Голові разової спеціалізованої
вченої ради ДФ 70.052.036
Хмельницького національного
університету
доктору технічних наук, професору
Тетяні ГОВОРУЩЕНКО
29016, м. Хмельницький,
вул. Інститутська, 11

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА
доктора технічних наук, професора Мухіна Вадима Євгенійовича
на дисертаційну роботу **Савенка Богдана Олеговича**
«Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах»,
подану до захисту на здобуття наукового ступеня **доктора філософії**
з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

1. Актуальність теми дисертаційної роботи.

Розвиток комп'ютерних мереж та подальше широке залучення комп'ютерних систем в різні сфери людської діяльності створюють можливості для активної діяльності зловмисників. Вони продовжують активно здійснювати комп'ютерні атаки (КА) та поширення зловмисного програмного забезпечення (ЗПЗ). Зловмисники вивчають сучасні системи попередження, виявлення та протидії ЗПЗ і КА для здійснення зловмисних дій. Особливо актуальними напрямами для них є корпоративні мережі. Тому, розробникам систем попередження, виявлення та протидії ЗПЗ і КА потрібно постійно їх вдосконалювати та покращувати ефективність їх функціонування. Зокрема, особливе місце в цьому процесі вдосконалення займають саме системи як платформи, що наповнюються різними спеціалізованими методами. Використання універсальних систем є недоцільним через специфіку їх подальшого застосування. В зв'язку з цим потребує постійного вдосконалення архітектура таких систем.

Важливим напрямом в розвитку архітектури систем попередження, виявлення та протидії ЗПЗ і КА для їх подальшого застосування в корпоративних мережах є приховування від зловмисників центру прийняття рішень. Така дія суттєво ускладнює здійснення зловмисних дій. Крім того, актуальним для таких систем є забезпечення їх спроможності до прийняття самостійних рішень щодо наступних кроків та до гнучкої перебудови їх архітектури в залежності від подій в корпоративній мережі. Все це в сукупності уможливлює синтез систем з такою архітектурою, в якій

поєднуються властивості централізації, самоорганізації та адаптивності. Таке поєднання повинно ускладнити зловмисникам розуміння принципів та особливостей функціонування систем, знаходження їх центру, рішення щодо наступних кроків та рішення про гнучку перебудову архітектури. Крім того, в частині принципу централізації на сьогодні недостатньо дослідженою є архітектура систем з частковою централізацією. Розвиток цього напряму в дослідженнях є актуальним особливо для систем, які створюються з метою приховуванням їх особливостей та розуміння їх функціонування зловмисниками.

Отже, актуальною науковою задачею є розроблення методів для покращення ефективності функціонування систем для виявлення ЗПЗ та КА в корпоративних мережах на основі поєднання принципів часткової централізації, самоорганізації та адаптивності та виявлення ЗПЗ з їх використанням за рахунок синтезу архітектури таким чином, щоб принципи функціонування таких систем ускладнювали зловмисникам їх розуміння.

2. Зв’язок роботи з науковими програмами, планами, темами.

Дослідження, результати якого викладено в дисертації, виконано в рамках науково-дослідної тематики Хмельницького національного університету, а саме, 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» (№ держреєстрації 0124U000980), в яких автор дисертації був виконавцем.

3. Наукова новизна отриманих результатів.

До основних наукових результатів дисертаційної роботи варто віднести:

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 центру 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.

4. Короткий аналіз основного змісту дисертації.

Науковий рівень викладення дисертації відповідає вимогам МОН України. Назва дисертації адекватно та повною мірою відображає її зміст.

У *вступі* обґрунтовано актуальність теми дисертації, визначено мету та основні завдання, предмет та об'єкт дослідження, відображено наукову новизну і практичне значення одержаних результатів.

У *першому розділі* здійснено аналіз предметної області дослідження, існуючих комерційних і дослідницьких розподілених систем, відомих методів та характерних особливостей розробки розподілених систем попередження, виявлення та протидії ЗПЗ, методи виявлення worm-вірусів в корпоративних мережах. У розділі підведено підсумки проведеного аналізу та здійснено постановку задачі дослідження.

У *другому розділі* представлено удосконалену модель частково централізованих розподілених систем. Вона стала основою формування таких систем, які створюють проблеми зловмисникам щодо визначення ними центру та принципів функціонування. Розроблено архітектуру компонент частково централізованих розподілених систем, що базується на отриманих аналітичних виразах. Вони є математичними моделями характеристичних показників значень рівнів безпеки компонентів та формалізують архітектуру компонент системи згідно наявних в них функцій, їх призначення, взаємодії, місця виконання, формування центру прийняття рішень та оцінювання рівня безпеки виконуваних обчислень.

У *третьому розділі* представлено розроблений метод синтезу математичних моделей рівнів безпеки компонентів системи, який дає змогу отримувати нові аналітичні вирази комплексного опису об'єктів та процесів. Він може бути застосований для дискретних та неперервних величин характеристичних показників. Отримані значення характеристичних показників рівнів безпеки в компонентах системи використовуватимуться для оцінювання результатів розподілених обчислень, які отримані з різних компонентів системи. Представлено розроблений метод організації функціонування частково централізованих розподілених систем. Він дає змогу створювати розподілені системи згідно поєднання принципів часткової

централізації, самоорганізації та адаптивності. З метою дослідження ефективності функціонування таких систем було розроблено метод виявлення worm-вірусів. Він базується на поділі worm-вірусів згідно характерних ознак за багатокласовою класифікацією.

У *четвертому розділі* подано методику для обчислення ефективності функціонування розподілених систем, в яких синтезовано поєднані принципи часткової централізації, самоорганізації та адаптивності, постановку і проведення експериментальних досліджень, оцінювання ефективності функціонування системи, а також підведено підсумки щодо проведеного дослідження згідно отриманих результатів.

У *висновках* подано отримані наукові та практичні результати дослідження.

5. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, їх достовірність.

Сформульовані у дисертації наукові положення, висновки та рекомендації є аргументованими і підкріплені успішною реалізацією.

Обґрунтованість наукових положень та висновків дисертації ґрунтується на детальному аналізі джерел, чіткій постановці задачі дослідження і використанні сучасних методів дослідження.

Достовірність результатів дисертації підтверджується їх апробацією на міжнародних і всеукраїнських наукових конференціях, а також їх впровадженням.

6. Практичні результати роботи.

В дисертації розроблена система виявлення worm-вірусів. В її основі синтезовано принципи часткової централізації, розподілення, самоорганізації та адаптивності. Вона може наповнюватись різними методами попередження, виявлення та протидії ЗПЗ та КА, тобто може бути платформою для різних дослідників в цій предметній області. Її дослідження показало належну стійкість та стабільність її компонентів при функціонуванні в комп’ютерних мережах. Розроблена частково централізована розподілена система забезпечує складність в розумінні її функціонування зловмисниками, самостійне та гнучке переміщення центру між компонентами в процесі функціонування системи, самостійне прийняття рішення щодо подальших кроків та не потребує при цьому залучення адміністратора. Реалізований метод виявлення worm-вірусів базується на багатокласовій класифікації об’єктів. Результати його застосування для виявлення worm-вірусів становлять більше 95%, що підтверджує ефективність функціонування таких систем.

У результаті проведених експериментальних досліджень було підтверджене коректне функціонування частково централізованої розподіленої системи в корпоративних мережах, 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.

7. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладу наукових положень та результатів в опублікованих працях.

Дисертаційна робота має логічну структуру і складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та шести додатків. Повний обсяг роботи становить 245 сторінки друкованого тексту, поміж яких, основний текст – на 162 сторінках, список використаних джерел зі 121 найменувань – на 13 сторінках та шість додатків – на 53 сторінках. Дисертація містить 15 рисунків та 85 таблиць. Оформлення дисертації відповідає необхідним вимогам.

У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

За результатами досліджень опубліковано 4 статті у наукових фахових виданнях, з яких дві статті в наукових журналах, проіндексованих в наукометричній базі Scopus, одне свідоцтво про реєстрацію авторського права на твір (програму), 6 тез доповідей у збірниках матеріалів конференцій, з яких 1 праця індексована в наукометричній базі Scopus.

Усі сформовані наукові положення і результати дисертації повністю викладено в опублікованих працях.

8. Мова та стиль дисертаційної роботи.

Текст дисертаційної роботи викладено в логічній послідовності. Матеріал дисертації достатньо проілюстрований схемами, рисунками, графіками й таблицями. Мова і стиль викладення змісту, оформлення дисертації відповідають вимогам до наукових праць.

9. Зауваження та дискусійні положення щодо змісту дисертації.

Зауваження та рекомендації до дисертації:

1. Використання багатьох варіантів зв'язків вимагає значних обчислювальних ресурсів для обробки та аналізу інформації про події в системі. Збільшена складність системи дещо ускладнює процес масштабування, особливо у випадку збільшення кількості компонент та зв'язків. Також, запровадження багатьох варіантів зв'язків збільшує ризики вразливості системи перед атаками зловмисників.

2. Визначення значень характеристичних показників та їх ваги (кроки методу: 1, 2, 6) ґрунтується, здебільшого, на суб'єктивному досвіді експертів, що може призвести до неоднорідності або неповності оцінки рівня безпеки. Кореляція може ускладнити моделювання та аналіз, особливо якщо вона не є лінійною або прямо визначена. Також, наявна певна обмеженість у визначенні вагових коефіцієнтів, (наприклад, ρw) які можуть бути довільно визначені, що впливає на результати моделювання.

3. Метод формування системи з компонент передбачає адаптивність, але він може бути недостатньо гнучким у вирішенні деяких непередбачених сценаріїв або змін в середовищі, зокрема, з врахуванням наявності багатьох факторів в процесі обміну повідомленнями та динамічної зміни системи може виникнути проблема забезпечення безпеки даних та відновлення системи в разі виникнення інцидентів.

4. Досить багато кроків в методі формування системи з компонент вимагають участі адміністратора системи, що призводить до збільшення витрат на управління та зниження ефективності системи у випадку недоступності, зокрема тимчасової, адміністратора системи. Такий відносно складний процес формування та зміни системи може призвести до збільшення ймовірності виникнення помилок, а їх виявлення та виправлення цих помилок може бути складним завданням через велику кількість можливих сценаріїв та взаємодій компонентів.

5. Використання випадкового вибору чисел для прийняття рішень щодо кількості та активності компонент центру прийняття рішень може призвести до неочікуваних результатів та погіршання якості рішень. Система може стати неефективною при збільшенні обсягів даних та кількості компонент, оскільки зростає складність процесу вибору активних компонент.

6. Успішність методу виявлення worm-вірусів значною мірою залежить від точності та ефективності сенсорів, які збирають інформацію про спроби завантаження файлів та функціонування процесів. Низька якість сенсорів може призвести до недооцінки або пропуску потенційно небезпечних процесів. Використання аналітичних виразів та шаблонів атак може призвести до помилкових спрацювань, коли невідомі або нові віруси можуть не відповідати наявним сигнатурам чи шаблонам.

7. У дисертаційній роботі зустрічаються деякі граматичні та орфографічні помилки, зокрема, на с. 108…

стилістичні та узгодження по тексту ст.71 «…формули (2.19)…»- потрібно «…формула (2.19)…»

Крім того, в дисертації неправильно оформлено джерело (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) в переліках праць та списку використаних джерел на стор. 13 (позиція 11), стор. 189 (позиція 107), стор. 193 (позиція 11).

Зазначені зауваження істотно не впливають на зміст дисертаційної роботи та не знижують її наукову новизну та практичну цінність.

Висновки щодо дисертації в цілому

На основі викладеного вище вважаю, що дисертація Савенка Богдана Олеговича на тему «Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп’ютерних мережах», що 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 йому наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент – доктор технічних наук, професор,
завідувач кафедри системного проектування,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Вадим МУХІН

Підпис завідувача кафедри системно проектування,
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
д.т.н., професора Мухіна В.Є.

засвідчую:

Вчений секретар
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Валерія ХОЛЯВКО

8 травня 2024 р.