Голові разової спеціалізованої
вченої ради ДФ 70.052.036
Хмельницького національного
університету
докторці технічних наук, професорці
Тетяні ГОВОРУЩЕНКО

РЕЦЕНЗІЯ
на дисертаційне дослідження Савенка Богдана Олеговича
на тему «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

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

Тривале активне поширення зловмисного програмного забезпечення (ЗПЗ) в комп'ютерних мережах створює проблеми користувачам. Для протидії його розроблено різні засоби та системи. Їх правильне конфігурування та використання забезпечують відносно належний рівень безпеки. Але зловмисники вивчають особливості таких систем та використовують їх для удосконалення проведення своїх атак, зокрема і з використанням цілеспрямованого ЗПЗ. Тому, потребують розроблення системи протидії ЗПЗ та КА не тільки в частині методів протидії, виявлення, попередження, але й в частині методі організації функціонування таких систем в комп'ютерних мережах.

Перспективним напрямом дослідження є розроблення нової архітектури систем або удосконалення наявної з метою покращення їх функціонування в частині ускладнення розуміння зловмисниками їх поведінки. Крім того, досягнення покращення функціонування таких систем найкраще може бути забезпечено саме в корпоративних мережах, оскільки на них накладені певні обмеження, внутрішня організація відома власникам мереж, а також до протидії КА та ЗПЗ можуть бути всі наявні комп'ютерні станції, що суттєво збільшує можливості захисту.

Для забезпечення ускладнення розуміння зловмисниками поведінки систем попередження, виявлення та протидії ЗПЗ і КА в архітектурі таких систем потрібно синтезувати принципи самоорганізації, адаптивності та централізації. Самоорганізація дасть змогу забезпечити прийняття рішень системою щодо подальших кроків без втручань адміністратора, що є актуальним в контексті доброчесності адміністратора. Адаптивність дасть змогу забезпечити гнучку перебудову системи на рівні її архітектури. Це є важливим для розподілених систем, бо частина компонентів може бути вимкненою або буде вмикатись і вимикатись в процесі експлуатації. Розроблення організації централізації є не менш важливою. Оскільки зловмисники як правило здійснюють пошук центру системи в корпоративних мережах, тому його задання в архітектурі системи

повинно бути таким, щоб унеможливити його виявлення. В дисертації автором запропоновано розподілити центр між частиною компонент системи, здійснювати його переміщення між частиною компонент, приймати рішення активними компонентами центру згідно принципу децентралізації. Тобто, в дисертації реалізовано принцип часткової централізації.

Таким чином, в результаті аналізу актуальності тематики проведеного дослідження встановлено, що покращення ефективності функціонування розподілених систем виявлення ЗПЗ в комп'ютерних мережах за рахунок синтезу в їх архітектурі принципів часткової централізації, самоорганізації та адаптивності є актуальною науково-прикладною задачею.

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.

Формулювання наукової задачі, мети й задач дослідження. Сучасний стан розвитку розподілених систем та комп'ютерних мереж дає змогу пропонувати методи синтезу частково централізованих розподілених систем.

Здобувачем правильно визначено об'єкт і предмет дослідження, відповідно до висунутої заздалегідь гіпотези дослідження. Так, об'єктом дослідження визначено процес синтезу частково централізованих розподілених систем виявлення ЗПЗ. Предметом дослідження є 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.

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.

Короткий аналіз основного змісту дисертації.

У вступі автором обґрунтовано актуальність теми, визначено мету, основні завдання, предмет та об'єкт дослідження, наведено наукову новизну, практичне значення одержаних результатів.

У першому розділі проаналізовано предметну область, існуючі розподілені системи виявлення ЗПЗ, відомі методи розроблення розподілених систем попередження, виявлення та протидії ЗПЗ, методи виявлення worm-вірусів в корпоративних мережах. Також, підведено підсумки проведеного аналізу та здійснено постановку задачі дослідження.

У другому розділі подано розроблення удосконаленої моделі частково централізованих розподілених систем. 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 запропонований метод синтезу математичних моделей рівнів безпеки компонентів системи, метод організації функціонування частково централізованих розподілених систем та метод виявлення worm-вірусів.

У четвертому розділі автором запропоновано методику визначення ефективності функціонування розподілених систем. Також, здійснено постановку і проведення експериментальних досліджень, оцінювання ефективності функціонування системи.

У висновках подано отримані наукові та практичні результати дослідження.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій. Наукові висновки та рекомендації, наведені в дисертації, ґрунтуються на адекватному та цілеспрямованому використанні математичних методів та алгоритмів для синтезу частково централізованих розподілених систем виявлення ЗПЗ. Успішна реалізація розробленої системи, а також ефективне впровадження результатів дослідження в комерційну діяльність підприємств, що використовують подібні системи, демонструє відповідність отриманих теоретичних результатів реальним результатам їхнього використання.

Практичне значення одержаних результатів. Розроблена частково централізована розподілена система виявлення ЗПЗ, зокрема worm-вірусів, має функціональність для 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. Тобто розроблена система є платформою, яку можна наповнювати різними методами попередження, виявлення та протидії ЗПЗ і КА. Особливістю розробленої частково централізованої розподіленої системи є складність в розумінні її функціонування зловмисниками, самостійне та гнучке забезпечення переміщення центру між компонентами в процесі функціонування системи, самостійне прийняття рішення щодо подальших кроків та не потребують при цьому 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».

Особистий внесок здобувача полягає в розробленні методів синтезу частково централізованих розподілених систем виявлення ЗПЗ та КА, що забезпечують розв'язання поставлених у дисертації задач. Усі основні наукові та прикладні результати дисертаційної роботи отримані здобувачем самостійно. За результатами проведених досліджень основні наукові результати опубліковано у 4 наукових статтях у фахових наукових журналах України та міжнародному науковому журналі, дві з яких проіндексовано в наукометричній базі Scopus. Апробація засвідчена публікаціями 6 праць в матеріалах міжнародних та всеукраїнських конференцій, з яких одна праця проіндексована у наукометричній базі Scopus. Опубліковано 1 свідоцтво про реєстрацію авторського права на твір (програму). У роботі, що опубліковані в співавторстві, здобувачеві належать основні ідеї, теоретична та практична розробка положень, відображених у характеристиці наукової новизни отриманих результатів, а саме: розроблена удосконалена модель частково централізованих розподілених систем та математичні моделі характеристичних показників значень рівнів безпеки компонентів; розроблено метод організації функціонування частково централізованих розподілених систем.

Апробація матеріалів дисертації. Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем у Хмельницькому національному університеті. Наукові результати роботи доповідалися на таких конференціях: 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS, IEEE), Dortmund, Germany, 2023; XIV всеукраїнської науково-практичній конференції «Актуальні проблеми комп'ютерних наук АПКН-2022» – Хмельницький: ХНУ, 18-19 листопада, 2022; International Conference on Innovative Solutions in Software Engineering. – Ivano-Frankivsk, Ukraine, November 29-30, 2022; XX міжнародній науково-практичній конференції «Математичне та програмне забезпечення інтелектуальних систем», м. Дніпро, 23-25 лист. 2022; Всеукраїнській науково-практичній конференції молодих вчених, аспірантів і студентів «Інформаційні технології та інженерія», м. Миколаїв, 7–10 лютого 2023; XII Міжнародній

науково-технічній конференції «Безпека інформаційних технологій (ITSec)», м. Ужгород, 2-4 травня 2023.

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 із 121 використаних джерел – на 13 стор., додатки – на 53 стор. Дисертація містить 15 рисунків та 85 таблиць.

Зауваження. У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. Для частково централізованих розподілених систем характерною особливістю є наявність великої кількості зв'язків. Це може суттєво ускладнити функціонування таких систем. В дисертації здійснено порівняння частково централізованої архітектури з централізованою та децентралізованою і показано розрахунки ефективності в частині функціонування. Але недостатньо обґрунтовано та промодельовано саме функціонування для великої кількості компонент системи.

2. В методі організації функціонування частково централізованих розподілених систем недостатньо обґрунтовано часові затримки в передачі та отримані повідомлень для формування системи з компонент або змін в середовищі, що може вплинути на показники стійкості та деградації.

3. При здійсненні формалізованого опису середовища корпоративної мережі аналітичними виразами досить багато рішень щодо значущості показників приймають експерти, що може вплинути на ефективність функціонування систем.

4. В методі виявлення worm-вірусів недостатньо деталізовано і проілюстровано прикладами обчислення суми значень характерних показників з різних класів ознак.

5. У дисертаційній роботі зустрічаються деякі граматичні та стилістичні помилки, зокрема, на ст.71 «…формули (2.19)…»- потрібно «…формула (2.19)…».

6. В переліках праць та списку використаних джерел на стор. 13 (п. 11), стор. 193 (п. 11), стор. 189 (п. 107) в дисертації неправильно оформлено подання авторського свідоцтва: 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.

Втім, зазначені зауваження суттєво не впливають на загальний, доволі високий, рівень проведеного дослідження.

Загальний висновок. Вважаю, що дисертаційна робота Савенка Богдана Олеговича за темою «Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах» містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі 12 Інформаційні технології, які в сукупності забезпечують розв'язання актуальної науково-прикладної задачі розроблення методів для покращення ефективності функціонування розподілених систем з частковою централізацією,

самоорганізацією та адаптивністю для виявлення ЗПЗ та КА в комп'ютерних мережах та виявлення ЗПЗ з їх використанням за рахунок синтезу архітектури таким чином, щоб принципи функціонування таких систем ускладнювали зловмисникам їх розуміння.

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:
д.т.н., професор, завідувач кафедри
комп'ютерних наук
Хмельницького національного університету Олександр БАРМАК

«Підпис Олександра БАРМАКА засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету Олег СИНЮК