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

ВІДГУК

офіційного опонента на дисертаційну роботу
Стецюка Юрія Васильовича
на тему: «Методи та засоби забезпечення безпеки спеціалізованих мережних операційних систем», представлену на здобуття наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дисертації. Забезпечення неперервності доступу до функцій та ресурсів інформаційних систем в корпоративних мережах, робота яких здійснюється в досить агресивних, постійно мінливих умовах, є однією із нагальних наукових задач сьогодення. Науковцями всього світу та України зокрема, ведеться постійна робота по розробці нових методів забезпечення стійкості ОС до витоків конфіденційної інформації, протидії деструктивним впливам зловмисного програмного забезпечення (ЗПЗ) та комп'ютерним атакам (КА). Кінцевою метою цієї багатогранної діяльності є створення бар'єру проти втрати даних, несанкціонованого доступу до них, які на сьогодні є найцінніщим ресурсом.

Але незважаючи на успіхи сучасної науки, велику кількість розроблених методів та засобів, застосування різноманітних комплексних систем захисту

інформації, існуючі на сьогодні ОС не в змозі гарантувати повну стійкість до витоку інформації через існування в них вразливостей з однієї сторони, та постійну загрозу зі сторони ЗПЗ, що продовжує тільки збільшуватись, з другої сторони.

Тому пошук шляхів вирішення цієї задачі не припиняється. Автором дисертації пропонується свій підхід у вирішенні задачі протидії витоку інформації та, загалом, несанкціонованому доступу до конфіденційної інформації через впровадження механізмів додаткового захисту ОС, що базовані на частково-централізованих системах безпеки спеціалізованих мережних ОС при їх роботі в умовах деструктивних впливів ЗПЗ та КА.

Усе вищезазначене зумовлює актуальність теми дисертаційної роботи Стецюка Ю.В., яка присвячена розв’язанню важливої науково-прикладної задачі, пов’язаної із забезпеченням стійкості ОС до витоку конфіденційної інформації та загалом захисту інформації, що обробляється в ІС під їх керуванням.

Зв’язок роботи з науковими програмами, планами темами. Дисертаційна робота виконана на кафедрі комп’ютерної інженерії та інформаційних систем Хмельницького національного університету. Її зміст відповідає тематиці науково-дослідних робіт за держбюджетної теми Хмельницького національного університету №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.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни. Наукова новизна результатів дисертаційного дослідження полягає в наступному:

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;

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;

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;

розроблено новий 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.

Наукові положення, висновки і рекомендації дисертаційної роботи Стецюка Ю.В. достатньо обґрунтовані коректним використанням математичного апарату, підкріплені успішною реалізацією, ефективним практичним впровадженням результатів дисертаційних досліджень, яке продемонструвало відповідність теоретичних досліджень із одержаними результатами. При розв'язанні поставленої науково-прикладної задачі використовувались основні положення абстрактної алгебри, теорія графів, теорія комп'ютерних мереж,

теоретичні основи інформаційних технологій, методи захисту інформації в комп'ютерних системах, методи проєктування інформаційних систем.

Обґрунтованість наукових положень та висновків, сформульованих у дисертаційній роботі, є достатньою і базується на детальному аналізі джерел за даною проблематикою, чіткій постановці задач дослідження, використання новітніх методів дослідження, правильним застосуванням математичного апарату при теоретичному розгляді наукових положень дисертації, а також проявляється у якісному та аргументованому формулюванні висновків.

Достовірність та обґрунтованість запропонованих методів і засобів підтверджується результатами експериментальних досліджень та коректним застосуванням методів, які були використані під час виконання роботи.

Наукові положення, висновки та рекомендації, сформульовані в дисертації, логічно випливають із результатів, одержаних за допомогою чітких викладок. Тому, можна вважати, що висновки та практичні рішення, одержані у роботі достатньо обґрунтовані і коректні.

Отже, в дисертаційній роботі поставлене наукове завдання 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 Стецюка Ю. В. повністю відповідає Стандарту вищої освіти зі спеціальності 123 та освітньо-науковій програмі ХНУ «Комп'ютерна інженерія» за спеціальністю 123 Комп'ютерна інженерія. Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям комп'ютерної інженерії.

Розглянувши результати перевірки дисертаційної роботи, можна зробити висновок, що дисертаційна робота Стецюка Юрія Васильовича є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень.

Використані результати і тексти інших авторів мають належні посилання на відповідне джерело.

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.

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 оперативна пам'ять, який часто є ціллю зловмисників. 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.

Результати дисертаційної роботи впроваджені в ТОВ Ультра ІТ, ТОВ ДЕВІКС ДІДЖИТАЛ, ТОВ Nolt technologies та в ІТ-системах фінансово-господарських служб Хмельницького національного університету, а також, в освітньому процесі Хмельницького національного університету на кафедрі комп'ютерної інженерії та інформаційних систем при викладанні дисципліни «Безпека та захист комп'ютерних систем».

Мова та стиль викладення результатів. Дисертаційна робота написана українською мовою. Дисертація написана логічно, доступно на високому технічному рівні з використанням сучасної термінології. Матеріали дисертаційної роботи викладено послідовно, доступно для розуміння і сприйняття. Стиль мовлення задовольняє вимоги до текстів науково-технічного змісту. Текст дисертації достатньо широко проілюстровано таблицями та рисунками. Здобувач використовує загальноприйняту термінологію.

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.

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. Основні результати дисертації опубліковані в 11 наукових працях, серед яких 5 статей у фахових наукових журналах України, включених на дату опублікування до переліку наукових фахових видань України категорії Б; 5 праць в матеріалах міжнародних та всеукраїнських конференцій (3 з яких проіндексовано у наукометричній базі

У підсумку, опубліковані праці віддзеркалюють повноту викладу результатів дисертаційної роботи. Науковий рівень публікацій – високий. У всіх публікація здобувачем дотримано принципів академічної доброчесності.

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

Недоліки та зауваження до дисертаційної роботи:

В першому розділі, при аналізі предметної області дисертаційного дослідження відмічено, що «спостерігається еволюція зловмисного програмного забезпечення в напрямку побудови різноманітних прихованих каналів проникнення …», але висновків про значимість створюваної в такий спосіб загрози комп’ютерним системам не приводиться.

В таблиці 2.1 стор. 67 наведена модель порушника, в якій властивості зовнішнього та внутрішнього порушника визначені однаково. Але на практиці, як правило, це два різні порушники, які описуються різними наборами властивих їм можливостей.

. На рис. 2-15 (стор. 77) приведено приклад можливої реалізації методу низькорівневого маркування конфіденційної інформації. Він важливий з точки зору представлення практичних результатів дослідження. Но дисертант не зумів виконати його так, щоб всі його елементи сприймались однаково чітко.

В третьому розділі приводиться розроблений метод рандомної передачі керування між мережними вузлами. Але в приведеному тексті дисертаційного дослідження не приводиться ніяких даних, при якій кількості мережевих вузлів цей метод збереже роботоздатність.

Деякі деталі окремих рисунків (у розділі 2 рис. 2.12 стр. 74, розділ 3 рис. 3.2 стр. 98, рис. 3.3. стр. 100 …) складні для читання, через надто малий шрифт. Можливо варто було використати інші формати рисунків, щоб покращити сприйняття та розуміння інформації представленої на них.

У дисертаційній роботі часто використовуються терміни «імовірність» та «ймовірність», «безпекові ресурси» та «ресурси безпеки». Здобувачу варто було б узгодити термінологію з цього приводу. Окрім цього у тексті дисертації зустрічаються деякі граматичні орфографічні помилки, зокрема на сторінках 72, 73, 123, 159 стосовно флексій слова «файл» в українській мові.

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

Висновок про дисертаційну роботу. Вважаю, що дисертаційна робота здобувача наукового ступеня доктора філософії Стецюка Юрія Васильовича на тему «Методи та засоби забезпечення безпеки спеціалізованих мережних операційних систем» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв’язує наукове завдання. 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», 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).

Здобувач Стецюк Юрій Васильович заслуговує на присудження наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент
Кандидат технічних наук, доцент
декан факультету комп'ютерних
інформаційних технологій
Західноукраїнського національного університету Ігор ЯКИМЕНКО