67-72-102/3
10.10.2019

# ВІДГУК

офіційного опонента на дисертаційну роботу Савенка Олега Станіславовича «Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах», яка подана на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

## 1. Актуальність теми дисертації.

Роль антивірусних засобів в умовах тотальної інформатизації суспільства на сьогоднішній день продовжує залишатись важливою. Динамічне зростання кількості комп'ютерних систем, їх об'єднання в локальні мережі та підключення до мережі Інтернет створює проблеми, пов'язані з їх використанням. Однією з таких проблем є розробка та поширення зловмисного програмного забезпечення (ЗПЗ). Його діяльність призводить до неправильного функціонування системного програмного забезпечення та витоку конфіденційної інформації.

Сучасні антивірусні засоби використовують велику кількість методів та підходів до пошуку та виявлення ЗПЗ, проте кожен із них має певні недоліки у виявленні нового ЗПЗ та не забезпечують повного виявлення, чим суттєво знижують достовірність та ефективність виявлення в комп'ютерних системах. Крім того, сучасне ЗПЗ представляє собою складні багатофункційні програмні системи та комплекси, які побудовані з використанням ефективних методів створення програмних засобів та методів поширення зловмисного коду. Дослідження відомих антивірусних методів та засобів вказують, що реалізація нових принципів, моделей та методів виявлення конкретних типів ЗПЗ шляхом створення відповідних систем виявлення потребує подальшого розвитку. Перспективним напрямом досліджень створення ефективних систем виявлення ЗПЗ є мережні системи, які використовуються в локальних комп'ютерних мережах (ЛКМ) організацій (підприємств). Такі засоби виявлення мають розподілену архітектуру і, тому, покращення ефективності виявлення ЗПЗ можливе за рахунок ефективної організації обчислювальних ресурсів ЛКМ.

Викладене вище достатньо аргументує актуальність дисертаційної роботи Савенка О.С., яка присвячена вирішенню наукової проблеми покращення ефективності виявлення ЗПЗ шляхом розроблення теорії і практики створення розподілених систем у ЛКМ на основі принципів децентралізації та самоорганізації. Актуальність проблеми та важливість отриманих результатів підтверджується їх впровадженням на підприємствах, які займаються розробленням програмного забезпечення та комп'ютерних і телекомунікаційних систем.

*Зв'язок роботи з науковими програмами, планами, темами.* Тематика дисертаційного дослідження відповідає пріоритетним напрямкам розвитку науки і техніки на період до 2020 року, визначеним Верховною Радою України. Дослідження, представлені у дисертації, проводились в межах держбюджетних науково-дослідних робіт Хмельницького національного університету 1Б-2001 «Методологія тестового комбінованого діагностування мікропроцесорних пристроїв та систем на базі компонентів штучного інтелекту», 4Б-2012 «Розвиток теоретичних основ та розробка методів статико-динамічного спектрального оцінювання сигналів в радіолокації», 1Б-2018 «Розроблення високоефективних методів відбору енергії від фотоелектричних модулів», 1Б-2019 «Агентно-орієнтована система підвищення безпеки та якості програмного забезпечення комп'ютерних систем».

**2. Ступінь обґрунтованості наукових положень, висновків та рекомендацій.**

Наукові положення, висновки і рекомендації дисертації обґрунтовані коректним та доцільним використанням математичного апарату, розробленими методами здійснення виявлення ЗПЗ, програмною реалізацією розробленої розподіленої багаторівневої системи (РБС) виявлення ЗПЗ в ЛКМ, ефективним практичним впровадженням результатів дисертаційного дослідження в підприємствах, що експлуатують комп'ютерні системи, яке продемонструвало відповідність теоретичних досліджень з реальними результатами застосування.

Наукові положення, висновки і рекомендації, сформульовані в дисертаційній роботі Савенка О.С., стосуються розроблення теорії та практики створення розподілених систем виявлення ЗПЗ в ЛКМ.

Для теоретичного обґрунтування наукових положень та висновків дисертант використав: принципи загальної теорії систем, системний аналіз, теоретико-множинні підходи, алгебраїчні системи і алгебри, теорію множин, евристичні оцінки, принципи створення розподілених та самоорганізованих систем, методи лексичного та синтаксичного аналізу. Розроблені дисертантом практичні рекомендації ґрунтуються на розроблених ним наукових положеннях. Отже, наукові положення, висновки та рекомендації дисертаційної роботи сформульовані обґрунтовано і логічно за результатами проведених теоретичних досліджень та експериментів.

**3. Достовірність наукових положень, висновків та рекомендацій.**

Достовірність наукових положень, висновків та рекомендацій забезпечується коректною постановкою проблеми та задач дисертаційного дослідження, які розв'язуються логічно, послідовно та аргументовано. Достовірність результатів підтверджується відповідністю методології дослідження поставленій проблемі покращення ефективності виявлення ЗПЗ,

повнотою розгляду об'єкта дослідження, застосуванням методів, адекватних предмету дослідження.

Достовірність результатів базується, також, на експериментальних дослідженнях, які продемонстрували збігання теоретичних досліджень з реальними результатами, а також в їх апробації на 45 Міжнародних та Всеукраїнських науково-технічних і науково-практичних конференціях та впровадженні отриманих рішень в Державному підприємстві «Новатор», ТОВ «ITT – telecommunication company», ТОВ «ЮКС++», компанії CYPRESS SEMICONDUCTOR, а також у навчальному процесі університету.

**4. Наукова новизна одержаних результатів.**

Наукова новизна досліджень полягає у вирішенні актуальної науково-технічної проблеми – здійсненню розвитку теорії і практики створення розподілених систем виявлення ЗПЗ в ЛКМ для покращення ефективності його виявлення. Вирішення даної проблеми має важливе значення в усіх галузях, де активно застосовуються ЛКМ.

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

1) Модель архітектури розподіленої системи виявлення ЗПЗ в ЛКМ, яка удосконалена комплексним врахуванням вимог розподіленості, децентралізованості, багаторівневості та самоорганізованості. Модель служить основою для створення розподілених систем та їх компонентів з автономним функціонуванням і самостійним прийняттям рішень про наявність ЗПЗ та нарощенням функціональних можливостей.

2) Модель архітектури типових компонентів РБС виявлення ЗПЗ, яка вперше розроблена на основі структур Кріпке з представленням компонентів через стани функціонування Модель є основою для визначення стану безпеки розподіленої системи та її окремих компонентів.

3) Метод взаємодії компонентів РБС виявлення ЗПЗ, який вперше розроблений з підтримкою її цілісності та визначення порядку передачі знань між її компонентами. Метод використовує встановлені аналітичні залежності між рівнями безпеки програмних модулів та рівнем безпеки всієї РБС для автономної зміни своєї архітектури та функцій і визначення стратегії подальшої роботи.

4) Моделі ЗПЗ, які удосконалені їх поданням за алгебрами поведінки для створення базису поведінкових сигнатур. Моделі враховують особливості функціонування ЗПЗ в ЛКМ і визначають його класифікацію за типами поведінки.

5) Метод виявлення бот-мереж у ЛКМ, який вперше розроблений із здійсненням активного моніторингу системних подій та узгодженням взаємодії компонентів розподіленої системи при прийнятті рішення. Метод

забезпечує створення засобів, здатних до інтегрування в розподілену систему, та класифікацію бот-мереж за їх поведінковими сигнатурами.

6) Метод виявлення файлового ЗПЗ в ЛКМ, який вперше розроблений з поєднанням роботи програмних агентів, що здійснюють виявлення ЗПЗ в окремих комп'ютерних системах, відповідно до імплементованих в них методів: динамічного формування поведінкової сигнатури, знаходження поліморфного та метаморфного програмного коду, сканування виконуваних програм. Метод покращує аналіз і підвищує достовірність виявлення ЗПЗ.

7) Метод виявлення файлового ЗПЗ, який вперше розроблений з динамічним формуванням поведінкової сигнатури за викликами прикладного програмного інтерфейсу. Метод дає змогу виявляти нові версії відомого ЗПЗ, враховуючи не тільки критичні виклики, але й їх взаємодію між собою.

8) Метод виявлення поліморфних та метаморфних вірусів з використанням функцій заплутування програмного коду, який розроблено вперше з поетапним аналізом і порівнянням функціональних блоків програмного об'єкта та його змінених версій, отриманих від різних компонентів розподіленої системи.

Матеріали кандидатської дисертації Савенка О.С. у його докторській дисертації не використовувались.

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

Практичне значення дисертаційної роботи полягає у розробленні архітектури і компонентів РБС виявлення ЗПЗ в ЛКМ, здійсненні їх програмної реалізації, а також розроблені апаратно-програмних засобів захисту інформації в складі компонентів РБС, використання яких регламентується вимогами безпеки. Крім того, здійснено формалізацію ЗПЗ для представлення об'єктів дослідження за їх типами характеристичної поведінки, що надало можливість виділяти ці особливості при виявленні. Результати експериментальних досліджень підтверджують ефективність розроблених програмних засобів, а також правильність наукових положень теорії розподілених систем, оскільки впровадження РБС виявлення ЗПЗ дозволяє підвищити достовірність виявлення на 5–12 % порівняно з відомими аналогами та знизити рівень помилок першого роду до 5 %.

Теоретичні та практичні результати роботи впроваджено в Державному підприємстві «Новатор», ТОВ «ІТТ – telecommunication company», ТОВ «ЮКС++», компанії CYPRESS SEMICONDUCTOR та навчальному 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 дисертаційної роботи можуть бути запропоновані для використання науковими організаціями і підприємствами, які займаються розробкою та впровадженням мережних антивірусних засобів з метою покращення ефективності їх функціонування.

**6. Оцінка змісту дисертаційної роботи.**

Дисертаційна робота містить анотацію, вступ, 6 розділів, висновок, перелік використаних джерел з 399 найменувань на 49 сторінках і додатків на 46 сторінках. Загальний обсяг дисертації становить 425 сторінок (304 сторінки основного тексту). Робота має 54 рисунки та 46 таблиць.

У *вступі* обґрунтовано актуальність тематики дослідження, визначено об'єкт, предмет, мету і завдання дослідження, визначено наукову новизну та практичну цінність одержаних результатів, а також вказано на зв'язок роботи з науково-дослідними роботами, які виконувались в Хмельницькому національному університеті, і надано інформацію щодо кількості публікацій та апробації результатів дисертації.

У *першому розділі* автором здійснено дослідження технологій розвитку ЗПЗ, систем виявлення ЗПЗ, достовірності результатів їх роботи, а також проаналізовано стандартні архітектури розподілених систем та їх відомі типові реалізації. Отримані автором результати дослідження функціонування ЗПЗ в ЛКМ та антивірусних засобів їх виявлення вказують на недоліки відомих хостових і мережних систем виявлення ЗПЗ, а також обґрунтовують перспективний напрям подальших досліджень для покращення ефективності виявлення ЗПЗ.

Обґрунтування актуальності вирішуваної наукової проблеми автор виконав в повній мірі.

У *другому розділі* автором розроблено та представлено удосконалену модель архітектури РБС виявлення ЗПЗ в ЛКМ. Архітектуру РБС було синтезовано на основі комплексного врахування вимог розподіленості, децентралізованості, багаторівневості та самоорганізованості. Запропоноване рішення дозволяє створювати системи виявлення ЗПЗ, які функціонуватимуть самостійно без втручання користувача.

Автором розроблена модель архітектури типових компонентів РБС на основі структур Кріпке. На основі цієї моделі запропоновано формувати РБС із сукупності однакових компонентів (програмних модулів). Кожен з них має однакову архітектуру. В кожному виділено чотири основних рівні залежно від функційного призначення та згрупованих у них завдань. Кожен рівень та відповідні йому узагальнені підсистеми в свою чергу представляються наборами підрівнів, в які закладено виконання певних функціоналів. Опис деталізованих підрівнів представлено структурами Кріпке, що надало змогу виразити аналітичними виразами стан безпеки всієї РБС.

Для встановлення порядку здійснення комунікації між компонентами РБС та обміну знаннями між ними автором розроблено метод взаємодії компонентів РБС виявлення ЗПЗ. Основним результатом застосування методу, який реалізується в РБС, це динамічне самостійне здійснення зміни архітектури РБС на основі обчислених значень рівнів безпеки.

У *третьому розділі* удосконалено моделі ЗПЗ за алгебрами поведінки для створення базису поведінкових сигнатур, в яких враховано особливості функціонування ЗПЗ у ЛКМ.

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, змогло подолати певні системи захисту і функціонує там. Розроблені алгебри поведінки типів ЗПЗ враховують особливості, які 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 ЛКМ, який базується на здійсненні активного моніторингу системних подій та узгодженій взаємодії компонентів РБС при прийнятті рішення. За об'єкти дослідження мережного ЗПЗ розглянуто керовані бот-мережі. Для їх виявлення пропонується пошук та виокремлення характерних для цього типу ознак. 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. В методі виявлення бот-мереж використано класифікатор для віднесення до одного із заданих типів бот-мереж.

У *п'ятому розділі* розроблено низку методів виявлення файлового ЗПЗ в ЛКМ: метод виявлення файлового ЗПЗ в ЛКМ, метод динамічного формування поведінкової сигнатури шляхом відстеження викликів прикладного програмного інтерфейсу, метод знаходження поліморфного та метаморфного програмного коду. Для виявлення файлового ЗПЗ згідно розробленого методу залучаються обчислювальні ресурси ЛКМ.

У *шостому розділі* представлена програмна реалізація РБС з використанням запропонованих рішень, що забезпечило проведення експериментальних досліджень. Також, в цьому розділі запропонована методика визначення ефективності виявлення ЗПЗ розподіленими системами.

*Висновки* по роботі сформульовані чітко, вони повністю висвітлюють отримані в роботі результати. За своїм рівнем висновки відповідають вимогам, які висуваються до результатів докторської дисертації.

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

*Додатки* до роботи є змістовними і підтверджують позитивні результати роботи. Зокрема, в додатку А містяться таблиці, в яких представлено значення функції переходів між станами компонентів РБС, стратегії для подій у локальній мережі, зв'язок шляхів поширення файлового ЗПЗ та команд, в додатку Б представлені розроблене програмне забезпечення Distributed Multilevel System, в додатку В наведено апаратно-програмний пристрій РБС, в додатку Д представлено фрагмент результатів роботи РБС Distributed Multilevel System, в додатку Е подано список публікацій здобувача та відомості про апробацію результатів дисертації, в додатку Е представлені 5 актів впровадження результатів дисертаційної роботи у навчальний процес та на підприємствах.

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

Стиль, обсяг, структура, оформлення матеріалів дисертаційного дослідження відповідають вимогам «Порядку присудження наукових ступенів» щодо дисертацій на здобуття наукового ступеня доктора технічних наук. Дисертаційна робота має логічну структуру. Зміст автореферату ідентичний основним положенням дисертації.

Основні наукові результати дисертаційної роботи, подані до захисту, опубліковані в необхідному обсязі у періодичних зарубіжних виданнях, індексованих у наукометричних базах, фахових наукових виданнях України, а також апробовані на 45 Міжнародних та Всеукраїнських науково-технічних та науково-практичних конференціях. Вимоги щодо кількості та якості публікацій виконано. За темою дисертаційної роботи опубліковано 21 наукова праця, з них: 2 статті у періодичних зарубіжних виданнях і 3 статті, що індексовані у наукометричних базах, 19 статей у фахових наукових виданнях України. Крім того, опублікована низка робіт апробаційного характеру: 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 одержано 3 патенти на корисну модель та 2 свідоцтва про реєстрацію авторського права на твір (програму).

Дисертація відповідає формулі та 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 недоліків дисертації слід віднести наступне:

1. В дисертації не проаналізовано відомі методи організації взаємодії компонентів розподілених систем, зокрема побудованих на принципах децентралізації та самоорганізації.

2. Розрахунок безпеки РБС здійснюється за двома формулами на двох етапах (стор. 138, формула (2.12); стор. 150, формула (2.39)), а в роботі не показано, як ці формули та результати отримані, взаємозв'язані та на скільки різниця між їх значеннями впливає на стратегію подальших дій системи в цілому.

3. В роботі не відображено взаємозв'язку методу взаємодії компонентів РБС (стор. 133, рис. 2.14) та методів виявлення ЗПЗ в частині покращення ефективності виявлення.

4. Виклик методів виявлення ЗПЗ відображений повною групою подій і їх розміщенням в чотирьох рівнях (стор. 110, рис. 2.9), але не показано узагальнення розподілення методів у випадку появи нових методів, які не можуть бути віднесеними до одного із заданих рівнів, що не дозволяє оцінити можливість нарощення системи новими засобами.

5. Методи виявлення мережного та файлового ЗПЗ в ЛКМ містять спільні кроки (стор. 252-254, кроки 8-12; стор. 288-290, кроки 8-12) по залученню інших компонентів РБС, тому потрібно було відобразити цю спільну складову схемою, показати цей взаємозв'язок і саму спільну складову формалізованих об'єктів мережного та файлового ЗПЗ як об'єктів дослідження.

6. В роботі не відображено результати перевірки якості результатів класифікації (стор. 312, 313, табл. 6.6) на основі математичного апарату ROC-аналізу.

7. При визначенні загальної ефективності (стор. 325, E=0,83) роботи розподіленої системи не здійснено розрахунку для випадку, коли в складі системи тільки одна компонента, що не дозволяє оцінити досягнення переваги розподіленої системи порівняно з хостовою системою.

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 Олега Станіславовича «Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах» є завершеною науковою працею, в якій вирішено актуальну науково-технічну проблему – покращення ефективності виявлення ЗПЗ шляхом розвитку теорії і практики створення розподілених систем у ЛКМ на основі принципів децентралізації та самоорганізації.

Основні положення дисертаційної роботи доведені, теоретично обґрунтовані і практично підтверджені. Отримані наукові результати є значущими для галузі 05.13 – інформатика, обчислювальна техніка та автоматизація. Дисертаційна робота відповідає спеціальності 05.13.05 – комп'ютерні системи та компоненти.

Враховуючи актуальність дисертаційної роботи, наукову цінність та практичну корисність отриманих результатів досліджень, наукову зрілість та професійні якості дисертанта, вважаю, що дисертаційна робота 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 «Комп'ютерні інтелектуальні
системи та мережі» Одеського національного
політехнічного університету
доктор технічних наук, професор О.В. Дрозд

Вчений секретар Одеського національного
політехнічного університету В. І. Шевчук