67-72-102/1
10.10.2019

ВІДГУК

офіційного опонента, доктора технічних наук, професора, завідувача кафедри «Електронні обчислювальні машини» Національного університету «Львівська політехніка»,
Мельника Анатолія Олексійовича
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.

В останні роки завдяки широкому використанню у всіх галузях людської діяльності комп'ютерів, підключених до локальних та глобальних комп'ютерних мереж, зростає шкода, яку наносить користувачам зловмисне програмне забезпечення (ЗПЗ). Існуючі антивірусні засоби різноманітного спрямування не здатні забезпечити надійного захисту інформації та повного виявлення ЗПЗ. Більше того, розробники ЗПЗ перейшли від розробки звичайних комп'ютерних вірусів до створення цілеспрямованих програмних систем з набором ефективних засобів для проникнення, поширення та завдання збитків користувачам комп'ютерів. Об'єктами дії ЗПЗ все частіше стають комп'ютерні засоби підприємств та організацій. При створенні таких засобів зловмисники активно використовують технології та методи теорії розподілених систем. Це дозволяє їм розробляти програмні засоби, побудовані із заданим цілеспрямованим функціоналом та багатоваріантністю, які можуть отримувати контроль над комп'ютерами користувачів, керувати великими розподіленими обчислювальними ресурсами, вирішувати поставлені завдання і, при цьому, приховувати реальне місце розміщення зловмисника. Це ЗПЗ орієнтоване на тривале використання, уникнення виявлення, цілеспрямований пошук об'єктів та оперативне застосування. Якщо користуватись тільки хостовими антивірусними засобами виявлення такого розподіленого ЗПЗ стає тривалою і важковирішуваною проблемою.

В дисертаційній роботі пропонується для протидії керованому розподіленому ЗПЗ використовувати розподілені антивірусні засоби. Автор дисертації доводить перевагу такого підходу як напряму подальших перспективних досліджень для вирішення проблеми покращення ефективності виявлення ЗПЗ шляхом побудови в локальній комп'ютерній мережі розподіленої системи, яка здійснює керування обчислювальними ресурсами мережі з використанням методів виявлення ЗПЗ, яке проникло в комп'ютери користувачів ззовні або

було безпосередньо внесено користувачами. При використанні таких розподілених систем виявлення адміністратор мережі підприємства отримує перевагу над ЗПЗ, оскільки до комп'ютерних систем завантажують типове програмне забезпечення на відміну від користувачів приватних комп'ютерів і, крім того, такі розподілені системи надають можливість аналізувати події з різних комп'ютерних систем. Пропоновані в дисертації розподілені системи виявлення спрямовані на пошук лише того ЗПЗ, яке пройшло попередні рівні захисту, має типові характерні ознаки ЗПЗ та може бути частиною великого програмного комплексу, зокрема, містити в локальній комп'ютерній мережі центр або кінцеві компоненти. Наявність компонентів ЗПЗ поза локальною комп'ютерною мережею через можливе перебування на великих фізичних відстанях такими розподіленими системами не відслідковується. Крім того, при визначенні достовірності виявлення досліджувані в роботі мережні системи виявлення ЗПЗ володіють рядом недоліків і не мають суттєвої переваги над хостовими.

Розроблена автором розподілена система наповнюється засобами виявлення, які реалізовані методами виявлення файлового та мережного ЗПЗ, що враховують особливості виявлення на основі їх застосування в локальних комп'ютерних мережах. Об'єкти дослідження формалізовано з використанням апарату абстрактної алгебри з подальшою їх деталізацією до рівня матриць та функцій прикладного програмного інтерфейсу, що дозволило узагальнити спільні особливості файлового та мережного зловмисного програмного забезпечення для представлення їх поведінковими сигнатурами в типових класах. З метою урізноманітнення виявлення ЗПЗ такими розподіленими системами та уникнення впливу адміністратора мережі в роботі пропонується створення розподілених систем виявлення на основі принципів децентралізації та самоорганізації, що створює зловмисникам проблеми з пошуком центру системи і усуває адміністратора мережі від прийняття рішень.

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.

Представлена дисертаційна робота Савенка О.С. 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), держбюджетної науково-дослідної роботи № 1Б-2001 «Методологія тестового комбінованого діагностування мікропроцесорних пристроїв та систем (МПП та С) на базі компонентів штучного інтелекту» (номер державної реєстрації 0101U005058), держбюджетної науково-дослідної роботи № 4Б-2012 «Розвиток теоретичних основ та розробка методів статико-динамічного спектрального оцінювання сигналів в радіолокації» (номер державної реєстрації 0112U002247), держбюджетної науково-дослідної роботи № 1Б-2018 «Розроблення високоефективних методів відбору енергії від фотоелектричних модулів» (номер державної реєстрації 0116U001548).

Тематика дисертаційного дослідження відповідає пріоритетним напрямам розвитку науки і техніки на період до 2020 року (статті 3 Закону України «Про пріоритетні напрями розвитку науки і техніки»), які визначені Верховною Радою України та Наказом МОН України №1446 від 28.12.2018 р.

2. Ступінь обґрунтованості наукових положень, висновків та рекомендацій.

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

Наукові положення, висновки та рекомендації, сформульовані в дисертації чітко та логічно випливають із результатів, які отримані за допомогою викладок з коректним використанням принципів загальної теорії систем, системного аналізу, методів аналізу та моделювання процесів, теоретико-множинних підходів, алгебраїчних систем та алгебр, теорії множин, евристичних оцінок, загальних принципів теорії розподілених систем та застосування принципів децентралізації і самоорганізації, як комплексних характеристик і властивостей систем.

Наукові положення, висновки і рекомендації, які сформульовані в дисертаційній роботі Савенка О.С. стосуються розроблення теорії та практики створення розподілених систем виявлення ЗПЗ в локальних комп'ютерних мережах.

Відзначаю, що наукові положення та рекомендації висновків до всіх розділів

дисертаційної роботи та загальних висновків до дисертаційної роботи сформульовано науково обґрунтовано і логічно за результатами аналізу, узагальнення відомих та отриманих нових результатів, теоретичних досліджень, а також експериментальної перевірки розробленої розподіленої багаторівневої системи виявлення ЗПЗ в локальних комп'ютерних мережах.

3. Достовірність наукових положень, висновків та рекомендацій.

Достовірність наукових положень, висновків та рекомендацій підтверджується повнотою розгляду об'єкта дослідження та застосуванням методів, адекватних предмету дослідження. Достовірність забезпечується також коректною постановкою проблеми, мети та наукових 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.

Достовірність і обґрунтованість результатів базується на обґрунтованому використанні: принципів загальної теорії систем, системного аналізу, методів аналізу та моделювання процесів, теоретико-множинних підходів, алгебраїчних систем та алгебр, теорії множин, евристичних оцінок, загальних принципів теорії розподілених систем та теорії проектування комп'ютерних мереж.

Достовірність результатів базується також на успішній апробації отриманих результатів на 45 Міжнародних та Всеукраїнських науково-технічних і науково-практичних конференціях (в тому числі на закордонних і таких, матеріали яких індексуються в наукометричних базах Scopus та Web of Science).

Достовірність теоретичних та практичних результатів підтверджується успішним впровадженням отриманих рішень в Державному підприємстві «Новатор», ТОВ «ІТТ – 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 – покращенні ефективності виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах шляхом розроблення теорії і практики створення розподілених систем виявлення. Вирішення цієї проблеми має важливе значення для усіх галузей, де застосовуються локальні комп'ютерні мережі.

В дисертаційній роботі Савенка О.С. отримані такі наукові результати:

1) удосконалено модель архітектури розподіленої системи виявлення ЗПЗ в

локальних комп'ютерних мережах, яка відрізняється від відомих комплексним врахуванням 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 ЗПЗ та нарощення своїх функціональних можливостей;

2) вперше розроблено модель архітектури типових компонентів розподіленої багаторівневої системи виявлення ЗПЗ 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 ЗПЗ 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 ЗПЗ шляхом їх подання алгебрами поведінки, що дозволило створити базис поведінкових сигнатур, і, на відміну від відомих представлень, врахувати особливості функціонування ЗПЗ 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 ЗПЗ в локальних комп'ютерних мережах, який полягає в поєднанні роботи програмних агентів, що здійснюють виявлення ЗПЗ 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 ЗПЗ;

7) вперше розроблено метод виявлення файлового ЗПЗ 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 ЗПЗ 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 ЗПЗ в локальних комп'ютерних мережах, яка є основою для створення мережних систем виявлення ЗПЗ. Розроблена архітектура розподіленої системи, в якій здійснено комплексне врахування вимог самоорганізованості, децентралізованості та багаторівневості, 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 можливості створення розподілених систем виявлення ЗПЗ та використовується для проведення експериментальних досліджень при порівнянні з існуючими мережними 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 в дисертаційній роботі проводились з врахуванням їх наступної практичної реалізації. Результати досліджень можуть бути рекомендовані до впровадження в діяльності ІТ 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, основний текст - 304 сторінки, які включають 54 рисунки та 46 таблиць.

Вступ дисертаційної роботи присвячено обґрунтуванню актуальності тематики дослідження, окреслено науково-технічну 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.

Перший розділ містить аналіз і дослідження стану розвитку ЗПЗ, мережних систем виявлення ЗПЗ та результатів достовірності їх роботи. В результаті дослідження функціонування ЗПЗ в локальних комп'ютерних мереж (ЛКМ) та антивірусних засобів їх виявлення автором зроблено такі висновки: розробники ЗПЗ володіють сучасними інформаційними технологіями для його створення; ЗПЗ може використовувати різні засоби для поширення та стійкості, що підвищує його життєздатність, можливості для поширення та ускладнює виявлення антивірусними засобами; певні типи ЗПЗ мають модульну архітектуру, що впливає на зниження ефективності виявлення існуючими антивірусними засобами; застосування відомих методів виявлення не гарантує належного рівня достовірності виявлення ЗПЗ в ЛКМ через можливість їх обходу; використання технологій поліморфізму 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 дає однозначної відповіді 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 зі сторони зловмисника до розробленої РБС виявлення ЗПЗ запропоновано включити вимоги такі, як самоорганізованість та децентралізованість.

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

Другий розділ містить удосконалену автором модель архітектури розподіленої багаторівневої системи виявлення ЗПЗ в ЛКМ. Також, автором розроблені модель архітектури типових компонентів РБС на основі структур Кріпке та метод взаємодії компонентів РБС. Архітектуру РБС спроектовано з врахування вимог розподіленості, децентралізованості, багаторівневості та самоорганізованості. РБС побудовано із сукупності однакових компонентів, які розміщуються у вузлах локальної комп'ютерної мережі і об'єднані зв'язуючою частиною програмного забезпечення, яке підтримує цілісність системи на основі розробленого методу взаємодії компонентів РБС. Особливістю розробленого методу є можливість динамічної зміни архітектури всієї РБС. 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.

Третій розділ дисертаційної роботи містить удосконалені моделі зловмисного програмного забезпечення. 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 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 ЛКМ. На основі удосконалених моделей типів зловмисного програмного забезпечення 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 метод виявлення бот-мереж у локальних комп'ютерних мережах, суть якого полягає в здійсненні активного моніторингу системних подій та узгодженій взаємодії компонентів розподіленої системи при прийнятті рішення про подальші кроки, включаючи виявлення. З метою розробки методу виявлення сформовано еталонну модель бот-мережі, яка увібрала в себе всі особливості такого типу керованого розподіленого ЗПЗ. Також сформовані і згруповані за типами відомі бот-мережі. Після

формування класів бот-мереж здійснено їх представлення через функції прикладного програмного інтерфейсу. Ці функції стали деталізацією характерних ознак бот-мереж, які подані вищим рівнем абстракції через можливі їх прояви та дії. ЗПЗ такого типу є складними програмними комплексами, які функціонують у глобальних комп'ютерних мережах, тому для їх виявлення розроблено метод, застосування та реалізація якого відповідними засобами імплементована саме в розподілених системах. Важливою особливістю розробленого методу та використання розподіленої системи є те, що РБС може динамічно змінювати свою архітектуру та визначати подальші кроки на основі стратегій.

П'ятий розділ присвячено представленню розроблених методів виявлення файлового ЗПЗ в ЛКМ, зокрема, методу виявлення файлового ЗПЗ в локальних комп'ютерних мережах, який полягає в поєднанні роботи програмних агентів, що здійснюють виявлення ЗПЗ 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 ЗПЗ. Метод виявлення файлового ЗПЗ 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. Розроблені методи реалізуються засобами, що включаються в РБС і тоді можлива динамічна зміна архітектури РБС в залежності від результатів застосування методів та визначення подальших кроків дій системи.

У **шостому розділі** представлена програмна реалізація РБС, результати її застосування при виявленні різних типів ЗПЗ у ЛКМ, а також розроблена методика обчислення ефективності роботи РБС. У розробленому варіанті програмного забезпечення РБС відображено вимоги децентралізованості, самоорганонізованості, багаторівневості та розподіленості. 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 (Баєсів класифікатор) 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.

В цьому ж розділі запропоновано методику обчислення ефективності розподілених систем виявлення, здійснено обчислення ефективності виявлення розробленою 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 і повністю відображають отримані результати. За своїм рівнем висновки відповідають вимогам, які висуваються до наукових результатів докторської дисертації.

Список використаних джерел охоплює предметну галузь на належному рівні та відображає опрацювання автором значної кількості сучасних іноземних джерел.

Додатки до роботи є змістовними, доповнюють представлені в роботі таблиці значень функцій, підтверджують позитивні результати роботи і містять таблиці з даними 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, акти 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

Дисертаційна робота Савенка О.С. подана з використанням формально-логічного способу викладення матеріалу. Для вираження логічних зв'язків автор використовує причинно-наслідкові відношення, що вказують на послідовність розвитку думки. Всі частини роботи взаємоузгоджені, а її структура є логічною. Мовностилістичне оформлення дисертаційної роботи здійснене на високому науковому рівні. В цілому дисертаційна робота оформлена у відповідності до вимог «Порядку присудження наукових ступенів» щодо дисертацій на здобуття наукового ступеня доктора технічних наук.

Зміст автореферату ідентичний основним положенням дисертаційної роботи.

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 наукову працю, 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 потрібно віднести наступне:

1. В дисертації відсутній детальний аналіз відомих розподілених комп'ютерних систем, побудованих на основі принципів децентралізації та самоорганізації, що затрудняє оцінити рівень новизни удосконаленої моделі архітектури розподіленої системи виявлення ЗПЗ в локальних комп'ютерних мережах в частині врахування вимог де централізованості та самоорганізованості.
2. В роботі не показано, який вплив на стратегію подальших дій системи в цілому мають значення рівня безпеки системи.
3. Для розуміння інформаційних потоків в розроблених розподілених багаторівневих системах потрібно було показати схеми об'єднання комп'ютерів в локальну мережу цими багаторівневими системами.
4. Розроблення аналітичних виразів та функцій (ст.141, формула (2.17); ст.142-143, таблиця 2.12), на основі яких здійснюється визначення розподіленою багаторівневою системою подальших кроків, базується на емпіричних представленнях можливих ступенів їх безпеки (ст.130, крок 7 методу), що впливатиме на точність у визначенні подальших дій розподіленої багаторівневої системи і тому потребує доведення правильності для застосування при створенні таких систем.
5. Результати дисертаційної роботи стосовно розроблення теорії створення розподілених систем виявлення ЗПЗ в локальних комп'ютерних мережах обмежуються місцем застосування (локальними мережами) і не поширюються шляхом їх масштабування на корпоративні мережі та інші обчислювальні системи з розподіленими компонентами, що є недостатнім для практики використання запропонованих рішень.
6. В роботі доцільно було провести дослідження можливої надмірності системи в зв'язку із реалізацією в архітектурі розподілених багаторівневих систем принципу децентралізованості, а також дослідити можливість перевантаженості системи та перевантаження трафіку мережі.
7. Для розвитку теоретичних основ побудови розподілених систем виявлення ЗПЗ доцільним було визначити вагу кожної з характеристик (самоорганізованість, децентралізованість, багаторівневість) та встановити визначальну з них для здійснення представлення таких систем, починаючи з визначальної характеристики.
8. В роботі недостатньо повно представлений планувальник стратегій прийняття рішення щодо подальших кроків розподіленої багаторівневої системи у випадку зміни стану її безпеки та виборі стратегії. Це не дозволяє здійснити оцінку можливих кроків при переході від однієї стратегії до іншої. Крім того, такий планувальник потребує функціонального опису.
9. Представлений в роботі метод взаємодії компонентів розподілених багаторівневих

систем використовує на кроці 6.4 (ст.129) результати обчислення за формулами (2.12) і (2.39), виведення яких здійснюється після завершення подання кроків методу, що порушує послідовність викладеного дослідження.

10. Розроблена розподілена багаторівнева система може бути основою для створення розподілених засобів виявлення ЗПЗ, але з практичної сторони функціонування локальних комп'ютерних мереж в роботі не врегульовано питання узгодження роботи таких систем з різними типами системного програмного забезпечення.

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

9. Загальні висновки.

Дисертаційна робота Савенка О. С. 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.

Враховуючи 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 – завідувач кафедри «Електронні обчислювальні машини»
Національного університету «Львівська політехніка»,
доктор технічних наук, професор А. О. Мельник

Підпис завідувача кафедри «Електронні обчислювальні машини»
Мельника А. О. засвідчую.
Учений секретар Національного університету
«Львівська політехніка»
кандидат технічних наук, доцент Р. Б. Брилинський