67-72-102/2
10.10.2019

ВІДГУК

офіційного опонента, доктора технічних наук, професора,
професора кафедри математичних методів системного аналізу
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського",
Мухіна Вадима Євгенійовича
про дисертаційну роботу Савенка Олега Станіславовича
«Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах»,
подану на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

1. Актуальність теми дисертації.

Зловмисне програмне забезпечення (ЗПЗ) викликає суттєві проблеми для користувачів комп'ютерних систем, що, зокрема, призводить до фінансових збитків підприємства та організацій. Сучасні антивірусні засоби не забезпечують високого рівня виявлення зловмисного програмного забезпечення. Тенденції останніх років вказують, що розробники ЗПЗ застосовують сучасні технології програмування та поширення зловмисного коду і урізноманітнюють копії ЗПЗ. Створення сучасного зловмисного програмного забезпечення базується на використанні технологій розробки складних багатофункційних систем, які побудовані із заданим цілеспрямованим функціоналом та багатоваріантністю. Першочергово розробники такого ЗПЗ мають на меті тривале його використання, уникнення виявлення, цілеспрямований пошук об'єктів та оперативне використання. Від такого ЗПЗ найбільше потерпають окремі приватні користувачі, а особливо комп'ютерні системи підприємств та організацій. Тому, проблема покращення ефективності виявлення ЗПЗ залишається актуальною.

Сучасне ЗПЗ зорієнтовано зловмисниками переважно на використання в комп'ютерних мережах, що дозволяє пришвидшити його поширення. При побудові такого типу ЗПЗ переважно застосовують методи теорії розподілених систем. Виявлення такого розподіленого ЗПЗ є тривалою і важковирішуваною задачею, якщо користуватись тільки хостовими антивірусними засобами.

В роботі пропонується використання розподілених систем виявлення ЗПЗ у локальних комп'ютерних мережах як перспективного напрямку досліджень для вирішення проблеми покращення ефективності виявлення. Для урізноманітнення виявлення ЗПЗ антивірусних засобів та уникнення впливу адміністратора мережі в роботі пропонується створення розподілених систем на основі децентралізації та самоорганізації.

Викладене вище аргументує актуальність дисертаційної роботи Савенка Олега Станіславовича, яка присвячена вирішенню науково-технічної проблеми покращення ефективності виявлення зловмисного програмного забезпечення шляхом розроблення теорії і практики створення розподілених систем у локальних комп'ютерних мережах на основі принципів децентралізації та самоорганізації.

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

Тематика дисертаційного дослідження відповідає пріоритетним напрямкам розвитку науки і техніки на період до 2020 року (пунктами 2-6 статті 3 Закону України «Про пріоритетні напрями розвитку науки і техніки») визначеними Верховною Радою України, а також Наказом МОН України №1446 від 28.12.2018 р.

Представлена робота відповідає науковому напряму кафедри комп'ютерної інженерії та системного програмування Хмельницького національного університету і пов'язана з планами наукових досліджень, які виконувалися в рамках держбюджетної науково-дослідної роботи Хмельницького національного університету № 1Б-2019 «Агентно-орієнтована система підвищення безпеки та якості програмного забезпечення комп'ютерних систем» (номер державної реєстрації 0119U100662), № 1Б-2001 «Методологія тестового комбінованого діагностування

мікропроцесорних пристроїв та систем (МПП та С) на базі компонентів штучного інтелекту» (номер державної реєстрації 0101U005058), № 4Б-2012 «Розвиток теоретичних основ та розробка методів статико-динамічного спектрального оцінювання сигналів в радіолокації» (номер державної реєстрації 0112U002247), № 1Б-2018 «Розроблення високоефективних методів відбору енергії від фотоелектричних модулів» (номер державної реєстрації 0116U001548).

2. Ступінь обґрунтованості наукових положень, висновків та рекомендацій.

Наукові положення, висновки і рекомендації дисертаційної роботи Савенка Олега Станіславовича достатньо обґрунтовані коректним використанням математичного апарату, підкріплені успішною реалізацією розподіленої багаторівневої системи виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах, яка забезпечує усунення людини з процесів опрацювання інформації щодо виявлення ЗПЗ та призначена для здійснення тривалого спостереження за подіями в КС, ефективним практичним впровадженням результатів дисертаційних досліджень, яке продемонструвало збіг теоретичних досліджень з реальними результатами.

Наукові положення, висновки та рекомендації, сформульовані в дисертації, логічно випливають із результатів, отриманих за допомогою чітких викладок з коректним використанням принципів загальної теорії систем, системного аналізу (ієрархічності, декомпозиції та ін.), методів аналізу та моделювання процесів, теоретико-множинних підходів, алгебраїчних систем, теорії множин, евристичних оцінок, загальних принципів створення розподілених систем та застосування принципів децентралізації і самоорганізації.

Наукові положення, висновки і рекомендації, які сформульовані в дисертаційній роботі, стосуються розроблення теорії та практики створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах.

Відзначаю, що наукові положення та рекомендації висновків до всіх розділів дисертаційної роботи (ст. 87-88, ст. 150-152, ст. 184-185, ст. 255-256, ст. 291-293, ст. 325-326) та загальних висновків до дисертаційної роботи (ст. 327-330) сформульовано науково обґрунтовано і логічно за результатами аналізу, узагальнення відомих та отриманих результатів, теоретичних досліджень, а також експериментальної перевірки розробленої розподіленої багаторівневої системи виявлення зловмисного програмного забезпечення.

3. Достовірність наукових положень, висновків та рекомендацій.

Достовірність отриманих результатів забезпечується коректною постановкою проблеми, мети та задач дисертаційного дослідження, які розв'язуються послідовно та аргументовано. Достовірність наукових положень, висновків та рекомендацій підтверджується відповідністю методології дослідження поставленій проблемі, повнотою розгляду на теоретичному та експериментальному рівнях об'єкта дослідження, застосуванням комплексу методів, адекватних предмету дослідження.

Достовірність і обґрунтованість результатів дисертаційного дослідження ґрунтуються на:

1) використанні основних положень теорії множин, абстрактної алгебри для представлення об'єктів дослідження;

2) застосуванні загальних принципів теорії розподілених систем для розроблення моделей архітектури розподіленої системи та її компонентів;

3) методи класифікації для здійснення віднесення програмних об'єктів до класів зловмисного програмного забезпечення;

4) теорії комп'ютерних мереж для представлення функціонування розподіленої системи, зокрема її програмних та апаратно-програмних компонентів.

Достовірність результатів базується на обґрунтованості припущень, результатах експериментальних досліджень, правильному аналізі отриманих результатів, а також на успішній їх апробації на 45 науково-технічних конференціях та успішному впровадженні отриманих рішень в Державному

підприємстві «Новатор», ТОВ «ITT – telecommunication company», ТОВ «ЮКС++», компанії CYPRESS SEMICONDUCTOR, а також у освітньому процесі.

4. Наукова новизна одержаних результатів.

Наукова новизна досліджень полягає у вирішенні актуальної науково-технічної проблеми – здійснено розвиток теорії і практики створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах для покращення ефективності його виявлення. Вирішення даної проблеми має важливе значення в усіх галузях, де активно застосовуються локальні комп'ютерні мережі.

В дисертаційній роботі Савенка О.С. отримані наступні важливі наукові результати:

1) удосконалено модель архітектури розподіленої системи виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах на основі комплексного врахування вимог розподіленості, децентралізованості, багаторівневості та самоорганізованості, що дозволяє створювати на її основі розподілені системи та їх компоненти, які функціонуватимуть автономно і самостійно прийматимуть рішення про наявність зловмисного програмного забезпечення та нарощення своїх функціональних можливостей;

2) вперше розроблено модель архітектури типових компонентів розподіленої багаторівневої системи виявлення зловмисного програмного забезпечення на основі структур Кріпке з представленням компонентів через стани, в яких вони можуть перебувати під час функціонування, що дає змогу враховувати перебування їх в різних станах і є основою для визначення стану безпеки всієї розподіленої системи та її компонентів;

3) вперше розроблено метод взаємодії компонентів розподіленої багаторівневої системи виявлення зловмисного програмного забезпечення на основі підтримки її цілісності та визначення порядку передачі знань між її компонентами і використання встановлених аналітичних залежностей між

рівнями безпеки програмних модулів та рівнем безпеки всієї розподіленої багаторівневої системи, що дозволяє системі автономно змінювати свою архітектуру та функції без втручання користувача, а також визначати стратегію своєї подальшої роботи;

4) удосконалено моделі зловмисного програмного забезпечення шляхом їх подання алгебрами поведінки, що дозволило створити базис поведінкових сигнатур, і, на відміну від відомих представлень, врахувати особливості функціонування зловмисного програмного забезпечення в локальних комп'ютерних мережах та здійснити його класифікацію за типами поведінки;

5) вперше розроблено метод виявлення бот-мереж у локальних комп'ютерних мережах, який базується на здійсненні активного моніторингу системних подій та узгодженій взаємодії компонентів розподіленої системи при прийнятті рішення, і, на відміну від відомих методів, дає можливість створення на його основі засобів, здатних інтегруватись в розподілену систему та класифікувати бот-мережі за їх поведінковими сигнатурами, що формуються закладеними в їх компоненти функціями;

6) вперше розроблено метод виявлення файлового зловмисного програмного забезпечення в локальних комп'ютерних мережах, який полягає в поєднанні роботи програмних агентів, що здійснюють виявлення зловмисного програмного забезпечення в окремих комп'ютерних системах, відповідно до імплементованих в них методів: динамічного формування поведінкової сигнатури шляхом відстеження викликів прикладного програмного інтерфейсу, знаходження поліморфного та метаморфного програмного коду, сканування виконуваних програм шляхом створення для них автономних процесів та відповідних програмних агентів у розподіленій системі, що, на відміну від аналогів, дозволяє покращити аналіз і підвищити достовірність виявлення зловмисного програмного забезпечення;

7) вперше розроблено метод виявлення файлового зловмисного програмного забезпечення на основі динамічного формування поведінкової сигнатури шляхом відстеження викликів прикладного програмного

інтерфейсу, в якому, на відміну від відомих методів, поведінкова сигнатура формується на основі критичних викликів прикладного програмного інтерфейсу за групами зловмисної активності та відображає частоту їх входження і характер взаємодії критичних функцій, що дає змогу виявляти нові версії відомого зловмисного програмного забезпечення не тільки за наявністю критичних викликів, але й за їх взаємодією між собою;

8) вперше розроблено метод виявлення поліморфних та метаморфних вірусів з використанням функцій заплутування програмного коду, відмінністю якого є поетапний аналіз і порівняння функціональних блоків програмного об'єкта та його змінених версій, отриманих, в тому числі, від різних компонентів розподіленої системи шляхом їх взаємодії між собою.

Наукові результати, отримані Савенком О.С. в дисертації на здобуття наукового ступеня кандидата технічних наук, не виносяться у представлену до захисту докторську дисертацію.

5. Практичне значення результатів та рекомендації щодо їх подальшого використання.

Практичне значення дисертаційної роботи Савенка О.С. полягає у розробленій архітектурі і компонентах самоорганізованої розподіленої багаторівневої системи (РБС) виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах. Розроблена архітектура стала основою для здійснення її програмної реалізації. В якості складових компонентів системи, також, розроблені апаратно-програмні засоби захисту інформації, використання яких задається вимогами безпеки. Реалізація РБС підтверджує теоретичні результати в частині можливості створення розподілених систем виявлення ЗПЗ та використовується для проведення експериментальних досліджень при порівнянні з існуючими системами.

Теоретичні та практичні результати роботи впроваджено в Державному підприємстві «Новатор», ТОВ «ІТТ – telecommunication company», ТОВ «ЮКС++», компанії CYPRESS SEMICONDUCTOR та освітньому процесі Хмельницького національного університету при викладанні дисциплін

«Безпека та захист комп'ютерних систем», «Технічна діагностика і надійність комп'ютерних пристроїв та систем», «Паралельні та розподілені обчислення» та «Системне програмне забезпечення».

Результати експериментальних досліджень підтверджують ефективність розроблених програмних засобів, а також правильність наукових положень теорії розподілених систем, оскільки впровадження розподіленої багаторівневої системи виявлення зловмисного програмного забезпечення дозволяє підвищити достовірність виявлення на 5–12 % порівняно з відомими аналогами та знизити рівень помилок першого роду до 5 %.

Дослідження проводились з врахуванням їх наступної практичної реалізації. Результати досліджень можуть бути рекомендовані до впровадження в діяльності софтверних компаній для покращення ефективності виявлення ЗПЗ.

6. Оцінка змісту дисертаційної роботи.

Дисертаційна робота складається з анотації, вступу, шести розділів, висновків, списку використаних джерел із 399 найменувань на 49 сторінках та шести додатків на 46 сторінках. Загальний обсяг дисертації становить 425 сторінок, з яких 304 сторінки основного тексту, які включають 54 рисунки та 46 таблиць.

У **вступі** проведено обґрунтування актуальності теми дисертаційної роботи, окреслено наукову проблему, визначено об'єкт, предмет, мету і завдання дослідження, виділено наукові задачі, визначено наукову новизну та практичну цінність одержаних результатів та вказано на зв'язок роботи з науковими програмами і науково-дослідними роботами за місцем виконання роботи та надано інформацію щодо кількості публікацій та апробації результатів дисертації.

У **першому розділі** проведено аналіз і дослідження стану розвитку зловмисного програмного забезпечення, мережних систем виявлення зловмисного програмного забезпечення та результатів достовірності їх роботи. В результаті дослідження функціонування ЗПЗ в КС локальних комп'ютерних

мереж (ЛКМ) та антивірусних засобів їх виявлення автором отримані такі висновки: розробники ЗПЗ володіють значними технічними засобами для його створення; ЗПЗ може використовувати різносторонні засоби для поширення та стійкості, що підвищує його життєздатність і можливості для поширення та ускладнює виявлення антивірусними засобами; певні типи ЗПЗ мають модульну структуру, що суттєво знижує ефективність виявлення існуючими антивірусними засобами; застосування стандартних методів виявлення не гарантує належного рівня достовірності виявлення ЗПЗ в КС; використання модулів шифрування у ЗПЗ ускладнює виявлення через створення різних копій одного і того самого ЗПЗ; застосування сучасних евристичних аналізаторів вимагає значних ресурсів КС; використання методів на основі контрольних сум не завжди дає однозначну відповідь щодо того, чи відбулося інфікування КС; використання мережних систем виявлення для покращення ефективності виявлення ЗПЗ знижує оперативність в прийнятті рішення через залучення адміністратора мережі до прийняття рішення; відомі мережні системи виявлення переважно побудовані з використанням централізованої архітектури, що активізує зловмисників до виявлення центру для зупинки системи; відомі мережні системи виявлення і антивірусні засоби переважно є хост-орієнтованими і не враховують можливостей ЗПЗ виконуватись в декількох КС одночасно. При проведенні дослідження автор виявив відсутність антивірусних засобів та систем виявлення ЗПЗ, які забезпечують його повне виявлення та зробив висновок щодо необхідності розроблення теорії і практики створення розподілених систем виявлення ЗПЗ як напряму подальших досліджень. При цьому для уникнення дослідження розробленої РБС виявлення ЗПЗ зі сторони ЗПЗ автор запропонував включити вимоги до РБС такі, як самоорганізованість та децентралізованість.

Обґрунтування актуальності вирішуваної наукової проблеми та постановку наукових задач для вирішення проблеми Савенко О.С. виконав в повному обсязі.

У **другому розділі** автором розроблено удосконалену модель архітектури розподіленої багаторівневої системи виявлення ЗПЗ в ЛКМ.

Також, розроблені модель архітектури типових компонентів РБС на основі структур Кріпке та метод взаємодії компонентів РБС. Архітектуру РБС було спроектовано з врахування вимог розподіленості, децентралізованості, багаторівневості та самоорганізованості. РБС побудовано із сукупності однакових компонентів, які розміщуються у вузлах локальної комп'ютерної мережі. Кожна компонента представлена програмним модулем системи, який має однакову архітектуру і в якому виділено вісім станів залежно від функційного призначення та згрупованих у них завдань. Встановлення порядку здійснення комунікації між компонентами РБС та обміну знаннями між ними автором розроблено метод взаємодії компонентів РБС виявлення ЗПЗ.

У **третьому розділі** в дисертаційній роботі удосконалено моделі зловмисного програмного забезпечення. Для цього їх подано алгебрами поведінки з метою створення базису поведінкових сигнатур, в яких враховано особливості функціонування ЗПЗ у локальних комп'ютерних мережах. В якості об'єкту для дослідження було розглянуто множину ЗПЗ, яке за певних обставин та протягом певного часу експлуатації ЛКМ, проникло в комп'ютерні системи, подолало певні системи захисту і функціонує там, тобто те ЗПЗ, яке на момент виявлення вже перебуває в КС, і в ЛКМ. На основі удосконалених моделей типів зловмисного програмного забезпечення було створено базис поведінкових сигнатур, які враховують особливості, що проявлятимуться при виконанні функцій, їх функціонування в ЛКМ та використовуються для здійснення класифікації за типами поведінки.

У **четвертому розділі** представлено розроблений автором метод виявлення бот-мереж у локальних комп'ютерних мережах. Він базується на здійсненні активного моніторингу системних подій та узгодженій взаємодії компонентів розподіленої системи при прийнятті рішення. В якості об'єктів дослідження мережного ЗПЗ розглянуто керовані зловмисником бот-мережі. Виділено характерну особливість, яка відрізняє цю підмножину ЗПЗ від інших. Для виявлення такого ЗПЗ пропонується пошук та виокремлення характерних для цього типу ознак, їх подальша формалізація та використання. Оскільки

ЗПЗ такого типу є складними програмними комплексами, які функціонують у глобальних комп'ютерних мережах, то для їх виявлення було розроблено метод, застосування та реалізація якого передбачена саме в розподілених системах.

У **п'ятому розділі** розроблено методи виявлення файлового ЗПЗ в ЛКМ, зокрема, метод виявлення файлового зловмисного програмного забезпечення в локальних комп'ютерних мережах, який полягає в поєднанні роботи програмних агентів, що здійснюють виявлення зловмисного програмного забезпечення в окремих комп'ютерних системах, відповідно до імплементованих в них методів: динамічного формування поведінкової сигнатури шляхом відстеження викликів прикладного програмного інтерфейсу; знаходження поліморфного та метаморфного програмного коду; сканування виконуваних програм шляхом створення для них автономних процесів та відповідних програмних агентів у розподіленій системі. Така комбінація методів дозволила покращити аналіз і підвищити достовірність виявлення зловмисного програмного забезпечення. Метод виявлення файлового зловмисного програмного забезпечення базується на основі динамічного формування поведінкової сигнатури шляхом відстеження API-викликів та включає формування сигнатури вірусної програми на основі трасування API-викликів, що дозволяє здійснити виявлення вірусної програми, яка представлена розробленою поведінковою сигнатурою з бази поведінкових сигнатур. Поведінкова сигнатура включає критичні API-виклики за групами зловмисної активності, відображає частоту їх входження, характер взаємодії критичних API-функцій вірусної програми та описує взаємозв'язок між критичними API-функціями. Це надає можливість розмежувати вірусні програми від корисних застосунків не тільки за наявністю критичних API-викликів, але й за їх взаємодією між собою. Для здійснення виявлення використовується класифікація. Метод виявлення поліморфних та метаморфних вірусів на основі аналізу функцій обфускації розроблено для файлового ЗПЗ, яке використовує техніки заплутування свого коду. Особливістю методу є аналіз програмного об'єкта та його модифікованих

версій, отриманих від різних програмних модулів РБС, і подальший аналіз на основі пошуку еквівалентних функціональних блоків. Це дозволило здійснити більш детальний аналіз коду програмного об'єкта на наявність поліморфних та метаморфних вірусів.

У **шостому розділі** представлена програмна реалізація РБС, результати її застосування при виявленні різних типів ЗПЗ у ЛКМ, а також розроблена методика оцінки ефективності роботи РБС. У розробленому варіанті програмного забезпечення РБС відображено вимоги децентралізованості, самоорганонізованості, багаторівневості та розподіленості. Розроблене програмне забезпечення РБС Distributed Multilevel System дозволяє здійснювати його доповнення новими методами, реалізує зв'язуючу частину розподіленої системи і було використано для проведення експериментальних досліджень.

Проведені експерименти з використанням розробленої РБС виявлення бот-мереж підтвердили можливість застосування методу виявлення, роботи класифікатора в структурі розподіленої системи та визначення залежності відсотка виявлених вузлів бот-мережі від їх представлення векторами та різними класифікаторами. Експерименти проводились, також, і для файлового ЗПЗ. Їх результати є достатніми для впровадження запропонованих рішень. Результати експериментальних досліджень з використанням розробленої системи Distributed Multilevel System підтверджують правильність наукових положень розроблених методів та ефективність архітектури РБС, оскільки її впровадження підвищує достовірність виявлення на 5–12 % в мережному представленні порівняно з хостовим, та на 2–4 % у порівнянні з існуючими мережними АПЗ виявлення файлового ЗПЗ. В цьому ж розділі запропоновано методику оцінки ефективності розподілених систем, здійснено оцінку ефективності розробленої РБС в порівняні її використання в хостовому представленні одним ПМ та РБС, в якій більше одного ПМ. В якості критеріїв ефективності було обрано такі: витрати часу на здійснення процесу виявлення хостом; витрати часу на здійснення процесу виявлення всією РБС; оперативність у прийнятті рішень; ресурсоспоживання; достовірність

виявлення за часом, який витрачався на обробку помилок першого, другого та третього роду. Для цих критеріїв було встановлено аналітичні залежності, за якими отримано числові значення.

Висновки в дисертаційній роботі сформульовані чітко. Вони повністю відображають отримані результати. За своїм рівнем висновки відповідають вимогам, які висуваються до наукових результатів докторської дисертації.

Список використаних джерел є інформативним, достатньо повно охоплює предметну галузь та відображає опрацювання автором значної кількості сучасних іноземних джерел.

Додатки до роботи є змістовними і підтверджують позитивні результати роботи. Вони містять таблиці з даними необхідними для визначення подальших кроків РБС, функції та модулі розробленого програмного забезпечення Distributed Multilevel System, розроблений апаратно-програмний пристрій компоненти РБС, фрагмент результатів роботи РБС Distributed Multilevel System, список публікацій здобувача, п'ять актів впровадження результатів дисертаційної роботи в підприємствах та у навчальний процес.

7. Стиль, оформлення дисертації, автореферату. Повнота викладення наукових положень, висновків та рекомендаціях у публікаціях та відповідність спеціальності

Об'єм, структура, оформлення матеріалів досліджень відповідають вимогам «Порядку присудження наукових ступенів» щодо дисертацій на здобуття наукового ступеня доктора технічних наук.

Дисертаційна робота має чітку логічну структуру. Висновки і рекомендації логічно витікають із результатів, які наведено у розділах роботи. Зміст автореферату ідентичний основним положенням дисертації.

Усі основні положення та найбільш важливі результати дисертації, подані до захисту, опубліковані в необхідному обсязі у фахових наукових виданнях України та закордонних виданнях, пройшли відповідну апробацію на 45 міжнародних науково-технічних конференціях. За темою дисертації з

викладенням основних її результатів опубліковано 51 наукових праць, з них в 21 викладено основні наукові результати: 2 статті у періодичних зарубіжних виданнях і 3 статті індексовані у наукометричних базах, 19 статей у фахових наукових виданнях України. Апробація засвідчена публікаціями 7 статей у періодичних зарубіжних серійних виданнях і 7 праць в матеріалах зарубіжних та українських конференцій, індексованих у наукометричній базі Scopus, з яких 9 індексовані у наукометричній базі Web of Science, 11 статей та тез доповідей у журналах та збірниках праць конференцій. Автором, також, опубліковано 3 патенти на корисну модель та 2 свідоцтва про реєстрацію авторського права на твір (програму). Вимоги щодо кількості та якості публікацій виконано.

Дисертація за змістом та отриманими науковими результатами відповідає паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти, зокрема, п. 6 «Теоретичні основи, методи й апаратно-програмні засоби комп'ютерної криптографії, розподілу доступу та захисту інформації в комп'ютерних системах і мережах», п. 1 «Теоретичні основи створення та вдосконалення високоефективних технічних і програмних компонентів комп'ютерних систем і мереж загального та спеціального призначення, розподілених систем та їх компонентів відповідно до різних ієрархічних рівнів їх організації й умов експлуатації», п.3 «Теоретичні основи, методи та технології системного та прикладного програмування, створення операційних систем для комп'ютерних систем і мереж загального та спеціального призначення, паралельних комп'ютерних систем і мереж, технічних і програмних засобів взаємодії людини з комп'ютерними системами та мережами, мережних технологій обробки інформації».

8. Зауваження.

До зауважень та недоліків дисертації відноситься наступне:

1. Модель взаємодії основних функцій рівнів децентралізації та прийняття рішень (рис. 2.4, стор. 95) подана дещо схематично, без конкретизації зв'язків між її складовими частинами.

2. Відсутнє формальне обґрунтування розрахунку значень коефіцієнтів загроз для різних станів програмних модулів (табл. 2.11, стор. 140).

3. В дисертації доцільно розглянути варіант протидії розподіленій керованій бот-мережі на основі застосування мережецентричного підходу, для забезпечення режиму оперативного моніторингу дій зловмисних програм на основі формування цілісного середовища засобів захисту, що забезпечить процес постійної актуалізації даних про атаки з урахуванням значного числа джерел інформації щодо атак.

4. Доцільно розглянути варіант аналізу поведінкової сигнатури в методі виявлення файлового зловмисного програмного забезпечення на основі використання нейромережевих технологій.

5. Відсутня узагальнена модель поведінки зловмисника, в т. ч. зловмисного програмного забезпечення в локальній комп'ютерній мережі.

6. Загальна ефективність роботи розподіленої системи обчислена тільки для одного випадку і не розглянуто для випадку, коли в складі системи тільки одна компонента, а також, коли кількість компонентів збільшена вдвічі порівняно з розрахунками для експериментального прикладу, що не дозволяє оцінити досягнення переваги розподіленої системи порівняно з хостовою системою та суттєвим зростанням кількості компонентів системи.

Зазначені зауваження не є принциповими, вони істотно не впливають на зміст дисертаційної роботи та не знижують її наукової цінності.

9. Загальні висновки.

Дисертаційна робота Савенка Олега Станіславовича є завершеною науково-дослідною роботою, яка містить нові науково обґрунтовані результати вирішення актуальної науково-технічної проблеми покращення ефективності виявлення зловмисного програмного забезпечення шляхом розроблення теорії і практики створення розподілених систем у локальних комп'ютерних мережах на основі принципів децентралізації та самоорганізації.

Отримано нові, науково обґрунтовані, теоретичні результати є значущими для галузі інформаційних технологій. Тема дисертації відповідає

спеціальності 05.13.05 – комп'ютерні системи та компоненти.

З огляду на актуальність теми дисертації, практичну корисність отриманих результатів досліджень, отриману сукупність теоретичних результатів, вважаю, що дисертація відповідає вимогам пп. 9, 10, 12 «Порядку присудження наукових ступенів», а її автор, Савенко Олег Станіславович, заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
професор кафедри математичних методів системного аналізу
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
доктор технічних наук, професор,

В.Є. Мухін

Підпис професора кафедри математичних методів системного аналізу
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
д. т. н., проф. Мухіна В.Є. засвідчую:

Вчений секретар
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
кандидат філософських наук, доцент

А.А. Мельниченко