності частково-централізованою системи безпеки ОС порівняно з централізованою системою відповідно до розробленої методики.

В цьому ж розділі представлено метод кількісної оцінки рівня стійкості ОС до витоку інформації з покращеною вибірковістю за рахунок множини вагових коефіцієнтів, які знаходяться в функціональній залежності не тільки від складових інтегрального параметра, но і від об'єкта оцінки. Такий підхід дозволив більш точно врахувати роль і вплив кожного локального параметра на інтегральний параметр, що в свою чергу дозволяє застосовувати цей метод як до абстрактних моделей ОС, так і для оцінювання фізично існуючих ОС.

У четвертому розділі представлено методику визначення ефективності системи безпеки ОС з імплементованим в неї методом низькорівневого маркування конфіденційної інформації. Також представлено середовище для постановки експериментів та описання проведених експериментів. За результатами експериментів виконано необхідні розрахунки ефективності та продуктивності для варіантів ОС з імплементацією в неї метода низькорівневого маркування та без імплементації.

У *висновках* сформульовано основні та практичні результати дисертаційного дослідження, що підтверджують досягнення поставленої мети та розв'язання всіх завдань. Надано конкретні рекомендації щодо використання розроблених методів та засобів підвищення стійкості спеціалізованих мережевих ОС до витоку інформації.

5. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, їх достовірність

Сформульовані у дисертації наукові положення, висновки та рекомендації є аргументованими і підкріплені практичною реалізацією.

Наукова обґрунтованість положень і висновків дисертації забезпечена аналізом літературних джерел, чітким формулюванням завдань дослідження та використанням сучасних методологічних підходів.

Достовірність одержаних результатів підтверджена їх апробацією на міжнародних та всеукраїнських наукових конференціях, а також практичним впровадженням.

6. Практичні результати роботи

Практичне значення отриманих результатів роботи полягає у тому, що по проведених здобувачем дослідженнях розроблено архітектуру частково-централізованої системи безпеки спеціалізованої мережної ОС, алгоритми та засоби забезпечення стійкості ОС до витоків інформації та її захисту в ІС, що працюють під керуванням такої ОС в умовах впливів ЗПЗ та комп'ютерних атак. Це дало змогу створювати спеціалізовані ОС з покращеними характеристиками стійкості до витоків конфіденційної інформації та її захисту, що працюють в умовах впливів ЗПЗ та комп'ютерних атак.

Застосування методу контролю руху конфіденційної інформації в комп'ютерній системі базований на її маркуванні спеціальним атрибутом конфіденційності на рівні дескриптора сторінок пам'яті кожного процесу, дозволило виключити витік інформації по такому каналу, як оперативна пам'ять, який часто є ціллю ЗПЗ та КА. Представлені в роботі розрахунки показали, що система безпеки ОС із імплементованим в неї методом низькорівневого маркування конфіденційної інформації має кращу ефективність на 18,28 % в

частині стійкості до витоків інформації порівняно з стандартним підходом, що підтверджено результатами проведених експериментальних досліджень.

Теоретичні та практичні результати дослідження впроваджені в ТОВ Ультра ІТ (м. Хмельницький), ТОВ ДЕВІКС ДІДЖИТАЛ (м. Хмельницький), ТОВ Nolt technologies (м. Хмельницький), а також, в освітньому процесі Хмельницького національного університету на кафедрі комп'ютерної інженерії та інформаційних систем при викладанні дисциплін «Технічна діагностика і надійність комп'ютерних пристроїв», «Безпека та захист комп'ютерних систем».

7. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладу наукових положень та результатів в опублікованих працях.

Дисертаційна робота має логічну структуру і складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та чотирьох додатків. Повний обсяг роботи становить 267 сторінок друкованого тексту, з них анотація – на 14 стор., зміст – на 5 стор., перелік умовних скорочень – на 1 стор., основний текст – на 148 стор., список із 140 використаних джерел – на 18 стор., додатки – на 73 стор. Дисертація містить 51 рисунок та 10 таблиць.

Робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 року №40 (Із змінами, внесеними згідно з Наказом Міністерства освіти і науки № 759 від 31.05.2019).

У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

За результатами досліджень опубліковано 5 статей у наукових фахових виданнях України, отримано одне свідоцтво про реєстрацію авторського права на твір (програму). Також результати дисертації були апробовані на 5 наукових

фахових конференціях з публікацією доповідей у збірниках матеріалів конференцій, з яких 3 праці індексовані в наукометричній базі Scopus.

Усі сформовані наукові положення і результати дисертації належним чином оприлюднені у наукових публікаціях здобувача, які всебічно відображають концептуальні засади проведеної роботи, ключові наукові здобутки та їхню практичну цінність. У працях опублікованих у співавторстві, особистий внесок здобувача є вагомим та полягає в генеруванні наукових ідей, розроблені математичних моделей, алгоритмічного забезпечення, а також в безпосередньому проведені експериментальних досліджень та аналізі отриманих даних.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

8. Мова та стиль дисертаційної роботи

Текст дисертаційної роботи викладено в логічній послідовності. Дисертація містить достатню кількість ілюстративного матеріалу – схем, рисунків, графіків і таблиць. Мова викладу, стиль та оформлення роботи повністю відповідають установленим вимогам до наукових праць.

9. Зауваження та дискусійні положення щодо змісту дисертації

Зауваження та рекомендації до дисертації:

1. У першому розділі дисертаційної роботи більш детально розглянуто частково - централізований підхід реалізації розподілених систем. В той же час мало уваги приділено аналізу децентралізованого підходу – в цьому випадку висновки в кінці першого розділу були би краще обґрунтованими.

2. У дослідженні запропоновано абстрактну модель частково централізованої системи керування безпекою, яка дозволяє отримати архітектуру безпеки ОС, позбавлену проблеми витоку конфіденційної

інформації при низькорівневих атаках ЗПЗ шляхом включення до складу ОС механізму маркування конфіденційної інформації. Було б доцільно визначити межі при яких застосування запропонованої моделі залишається адекватним.

3. В другому розділі досить детально описано кроки запропонованого методу низькорівневого маркування конфіденційної інформації та приклад його реалізації в ОС на базі сучасних процесорів, але при цьому, в дисертаційній роботі відсутня інформація про те, чи існують якісь обмеження, що можуть унеможливити реалізацію цього методу.

4. Для проведення експериментів в ході виконання завдань дисертаційного дослідження в якості експериментального середовища для більшості експериментів використовувалась віртуальна мережа з чотирьох-п'яти віртуальних машин. Реальні корпоративні мережі значно чисельніші, це може вплинути на розрахунок коефіцієнту ефективності в запропонованих методах.

5. На рисунках 2.17, 2.18 (стор. 83, 85) показані розроблені графові моделі централізованої та частково-централізованої системи безпеки ОС. Було б більш інформативно, якби ребра графів вказували на порядок взаємодії між елементами моделі та виконувану функцію.

Зазначені зауваження істотно не впливають на зміст дисертаційної роботи та не знижують її наукову новизну та практичну цінність.

Висновки щодо дисертації в цілому

На основі викладеного вище вважаю, що дисертація Стецюка Юрія Васильовича на тему «Методи та засоби забезпечення безпеки спеціалізованих мережних операційних систем», що подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам пп. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора

філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (із змінами, внесеними згідно з Постановами КМ № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024), а її автор, Стецюк Юрій Васильович, заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент:

доцент кафедри обчислювальної техніки
Національного технічного університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»,
кандидат технічних наук, доцент Артем ВОЛОКИТА

05.01.2026