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 Поночовного Юрія Леонідовича
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.

Системи протидії зловмисному програмному забезпеченню (ЗПЗ) та комп'ютерним атакам (КА) в корпоративних мережах потребують постійного вдосконалення. Одним з напрямків такого вдосконалення є проєктування та впровадження систем, які були б складними для розуміння зловмисників, а також могли б самостійно приймати рішення щодо своїх подальших дій. Універсальних систем такого напрямку для їх наповнення методами виявлення ЗПЗ немає, оскільки їх область застосування є специфічною. Зловмисники можуть і будуть вивчати поведінку таких систем. Тому перспективним напрямком дослідження залишається синтез розподілених систем виявлення ЗПЗ і КА.

Для ускладнення розуміння зловмисниками поведінки систем в корпоративних мережах потрібно забезпечувати їх функціонал таким чином, щоб вони могли гнучко перебудовувати архітектуру, самостійно приймати рішення щодо подальших кроків при зміні навколишнього середовища та організовувати функціонування центру системи за різними стратегіями. Все це може бути досягнуто комбінуванням принципів часткової централізації, самоорганізації та адаптивності в архітектурі розподілених систем.

Дослідження в цій області проводяться постійно і активно, оскільки зловмисники постійно збільшують свої ресурси для здійснення КА та поширення ЗПЗ. Методи протидії, виявлення КА та ЗПЗ можуть забезпечити надійний результат при поєднанні їх з архітектурою розподілених та частково децентралізованих систем, і це поєднання може підвищити ефективність виявлення та протидії ЗПЗ та КА.

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

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

Дисертаційна робота виконувалась 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.

3. Наукова новизна результатів дисертаційної роботи.

Наукова новизна одержаних результатів полягає в наступному:

Вперше розроблено:

1) 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;

2) 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;

3) 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.

Удосконалено:

4) 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 з нею 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;

4. Короткий аналіз основного змісту дисертації.

У вступі представлено обґрунтування актуальності розв'язуваної наукової задачі. Її суть полягає у покращенні ефективності виявлення ЗПЗ і КА розподіленими системами в корпоративних мережах. За перспективний напрям для досліджень визначено синтез розподілені системи згідно з принципами

часткової централізації, самоорганізації та адаптивності. Проаналізовано актуальні дослідження вітчизняних та закордонних вчених, які займаються проблематикою в частині розподілених систем та виявлення ЗПЗ і КА та протидії їм.

У першому розділі проведено аналіз комерційних і безкоштовних систем досліджуваного спрямування, методів розробки розподілених систем попередження, виявлення та протидії ЗПЗ, методи виявлення worm-вірусів в корпоративних мережах. Також виконано підсумки проведеного аналізу з виділенням проблемних завдань та здійснено постановку задачі дослідження.

У другому розділі представлено удосконалену модель частково централізованих розподілених систем, яка є основою їх формування. Системи створені на основі запропонованої моделі повинні бути такими, що ускладнюють їх розуміння зловмисниками. До проблем для зловмисників віднесено такі: визначення центру системи; розуміння принципів функціонування. Архітектуру системи деталізовано до рівня компонент. Для кожної компоненти системи розроблено аналітичні вирази, які описують функціональний склад компоненти та її участь у групі частково децентралізованого управління. Ці вирази дають змогу визначити рівні безпеки компонентів і є математичними моделями характеристичних показників. Значення характеристичних показників рівнів безпеки компонентів систем потрібні для формування рішень щодо її подальших змін та визначення ЗПЗ.

У третьому розділі представлено метод синтезу математичних моделей рівнів безпеки компонентів системи. Згідно з ним отримуються нові аналітичні вирази комплексного опису об'єктів та процесів, які будуть відбуватись в частково централізованих розподілених системах. Вони враховуватимуться при оцінюванні безпеки компонент системи. Особливістю розробленого методу синтезу є можливість застосування до дискретних та неперервних величин характеристичних показників. Також, представлено метод організації функціонування частково централізованих розподілених систем, згідно з яким можна створювати такі системи. Для забезпечення функціонування такого типу систем проведено розподіл компонент за відношенням до центру прийняття рішень. Це дало змогу реалізувати часткову централізацію сумісно з принципами самоорганізації та адаптивності. Для дослідження ефективності функціонування систем було розроблено метод виявлення worm-вірусів та імплементовано його в розподілену систему з частковою децентралізацією управління.

У четвертому розділі розроблено методику для визначення ефективності функціонування розподілених систем і застосовано її до систем з частковою централізацією, самоорганізацією та адаптивністю. Також здійснено постановку і проведення експериментальних досліджень із застосуванням розробленої частково централізованої розподіленої системи.

У висновках представлено отримані наукові та практичні результати роботи.

У додатках подано наукові публікації, які відображають наукові результати роботи, акти впровадження результатів роботи, фрагмент лістингу програмного забезпечення, таблиці з результатами експериментів.

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

Наукові положення, висновки і рекомендації дисертації обґрунтовані коректним та доцільним використанням математичного апарату, успішною реалізацією розробленої розподіленої системи, ефективним практичним впровадженням результатів дисертаційного дослідження на підприємствах, що використовують такі системи. Це продемонструвало відповідність теоретичних досліджень з реальними результатами застосування.

Обґрунтованість наукових положень та висновків, сформульованих у дисертаційній роботі, є достатньою і ґрунтується на детальному аналізі джерел за даною проблемою, чіткій постановці мети і задач дослідження, використанні сучасних методів дослідження, а також проявляється у якісному та аргументованому формулюванні висновків.

Достовірність та обґрунтованість запропонованих методів і засобів підтверджується результатами експериментальних досліджень та коректним застосуванням методів, які були використані під час виконання роботи.

6. Практичні результати роботи.

Практичне значення роботи полягає у впровадженні запропонованих моделей і методів у розроблену частково централізовану розподілену систему виявлення worm-вірусів. Вона має можливість наповнення різними методами попередження, виявлення та протидії ЗПЗ та КА, а також забезпечує належну стійкість та стабільність її компонентів при функціонуванні в комп'ютерних мережах. Особливістю розробленої частково централізованої розподіленої системи є складність в розумінні її функціонування зловмисниками, а також самостійне та гнучке забезпечення переміщення центру між компонентами в процесі функціонування системи, самостійне прийняття рішення щодо подальших змін, які не потребують при цьому залучення адміністратора. Реалізований метод виявлення worm-вірусів базується на багатокласовій класифікації об'єктів і результати його застосування для виявлення становлять понад 95% та підтверджують ефективність запропонованого рішення.

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».

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

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 ст., зміст – на 2 ст., перелік умовних скорочень – на 1 ст., основний текст – на 162 ст., список зі 121 використаного джерела – на 13 ст., додатки – на 53 ст. Дисертація містить 15 рисунків та 85 таблиць.

Дисертаційна робота має логічну структуру. Основні висновки й рекомендації логічно слідують із результатів, які наведено в розділах роботи.

Отримані результати свідчать про індивідуальність роботи. По всьому тексту дисертації простежується авторський стиль. У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

За результатами проведених досліджень опубліковано 10 наукових праць, з яких основні наукові результати опубліковано у 4 наукових статтях у трьох фахових наукових журналах України та міжнародному науковому журналі, дві з яких в наукових журналах, проіндексованих в наукометричній базі Scopus. Апробація засвідчена публікаціями 6 праць у матеріалах міжнародних та всеукраїнських конференцій, з яких одна праця проіндексована в наукометричній базі Scopus. Опубліковано 1 свідоцтво про реєстрацію авторського права на твір (програму).

Основі положення дисертації повністю викладено в опублікованих працях. Вимоги щодо кількості та якості публікацій виконано.

8. Мова та стиль дисертаційної роботи.

Текст дисертаційної роботи викладений чітко та в логічній послідовності. Матеріал дисертації достатньо проілюстрований схемами, рисунками, графіками й таблицями. Загальні висновки та рекомендації у дисертації випливають з проведених здобувачем досліджень та відображають основні результати роботи. Мова і стиль викладення змісту, оформлення дисертації відповідають вимогам, які ставляться до наукових праць.

Тема, зміст та отримані наукові результати роботи відповідають предметній області спеціальності 123 Комп'ютерна інженерія галузі знань 12 Інформаційні технології.

9. Зауваження та дискусійні положення щодо змісту дисертації.

До зауважень та недоліків дисертації варто віднести наступне:

1. Частина характеристичних показників для опису оточуючого середовища корпоративної мережі встановлюється адміністратором або експертом, що може впливати на результат функціонування системи.

2. Процес формування та гнучкої зміни архітектури розподіленої системи при великій кількості компонент може призвести до деградації та втрати стабільності системи.

3. Недостатньо досліджено зростання складності при виборі активних компонент в процесі тривалого функціонуванні системи.

4. Недостатньо деталізовано метод виявлення worm-вірусів в частині використання аналітичних виразів для їх ідентифікації за багатокласовою класифікацією.

5. Не зрозуміло використання посилань на літературні джерела у переліку умовних скорочень, також використання скорочення АЗ як «антивірусні засоби» важко сприймається для галузі 12 (як правило, АЗ – це «апаратні засоби, апаратне забезпечення».

6. Для запропонованих методів було б доречно навести блок-схеми їх етапів, зокрема для кроків методу організації функціонування частково централізованих розподілених систем (п.3.3.2, с. 130).

7. Для систем з частковою децентралізацією (с. 168) бажано використовувати показник, обернений (як $1–E_{11}$) до запропонованого E_{11}.

8. При оформленні додатків слід також підтримувати науковий послідовний стиль розкриття отриманих результатів. Так, табл. Г.1 містить два поля(стовпця), позначених як E_{11} з різними значеннями, таблиці додатку Д взагалі не мають назв стовпчиків, у додатку Е не зрозуміло, чи є кореляція між парами таблиць «результати серії…» та «значення рівнів безпеки…» за виділеними заливкою значеннями чарунок.

9. У дисертаційній роботі зустрічаються деякі граматичні та орфографічні помилки, зокрема, на с. 60 вказано, що (2.11) – «бітова карта активних функцій», але у (2.11) використано не двійкове, а трійкове представлення; у додатку В фрагменти коду мають різне текстове форматування; номери держреєстрації науково-дослідних робіт заповнені за різними шаблонами у вступі; на с.71 посилання на формулу (2.19) перед формулою (2.20) не логічне.

10. В дисертації 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 (ст. 13 і ст. 193 (позиція 11)) і списку використаних джерел (ст. 189 (позиція 107)) неправильно оформлено та подано.

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

10. Загальні висновки щодо дисертації

Представлена дисертаційна робота «Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах» є завершеною науково-дослідною роботою, яка містить нові науково обґрунтовані результати.

У дисертації розв'язано актуальну науково-прикладну задачу покращення ефективності функціонування розподілених систем виявлення ЗПЗ в комп'ютерних мережах за рахунок синтезу в їх архітектурі принципів часткової централізації, самоорганізації та адаптивності.

Одержані наукові та практичні результати є значущими для галузі 12 Інформаційні технології загалом та спеціальності 123 Комп'ютерна інженерія зокрема. Тема і зміст дисертації повністю відповідають спеціальності 123 Комп'ютерна інженерія.

Отже, з огляду на актуальність теми дисертації, обґрунтованість наукових положень, висновків та рекомендацій, сформульованих у дисертації, їх новизну та практичну цінність, повноту викладу в наукових публікаціях, відсутність порушень академічної доброчесності, вважаю, що дисертація цілком 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,
професор кафедри інформаційних систем та технологій,
Полтавський державний аграрний університет,

Юрій ПОНОЧОВНИЙ

Підпис професора кафедри інформаційних систем та технологій Полтавського державного аграрного університету, д.т.н., професора Поноочовного Ю.Л..

засвідчую:

ЗАВІРЯЮ
Заступник начальника відділу кадрів
Полтавського державного аграрного
університету
Олена ПІХУЛЯ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ Ідентифікаційний код 00493014