

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

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

Розвиток та масове розповсюдження корпоративних інформаційних систем охоплює практично всі сфери світової економіки. Вони забезпечують автоматизацію управління, обробку великих обсягів даних, підтримку бізнес-процесів і прийняття управлінських рішень. Зростання залежності економічних структур від корпоративних ІС підвищує вимоги до їх надійності, безперервності функціонування та безпеки оброблюваної інформації.

Тому, мережні операційні системи (ОС) займають ключове місце в забезпеченні обробки інформації в корпоративних мережах. Саме ОС реалізує механізми керування апаратними ресурсами, ізоляції процесів, контролю доступу та взаємодії мережних компонентів. Від архітектури та реалізації ОС безпосередньо залежить рівень захищеності корпоративної інформаційної системи в цілому.

Разом з тим їх робота знаходиться під постійним тиском зловмисного програмного забезпечення (ЗПЗ), яке постійно удосконалюється та активно експлуатує вразливості операційних систем і процесорної архітектури з метою заволодіння конфіденційною інформацією. Атаки спрямовані як на програмні помилки, так і на особливості апаратної реалізації, що загрожує

створенням додаткових каналів витоку даних та, одночасно, ускладнює їх виявлення і блокування. Наукова робота Стецюка Ю.В. спрямована саме на розробку методів та засобів протидії витоку інформації в умовах впливів ЗПЗ та КА.

Дослідження, результати яких наведено в дисертації, 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.

Тому, вирішення науково-прикладної задачі протидії витоку інформації та використанню вразливостей комп'ютерних систем ЗПЗ, є актуальним у сучасних умовах.

2. Формулювання наукової задачі та мети й задач дослідження

Здобувач правильно визначив об'єкт і предмет дослідження. Так, об'єктом дослідження є процес забезпечення стійкості мережних ОС до витоку конфіденційної інформації, що обробляється в інформаційних системах під її 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.

Поставлену мету досягнуто в результаті розв'язання таких задач:

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 використанні 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 керування 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 витоків КІ;

6) розроблено архітектуру системи безпеки спеціалізованих ОС з підсистемами забезпечення стійкості до витоків КІ, проведено з нею експериментальні дослідження щодо встановлення покращення її характеристик при впливах ЗПЗ і КА та її подальшого впровадження для практичного застосування.

3. 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 витоків 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.

4. Аналіз основного змісту дисертації

У вступі обґрунтовано актуальність задачі підвищення ефективності виявлення інфікованих програм, що використовують методи уникнення виявлення. Визначено перспективність застосування архітектури частково-централізованої системи безпеки мережної ОС з рандомною передачею керування між її вузлами. Представлено зв'язок теми з науковими дослідженнями, результати роботи та приклади впровадження.

У першому розділі здійснено огляд предметної області дослідження, розглянуто проблеми мережних ОС з децентралізованою системою безпеки, зокрема особливості розподілу механізмів контролю та їх вплив на загальний рівень захищеності. Проаналізовано методи захисту основних елементів ОС, їх відомі вразливості та вразливості процесорів і можливі причини їх виникнення. Окрему увагу приділено захисним механізмам комерційних і некомерційних мережевих ОС, що дозволило виявити їх переваги та обмеження, а також сформулювати невирішені проблеми.

У другому розділі представлено абстрактну модель частково-централізованої системи безпеки з імплементованим в неї методом маркування, а також представлено розробку методу низькорівневого маркування конфіденційної інформації в якому, контроль конфіденційності винесений на межі апаратно-програмної взаємодії КС, що дає можливість ефективно перекривати більшість каналів витоку конфіденційної інформації через ОП системи і робить обхід контролю неможливим.

У третьому розділі запропоновано метод рандомної динамічної передачі керування між вузлами комп'ютерної мережі на основі абстрактної моделі частково-централізованої системи безпеки ОС, керівний центр якої постійно мігрує між вузлами мережі, не дозволяючи ЗПЗ вести розвідку мережі, нівелюючи тим самим комп'ютерні атаки.

Представлено метод кількісної оцінки рівня стійкості ОС до витоку інформації, що базується на спільній для всіх досліджуваних ОС множині параметрів, при цьому, кожній множині параметрів в межах досліджуваної ОС відповідає власний набір вагових коефіцієнтів, що дозволило більш точно врахувати роль і вплив кожного локального параметра на інтегральний параметр.

У четвертому розділі наведено методику визначення ефективності системи безпеки ОС з імплементованим в неї методом низькорівневого маркування конфіденційної інформації. Представлено середовище для постановки експериментів та описання проведених експериментів. За результатами експериментів виконано необхідні розрахунки ефективності та продуктивності для двох варіантів реалізації ОС.

У висновках подано здобуті теоретичні та практичні результати досліджень.

Додатки містять наукові статті, що відображають результати роботи, акти про впровадження, а також лістинг коду розробленого програмного забезпечення.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.

Наукові положення, висновки і рекомендації дисертації обґрунтовані коректним та доцільним використанням математичного апарату, алгоритмами забезпечення стійкості спеціалізованих мережних ОС до витоку КІ, успішною програмною реалізацією функцій захисних механізмів системи безпеки ОС, практичним впровадженням результатів дисертаційного дослідження в організаціях, що експлуатують КС, яке продемонструвало відповідність теоретичних досліджень з реальними результатами застосування, а також їх апробацією на міжнародних та всеукраїнських наукових конференціях.

6. Практичне значення отриманих результатів

За результатами виконаних досліджень здобувачем 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 КА. Це дало змогу створювати спеціалізовані ОС з

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

Застосування частково-централізованого підходу на основі методу рандомної динамічної передачі керування між мережними вузлами дозволило підвищити ефективність захисних механізмів ОС в частині її стійкості до витоку інформації на 10 % порівняно з винятково централізованою системою.

Експериментальні дослідження підтвердили коректність функціонування частково-централізованої системи безпеки мережної ОС з імплементованим в неї методом низькорівневого маркування конфіденційної інформації.

Теоретичні та практичні результати дослідження впроваджені при розробці компонентів системи безпеки ОС FreeBSD 13.1 в ТОВ Ультра ІТ, ТОВ ДЕВІКС ДІДЖИТАЛ, ТОВ Nolt technologies, 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. Особистий внесок здобувача полягає в розробленні архітектури частково-централізованої системи безпеки мережної ОС на основі динамічної зміни керівного центра для протидії зловмисному програмному забезпеченню та комп'ютерним атакам. 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 три праці індексовані у наукометричній базі Scopus. Опубліковано 1 свідоцтво про реєстрацію авторського права на твір (програму).

8. Структура та обсяг дисертації.

Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та чотирьох 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 рисунок та 10 таблиць.

9. Зауваження

1. В першому розділі, в процесі аналізу розглянуто велику кількість аспектів, що стосуються методів забезпечення безпеки ОС, протидії витоку інформації в них. Доцільно, було б, звести їх в таблицю з короткими відомостями про вирішені та невирішені проблеми, щоб подати стислу, інтегровану картину стану предметної області.

2. При опису прикладу реалізації методу низькорівневого маркування конфіденційної інформації здобувач скористався 32-х розрядною апаратною платформою. Було б доцільніше демонструвати реалізацію методу на 64-х розрядній платформі.

3. На рис. 2.13 (стор. 75) наведено алгоритм роботи модуля безпеки ОС, але з приведеного опису не дуже зрозуміло місце його реалізації в операційній системі.

4. В даному дослідженні здобувачем пропонується ряд методів, що передбачають протидію витоку конфіденційної інформації. В той же час у відношенні організації обробки конфіденційної інформації в КС діє ряд законів та законодавчих актів, зокрема Закон України «Про захист інформації в інформаційно-комунікаційних системах» якими введені в дію «Профілі безпеки». В роботі відсутня інформація, що до того, чи запропоновані методи враховують необхідність використання та не є суперечливими по відношенню до означених «Профілів безпеки».

5. Доволі великий текст дисертації можна було би скоротити за рахунок більш широкого використання загальноприйнятих скорочень. Та автор не скрізь, скористався такою можливістю, наприклад стосовно терміну «частково-централізована система безпеки – ЧЦСБ».

6. В основній частині роботи всього десять таблиць, але виконані вони в різних форматах (наприклад: стор. 127 таблиця 3.1 та стор. 132 таблиця 3.2). Окрім цього, зустрічаються деякі граматичні та стилістичні помилки, зокрема на сторінках 83 та 145.

Однак зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

10. Загальний висновок.

Отже, дисертаційна робота Стецюка Юрія Васильовича за темою «Методи та засоби забезпечення безпеки спеціалізованих мережних операційних систем» є завершеною науковою кваліфікаційною працею, яка містить новий та актуальний науково-прикладний внесок. Усі результати, які виносяться на захист, є достовірними та отримані автором особисто.

Тому, з огляду на вище вказане, вважаю, що 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:

кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки

Хмельницького національного університету



Юрій КЛЬОЦ

«Підпис Юрія КЛЬОЦА засвідчую»:

Проректор з наукової роботи

Хмельницького національного університету



Олег СИНЮК