Голові разової спеціалізованої
вченої ради ДФ 70.052.036
Хмельницького національного
університету
доктору технічних наук, професору
Тетяні ГОВОРУЩЕНКО

**РЕЦЕНЗІЯ**

на дисертаційне дослідження Савенка Богдана Олеговича
за темою «Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах»,
подане на здобуття ступеня доктора
філософії з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

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

Системи виявлення зловмисного програмного забезпечення (ЗПЗ) та комп'ютерних атак (КА) виступають об'єктами дослідження зловмисників. Для здійснення ефективних атак з використанням цілеспрямованого ЗПЗ зловмисники вивчають поведінку таких систем, а також досліджують їх надсилаючи в комп'ютерні станції запити. Тому, такі системи потрібно створювати таким чином, щоб вони створювали проблеми зловмисникам в частині розуміння їх поведінки.

Перспективною областю для розвитку розподілених систем протидії, виявлення та попередження ЗПЗ є корпоративні мережі. Їх організація та сформоване в них середовище дозволяють ефективно поєднати ресурси для протидії ЗПЗ та КА порівняно з іншими типами мереж. В зв'язку з цим дослідження систем попередження, виявлення та протидії ЗПЗ та КА в корпоративних мережах є актуальним.

Для забезпечення попередження, виявлення чи протидії ЗПЗ та КА розроблено багато різних методів. Ці методи втілені в архітектуру розподілених систем. Досліджень щодо саме впливу архітектури таких систем недостатньо. Універсальних платформ з різною архітектурою для імплементації в них методів виявлення, протидії та попередження ЗПЗ і КА немає, оскільки ця предметна область є досить специфічною і зловмисники отримали б доступ до них для вивчення їх поведінки, що призвело б до втрат в ефективності функціонування і досягнення ними належного результату. Тому, розроблення розподілених систем для виявлення, протидії та попередження ЗПЗ і КА в частині саме архітектури є перспективним, бо може покращити ефективність функціонування всієї системи, включаючи і втілені в неї методи.

В дисертації синтез розподілених систем виявлення, протидії та попередження ЗПЗ і КА запропоновано здійснювати згідно поєднання принципів часткової централізації, самоорганізації та адаптивності. Таке поєднання дає змогу отримати розподілені системи, в яких центр системи буде мігрувати між компонентами, система буде приймати рішення без втручань адміністратора та система буде здійснювати гнучку перебудову своєї архітектури в залежності від зміни

середовища корпоративної мережі. Такий напрям дослідження є перспективним та актуальним.

Отже, науково-прикладна задача з розроблення методів синтезу розподілених систем виявлення ЗПЗ в комп'ютерних мережах для покращення ефективності їх функціонування за рахунок поєднання в їх архітектурі принципів часткової централізації, самоорганізації та адаптивності є актуальною.

Дослідження, результати яких наведено в дисертації, проведені в рамках науково-дослідної тематики Хмельницького національного університету: держбюджетної науково-дослідної теми №1Б-2021 «Самоорганізована розподілена система виявлення зловмисного програмного забезпечення в комп'ютерних мережах» (ДР № 0121U109936); держбюджетної науково-дослідної теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (ДР № 0124U000980), в яких автор дисертації був виконавцем.

**2. Формулювання наукової задачі, мети й задач дослідження.**

Здобувачем правильно визначено об'єкт і предмет дослідження. Так, об'єктом дослідження визначено процес синтезу частково централізованих розподілених систем виявлення ЗПЗ. Предметом дослідження встановлено методи і розподілені системи з частковою централізацією для виявлення ЗПЗ в комп'ютерних мережах.

Мету дисертаційної роботи визначено, як покращення ефективності функціонування розподілених систем виявлення ЗПЗ в комп'ютерних мережах за рахунок синтезу в їх архітектурі принципів часткової централізації, самоорганізації та адаптивності.

Поставлену мету досягнуто в результаті розв'язання таких задач: 1) провести аналіз методів синтезу архітектури розподілених систем, моделей показників оточуючого середовища для розподілених систем в корпоративних мережах, методів організації функціонування розподілених систем та методів виявлення ЗПЗ, зокрема worm-вірусів; 2) розробити формальний опис середовища функціонування розподілених систем через характеристичні показники, які повинні враховуватись при визначенні рівнів безпеки компонентів частково централізованих розподілених систем та формування рішень щодо її подальших кроків і виявлення ЗПЗ; 3) розробити метод синтезу математичних моделей рівнів безпеки компонентів системи для отримання нових аналітичних виразів для комплексного опису оточуючого середовища і процесів, які відбуватимуться в частково централізованих розподілених системах; 4) удосконалити модель частково централізованих розподілених систем, в яких синтезувати принципи самоорганізації і адаптивності та врахувати характеристичні показники оточуючого середовища корпоративних мереж і процесів в розподілених системах, з метою розроблення згідно неї таких засобів, що будуть створювати проблеми зловмисникам щодо визначення ними центру їх системи, принципів функціонування, прийняття самостійних рішень та гнучкої перебудови їх архітектури; 5) розробити метод організації функціонування частково централізованих розподілених систем, в якому для функціонування такого типу систем провести розподіл компонент за відношенням до центру прийняття рішень, щоб реалізувати часткову централізацію сумісно з принципами самоорганізації та адаптивності, які задають механізми до самостійного прийняття рішень щодо

подальших кроків системою та перебудови її архітектури за потреби; 6) розробити метод виявлення worm-вірусів з використанням поділу їх на класи за спільними ознаками і визначеними критеріями та імплементувати його в архітектуру частково централізованих розподілених систем для прийняття рішення системою щодо виявлення ЗПЗ; 7) розробити частково централізовану розподілену систему виявлення worm-вірусів, провести з нею експериментальні дослідження щодо встановлення ефективності функціонування і достовірності виявлення worm-вірусів та впровадити її у виробництво.

**3. Наукова новизна** одержаних автором результатів полягає в наступному:

1) удосконалено модель частково централізованих розподілених систем виявлення зловмисного програмного забезпечення, в якій на відміну від відомих моделей синтезовано принципи самоорганізації та адаптивності таким чином, що така модель дала змогу створювати згідно неї системи виявлення зловмисного програмного забезпечення, функціонування яких ускладнює розуміння їх зловмисниками, дозволяє самостійно здійснювати прийняття рішень та гнучку перебудову архітектури, що покращує їх стійкість до зловмисних дій та виявлення зловмисного програмного забезпечення;

2) вперше розроблено метод синтезу математичних моделей рівнів безпеки компонентів системи для отримання нових аналітичних виразів комплексного опису оточуючого середовища корпоративних мереж і процесів, які відбуватимуться в частково централізованих розподілених системах, що дало змогу узгодити між собою характеристичні показники, які задані дискретними та неперервними величинами, та для формування нових характеристик аналітичними виразами з врахуванням їх при визначенні рівнів безпеки в компонентах і системах в цілому;

3) розроблено новий метод організації функціонування частково централізованих розподілених систем, в якому проведено розподіл компонент системи по відношенню до центра прийняття рішень для реалізації часткової централізації, самоорганізації та адаптивності, що дало змогу задати механізми ускладнення розуміння принципу їх функціонування, самостійного прийняття рішень щодо подальших кроків, перебудови їх архітектури та наповнення системи методами виявлення зловмисного програмного забезпечення;

4) розроблено новий метод виявлення worm-вірусів, суть якого в здійсненні поділу їх на класи за спільними ознаками і визначеними критеріями за багатьма класами ознак та прийнятті рішення щодо віднесення worm-вірусу до певного класу частково централізованою розподіленою системою, що покращило достовірність виявлення, зокрема за рахунок приховування принципів функціонування системи.

Аналіз основного змісту дисертації.

У вступі здійснено обґрунтування актуальності теми, визначено мету, основні завдання, предмет та об'єкт дослідження, методи дослідження, наведено наукову новизну, практичне значення одержаних результатів.

У першому розділі здійснено дослідження предметної області, розподілених систем виявлення ЗПЗ, методів розроблення розподілених систем попередження, виявлення та протидії ЗПЗ, методів виявлення worm-вірусів в корпоративних

мережах, підведення підсумків проведеного аналізу та постановку задачі дослідження.

У другому розділі подано розроблену удосконалену модель частково централізованих розподілених систем виявлення ЗПЗ. Розроблено архітектуру компонент частково централізованих розподілених систем, що базується на отриманих аналітичних виразах. Вони є математичними моделями характеристичних показників значень рівнів безпеки компонентів.

У третьому розділі наведено методи синтезу математичних моделей рівнів безпеки компонентів системи, організації функціонування частково централізованих розподілених систем та виявлення worm-вірусів.

У четвертому розділі подано методику визначення ефективності функціонування розподілених систем, здійснено постановку експериментів і проведення експериментальних досліджень, оцінювання ефективності функціонування системи.

У висновках подано отримані наукові та практичні результати дослідження.

У додатках подано перелік праць здобувача, акти впровадження, фрагмент лістингу програмного коду та таблиці із значеннями, які отримані в результаті проведених експериментів.

**4. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.**

Наукові висновки та рекомендації, подані в дисертації, ґрунтуються на адекватному використанні методів для опису середовища корпоративних мереж та методів синтезу розподілених систем. Успішна реалізація розробленої системи, а також ефективне впровадження результатів дослідження в комерційну діяльність підприємств, що використовують подібні розподілені системи, демонструє відповідність теоретичних результатів реальним результатам їх використання.

**5. Практичне значення отриманих результатів.**

За результатами виконаних досліджень здобувачем розроблено методи та засоби покращення ефективності функціонування розподілених систем виявлення зловмисного програмного забезпечення в комп'ютерних мережах за рахунок синтезу в їх архітектурі принципів часткової централізації, самоорганізації та адаптивності.

Розроблена частково централізована розподілена система виявлення ЗПЗ, зокрема worm-вірусів, має можливість її наповнення різними методами попередження, виявлення та протидії ЗПЗ та КА, а також забезпечує належну стійкість та стабільність при функціонуванні в комп'ютерних мережах її компонентів. Розроблена система дає змогу ускладнити її розуміння функціонування зловмисниками. Вона самостійно та гнучко забезпечує переміщення центру між компонентами в процесі функціонування системи, самостійно приймає рішення щодо подальших кроків та не потребує залучення адміністратора. Крім того, реалізований метод виявлення worm-вірусів базується на багатокласовій класифікації об'єктів і результати його застосування для виявлення становлять більше 95% та підтверджують ефективність запропонованого рішення.

У результаті проведених експериментальних досліджень з розробленою системою було підтверджене коректне функціонування частково централізованої розподіленої системи, можливість застосування її до виявлення worm-вірусів, а також належні рівні стійкості та деградації системи.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «ІТТ» (м. Хмельницький), Державному підприємстві «Новатор» (м. Хмельницький), ПП «НОЛТ ТЕХНОЛОДЖИС» (м. Хмельницький), а також, в освітньому процесі Хмельницького національного університету при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для спеціальностей 123 Комп'ютерна інженерія, 126 Інформаційні системи та технології, зокрема в курсах «Теорія і проєктування комп'ютерних та кіберфізичних систем і мереж», «Теорія і технології проєктування спеціалізованих операційних систем», «Методи розв'язування наукових задач комп'ютерної інженерії» та «Технології та методи забезпечення надійності та безпеки інформаційних систем та технологій».

**6. Особистий внесок здобувача** полягає в розробленні методів синтезу частково централізованих розподілених систем на основі принципів самоорганізації та адаптивності. Усі основні наукові та прикладні результати дисертаційної роботи отримані здобувачем самостійно. За результатами проведених досліджень основні наукові результати опубліковано у 3 наукових статтях у фахових наукових журналах України, одна з яких в журналі категорії А, та одній науковій статті в міжнародному науковому журналі, який проіндексовано в наукометричній базі Scopus. Апробація засвідчена публікаціями 6 праць в матеріалах міжнародних та всеукраїнських конференцій, з яких одна праця індексована у наукометричній базі Scopus. Опубліковано 1 свідоцтво про реєстрацію авторського права на твір (програму). У роботах, що опубліковані в співавторстві, здобувачеві належать: удосконалена модель частково централізованих розподілених систем; математичні моделі характеристичних показників значень рівнів безпеки компонентів; метод організації функціонування частково централізованих розподілених систем..

**7. Структура та обсяг дисертації.**

Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та шести додатків. Повний обсяг роботи містить 245 сторінок друкованого тексту, з них анотація – на 12 стор., зміст – на 2 стор., перелік умовних скорочень – на 1 стор., основний текст – на 162 стор., список зі 121 використаних джерел – на 13 стор., додатки – на 53 стор. Дисертація містить 15 рисунків та 85 таблиць.

**8. Зауваження.**

1. Метод синтезу математичних моделей характеристичних показників рівнів безпеки при застосуванні його некваліфікованим адміністратором може призвести до погіршення функціонування системи через потребу задавати ранжування показників в ручному режимі.

2. Метод організації функціонування частково централізованих розподілених систем не враховує різні часові витрати на виконання поставлених завдань в різних за обчислювальними спроможностями комп'ютерними станціями, що може

призвести до затримок в отриманні результатів і, як наслідок, неправильному оцінюванні значень рівнів безпеки в таких вузлах корпоративної мережі.

3. Метод виявлення worm-вірусів базується на використанні отриманих автором аналітичних виразів для обчислення значень характерних показників з різних класів ознак, але при цьому він не порівнюється в цій частині з відомими методами.

4. В дисертації допущено неправильне оформлення авторського свідоцтва на твір в переліках праць на стор. 13 (номер 11), стор. 193 номер 11), та списку використаних джерел на стор. 189 (номер 107):

Савенко Б., Севостьянов В., Матьокін О. А. с. 124480, Україна. Комп'ютерна програма «Проміжне програмне забезпечення частково централізованих розподілених систем виявлення зловмисного програмного забезпечення в комп'ютерних мережах». Дата реєстрації 07.03.2024.

Однак, зазначені зауваження не впливають на загальний рівень проведеного дослідження.

**9. Загальний висновок.**

Отже, дисертаційна робота Савенка Богдана Олеговича за темою «Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах» є завершеною науковою кваліфікаційною працею, яка містить новий та актуальний науково-прикладний внесок. Усі результати, які виносяться на захист, є достовірними та отримані автором особисто.

Тому, з огляду на вище вказане, вважаю, що дисертаційна робота «Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах», яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам пп. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а її автор, Савенко Богдан Олегович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Рецензент:
к.т.н., доцент,
завідувач кафедри кібербезпеки
Хмельницького національного університету Юрій КЛЬОЦ

«Підпис Юрія КЛЬОЦА засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету Олег СИНЮК