Голові разової спеціалізованої
вченої ради PhD 11440
Хмельницького національного
університету
доктору технічних наук,
професору Сергію ЛИСЕНКО

# РЕЦЕНЗІЯ

на дисертаційне дослідження Стецюка Юрія Васильовича
за темою «Методи та засоби забезпечення безпеки спеціалізованих мережних операційних систем», подане на здобуття ступеня доктора філософії
з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

*Актуальність теми дослідження та її зв'язок із планами наукових робіт університету.*

Інтенсивний розвиток інформаційних технологій спричинив радикальні зміни у функціснуванні сучасного суспільства. Вся інформаційна діяльність перебуває під постійним впливом зловмисного програмного забезпечення (ЗПЗ), яке динамічно розвивається, адаптується та ускладнюється. Зловмисні програми охоплюють увесь спектр інструментів порушника, від простих сценаріїв до цілеспрямованих складних атак, що враховують особливості конкретних платформ і мережних сервісів, і це створює безперервний тиск на їх системи захисту та вимагає постійного їх оновлення.

З огляду на поширеність мережних ОС у корпоративних середовищах особливої ваги набувають засоби протидії використанню їх вразливостей. Саме мережні ОС часто становлять ключову ланку цифрової інфраструктури, а тому зловмисники активно досліджують і експлуатують їх слабкі сторони. Аналіз сучасного стану сектору захисту інформації підтверджує, що проблема безпеки залишається надзвичайно високою. Зростання кількості інцидентів, ускладнення методів атак та розширення поверхні потенційних загроз вимагають від дослідників і практиків поглиблених рішень. Захист інформації перетворюється на невід'ємний стратегічний компонент розвитку корпоративних ІС.

Саме спробі вирішення однієї з названих проблем присвячено дисертаційне дослідження Стецюка Ю.В.. Ним, для підвищення стійкості ОС до витоку конфіденційної інформації (КІ), запропоновано використання підходу, базованого на частковій централізації керування ресурсами безпеки з динамічною передачею управління мережею між її вузлами при побудові систем безпеки спеціалізованих мережних ОС які працюють в умовах впливів зловмисного програмного забезпечення та комп'ютерних атак (КА).

Дослідження, результати яких наведено в дисертації, проведені у рамках науково-дослідної тематики Хмельницького національного університету:

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 яких автор дисертації був виконавцем.

Загалом, обраний дисертантом напрям досліджень є актуальною науково-прикладною задачею.

*Формулювання наукової задачі, мети й задачі дослідження.*

Здобувачем правильно визначено об'єкт і предмет дослідження, відповідно до висунутої загалегідь гіпотези дослідження. Так, об'єктом дослідження є процес забезпечення стійкості мережних ОС до витоку конфіденційної інформації, що обробляється в інформаційних системах під їх керівництвом в умовах впливів ЗПЗ та КА. Предметом дослідження є моделі, методи та засоби забезпечення стійкості мережних операційних систем до витоку конфіденційної інформації, що обробляється в комп'ютерних системах під її керуванням в умовах впливів ЗПЗ та КА.

Мету дисертаційної роботи визначено, як покращення безпеки мережних операційних систем за рахунок випадкових динамічних передач керування між вузлами та низькорівневого маркування конфіденційної інформації у вузлах комп'ютерних мереж.

Поставлена мета досягнена в результаті розв'язання таких завдань: 1) проведено аналіз методів забезпечення безпеки спеціалізованих мережних ОС, їх виявлених вразливостей щодо впливів різних типів ЗПЗ і КА та їх потенційно можливих каналів витоку інформації, які обробляється в КС під їх керуванням; 2) розроблено абстрактну модель частково-централізованої системи керування механізмами безпеки з урахуванням шляхів витоків КІ; 3) розроблено метод забезпечення стійкості ОС до витоків КІ базований на використані низькорівневого маркування сторінок оперативної пам'яті (ОП) з КІ в умовах впливів ЗПЗ та КА; 4) розроблено метод динамічної передачі керування між вузлами комп'ютерної мережі для системи керування безпекою спеціалізованої ОС, що забезпечує безперервність керованістю корпоративною комп'ютерною мережею в умовах впливів ЗПЗ та КА; 5) розроблено метод кількісної оцінки рівня стійкості спеціалізованої ОС до витоків КІ, оброблюваної в ІС, під її керуванням, базований на розрахунку вагових коефіцієнтів кінцевої ранжованої множини критеріїв для оцінки стійкості спеціалізованих мережних ОС до витоку КІ; 6) розроблено архітектуру системи безпеки спеціалізованих ОС з підсистемами забезпечення стійкості до витоку КІ, проведено з нею експериментальні дослідження щодо встановлення покращення її характеристик при впливах ЗПЗ і КА та її подальшого впровадження для практичного застосування.

*Наукова новизна отриманих автором результатів полягає в наступному:*

1) розроблено нову модель частково-централізованої системи безпеки ОС, яка на відміну від існуючих, з метою контролю руху інформації включає механізм маркування конфіденційної інформації, який є базовим елементом в архітектурі мережної ОС та забезпечує спроможність динамічної передачі керування між її вузлами;

2) розроблено метод низькорівневого маркування конфіденційної інформації для захищених спеціалізованих ОС, який на відміну від відомих методів, працює на межі програмно-апаратної взаємодії засобів КС, що дає змогу покращити рівень стійкості комп'ютерних систем до витоку конфіденційної інформації через ОП в умовах впливів ЗПЗ та КА, контролювати рух конфіденційної інформації каналами інформаційної системи з можливістю блокування несанкціонованого поводження з інформацією;

3) розроблено метод рандомної динамічної передачі керування між центральними керівними модулями вузлів мережної ОС, який на відміну від відомих методів підтримує постійну наявність резервного керівного вузла, підтримку кожним мережним вузлом локальної бази привілеїв, та актуалізацію основної бази привілеїв і активних процесів мережі при забезпеченні ним керування системою шляхом реплікації локальних баз привілеїв, що дозволяє зменшити час передачі керування, зменшити ризик втрати актуальної бази привілеїв та активних процесів, що зменшує ризик втрати конфіденційної інформації в умовах впливів ЗПЗ та КА;

4) розроблено метод кількісної оцінки рівня стійкості ОС до витоку інформації, що на відміну від відомих методів, базується на спільній для всіх досліджуваних об'єктів множині параметрів, які є аргументами інтегрального параметра щодо стійкості ОС до витоку інформації і кожна множина локальних параметрів в межах ОС пов'язана з власною множиною вагових коефіцієнтів, що покращило чутливість до змін в системах, точність впливу кожного локального параметра на інтегральний параметр.

*Короткий аналіз основного змісту дисертації.*

У вступі автором обґрунтовано актуальність теми, визначено мету, основні завдання, предмет та об'єкт дослідження, наведено наукову новизну, практичне значення одержаних результатів.

У першому розділі проаналізовано предметну область, а саме відомі методи забезпечення безпеки спеціалізованих мережних ОС, методи протидії витоку конфіденційної інформації, що обробляється в комп'ютерних системах під керуванням ОС та здійснено постановку задачі дослідження.

У другому розділі представлено розробку методу низькорівневого маркування конфіденційної інформації в якому, контроль конфіденційності винесений на межі апаратно - програмної взаємодії комп'ютерної системи, що дозволило ефективно перекривати більшість каналів витоку конфіденційної інформації через оперативну пам'ять системи шляхом задіювання в ньому схем

процесора, що унеможливлює його обхід. Також, представлено абстрактну модель частково-централізованої системи безпеки з імплементованим в неї методом маркування. Нею задано підхід до побудови архітектури спеціалізованої мережної ОС з підвищеними параметрами стійкості до витоку конфіденційної інформації.

У третьому розділі представлено метод рандомної динамічної передачі керування між вузлами комп'ютерної мережі на основі абстрактної моделі частково-централізованої системи безпеки ОС, який не має постійного керівного центра мережею. Метод включає ряд основних кроків, в результаті виконання яких, керівний центр мережі постійно мігрує між вузлами мережі, не дозволяючи ЗПЗ вести розвідку за ним, нівелюючи тим самим комп'ютерні атаки. Також представлено розроблені алгоритми передачі керування між вузлами та розрахунок ефективності. Також, представлено метод кількісної оцінки рівня стійкості ОС до витоку інформації, базований на спільній для всіх досліджуваних ОС множині параметрів і, при цьому, кожній множині параметрів в межах досліджуваної ОС відповідає власний набір вагових коефіцієнтів, що покращило його вибірковість методу, дозволило більш точно врахувати роль і вплив кожного локального параметра на інтегральний параметр, що дозволяє застосовувати метод як до абстрактних моделей ОС, так і для оцінювання реальних 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 для варіантів ОС з імплементацією в неї метода низькорівневого маркування та без імплементації.

*Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.* Наукові висновки та рекомендації, подані в дисертації, обґрунтовані коректним та доцільним використанням математичного апарату абстрактної алгебри, теорії графів, теорії комп'ютерних мереж, успішною програмною реалізацією функцій захисних механізмів системи безпеки ОС, ефективним практичним впровадженням результатів дисертаційного дослідження в організаціях, що експлуатують комп'ютерні системи, яке продемонструвало відповідність теоретичних досліджень з реальними результатами застосування.

*Практичне значення одержаних результатів.* Результатом дисертаційної роботи є розроблена архітектура 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 КА. Це дало змогу створювати спеціалізовані ОС з

покращеними характеристиками стійкості до витоків конфіденційної інформації та її захисту, що працюють в умовах впливів ЗПЗ та КА.

Також, розроблено приклад застосування методу контролю руху конфіденційної інформації в комп'ютерній системі оснований на її маркуванні спеціальним атрибутом конфіденційності на рівні дескриптора сторінок пам'яті кожного процесу, основаного на використанні користувацьких ресурсів сучасних процесорів. Такий підхід дозволив виключити витік інформації по такому каналу, як ОП, який часто є ціллю зловмисників. Як показали проведені експериментальні дослідження, ефективність роботи системи безпеки ОС покращилась на 18,28 відсотків порівняно з стандартним підходом.

Це дає змогу створювати спеціалізовані ОС з покращеними характеристиками стійкості до витоків конфіденційної інформації та її захисту, що працюють в умовах впливів ЗПЗ та КА.

*Особистий внесок здобувача* полягає в розробленні методів та засобів організації функціонування частково-централізованої системи безпеки мережної ОС на основі рандомної передачі керування між її вузлами. Усі основні наукові та прикладні результати дисертаційної роботи отримані здобувачем самостійно. За результатами проведених досліджень основні наукові результати опубліковано у 5 наукових статтях у фахових наукових журналах України. Апробація засвідчена публікаціями 5 праць в матеріалах міжнародних та всеукраїнських конференцій, з яких 3 праці проіндексовані у наукометричній базі Scopus. Опубліковано 1 свідоцтво про реєстрацію авторського права на твір (програму).

*Апробація матеріалів дисертації.*

Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем у Хмельницькому національному університеті. Наукові результати роботи доповідалися на міжнародних та всеукраїнських науково-практичних конференціях: 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, March 28, 2024); 6th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, April 4, 2025); 1st International Workshop on Advanced Applied Information Technologies (AdvAIT-2024) (Khmelnytskyi, Ukraine - Zilina, Slovakia, December 5, 2024); XV Всеукраїнська науково-практична конференція «Актуальні проблеми комп'ютерних наук АПКН-2023» (Хмельницький, Україна, 17-18 листопада 2023); XVI Всеукраїнська науково-практична конференція «Актуальні проблеми комп'ютерних наук АПКН-2024» (Хмельницький, Україна, 15-16 листопада 2024).

*Структура та обсяг дисертації.*

Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та восьми додатків. Повний обсяг роботи містить 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 рисунків та 10 таблиць.

*Зауваження.*

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. В першому розділі досить детально проаналізовано як використання мов програмування C та C++ може стати причиною появи вразливостей в ОС, але відсутній аналіз проблем, що привносить інший програмний інструментарій, використовуваний при розробці ОС (Наприклад Visual Studio, Xcode, …).

2. Наведений опис прикладу реалізації методу низькорівневого маркування (стор. 76, 77) було б доцільно доповнити засобами адміністрування та налаштування.

3. Підрозділ 3.1.6 було б доцільно доповнити аналізом навантаження на ІС при динамічній передачі керування, оскільки зміна головного вузла приводить до інтенсивного обміну службовими даними, що може впливати на загальну ефективність системи.

4. В третьому розділі, при описі методу рандомної передачі керування між мережними вузлами не проаналізовано цілком імовірну ситуацію і, то як будуть розвиватись події у випадку, коли зловмиснику все ж вдасться атакувати вузол, що в даний момент є поточним.

5. Дисертація достатньо проілюстрована. Але деякі рисунки, наприклад рис. 2.15 (стор. 77) і ряд інших є досить інформативними і займають вагоме місце в науковій роботі, але разом з тим їх недоліком є велика кількість деталізацій, які зменшують їх читабельність та сприйняття. Окрім цього, в роботі присутні деякі орфографічні та стилістичні помилки, а саме на сторінках 72, 159.

Втім, зазначені зауваження суттєво не впливають на загальний, доволі високий рівень проведеного дослідження.

*Загальний висновок.*

Вважаю, що дисертаційна робота Стецюка Юрія Васильовича за темою «Методи та засоби забезпечення безпеки спеціалізованих мережних операційних систем» містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі 12 Інформаційні технології, які в сукупності забезпечують розв'язання актуальної науково-прикладної задачі розроблення методів для покращення ефективності роботи систем безпеки спеціалізованих мережних ОС на основі частково-централізованого підходу з рандомною передачею керування між її вузлами.

Дисертаційна робота «Методи та засоби забезпечення безпеки спеціалізованих мережних операційних систем», яка 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 (зі змінами, внесеними згідно з Постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024), а її автор, Стецюк Юрій Васильович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Рецензент:
доктор технічних наук, доцент,
професор кафедри комп'ютерної
інженерії та інформаційних систем
Хмельницького національного університету _____ Антоніна КАШТАЛЬЯН

«Підпис Антоніни КАШТАЛЬЯН засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету _____ Олег СИНЮК