ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації

на тему «Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах»
(назва роботи)

здобувача наукового ступеня доктора філософії

Савенко Богдан Олегович
(прізвище, ім'я, по батькові)

з галузі знань 12 Інформаційні технології
(шифр, назва галузі знань)

за спеціальністю 123 Комп'ютерна інженерія.
(шифр, назва спеціальності)

Публічна презентація проведена на кафедрі комп'ютерної інженерії та інформаційних систем
(назва)

«23» березня 2024 року, протокол № 11.

1. Актуальність теми дослідження.

Розповсюдження зловмисного програмного забезпечення (ЗПЗ) відбувається постійно та зростає. Сучасні засоби та системи попередження, виявлення та протидії ЗПЗ і комп'ютерним атакам (КА) є досить ефективними, забезпечують великий відсоток виявлення та функціонують на належному рівні. Але зловмисники постійно вивчають спроможності таких засобів та систем, вдосконалюють ЗПЗ та здійснення КА і досягають певних результатів. Тому, розробники засобів та систем попередження, виявлення та протидії ЗПЗ та КА повинні постійно їх вдосконалювати. Особливо актуальним є захист корпоративних мереж, які в сукупності є типовим класом об'єктів, до якого можуть бути застосовані ефективні типові рішення. Цей клас об'єктів порівняно з одиничними комп'ютерними станціями може бути ефективно конфігурований для збільшення обчислювальних ресурсів при вирішенні завдань попередження, виявлення та протидії ЗПЗ та КА для захисту корпоративних мереж.

Крім нових чи удосконалення відомих методів попередження, виявлення та протидії ЗПЗ та КА, важливим та перспективним напрямом залишається напрям з дослідження, удосконалення чи створення принципово нової архітектури засобів та систем попередження, виявлення та протидії ЗПЗ та КА. Така архітектура повинна включати можливості систем до інтеграції в неї методів виявлення і результатом такого поєднання повинна бути система, в якій наявний центр для прийняття рішень, методи виявлення та підсистема залучення обчислювальних ресурсів комп'ютерних станцій, з яких її сформовано. Також, така архітектура повинна бути основою для розроблення систем, які будуть важко зрозумілими та прогнозованими щодо функціонування для зловмисників, бо зловмисники можуть бути присутніми і в межах периметру захисту корпоративної мережі. В цьому контексті важливою вимогою до системи є її спроможність приймати рішення без втручання користувача. Все це в сукупності вимагає синтезувати в архітектурі таких систем ефективний центр прийняття рішень, який міг би,

також, переміщуватись в залежності від зміни стану в корпоративній мережі та безпосередньо в системі.

Дослідження та розроблення архітектури розподілених систем попередження, виявлення та протидії ЗПЗ та КА саме зі спрямуванням на особливості та варіанти їх центру прийняття рішень, а також дослідження, відповідно, впливу варіантів архітектури на ефективність та достовірність таких систем, є недостатнім. Крім того, не тільки безпосередньо центр прийняття рішень як цілісна частина системи впливатиме на її функціонування, а саме його архітектура та принцип реалізації є перспективним напрямом для дослідження. Найбільш дослідженими є системи з централізованою та децентралізованою архітектурою в контексті завдань з попередження, виявлення та протидії ЗПЗ та КА. Але на сьогодні недостатньо дослідженою є архітектура розподілених систем з частковою централізацією. Вона актуальна для систем з приховуванням їх особливостей та розуміння їх функціонування зловмисниками.

Тому, актуальною науковою задачею є 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 їх архітектури таким чином, щоб принципи функціонування таких систем ускладнювали зловмисниками їх розуміння.

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

Дисертаційне дослідження виконувалось у 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» (№ держреєстрації 0124U000980), в яких автор дисертації був виконавцем.

3. Наукова новизна отриманих результатів.

У дисертації вперше одержані такі нові наукові результати:

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 неперевними 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. Теоретичне та практичне значення результатів дисертації

Наукові положення, висновки і рекомендації дисертації обґрунтовані коректним та доцільним використанням математичного апарату, зокрема математичні моделі характеристик оточуючого середовища задані розробленими аналітичними виразами для дискретних і неперервних величин, а розроблені методи базуються на математичних моделях характеристик оточуючого середовища, реалізацією розробленої частково централізованої розподіленої системи виявлення ЗПЗ, ефективним практичним впровадженням результатів дисертаційного дослідження на підприємствах, що використовують такі розподілені системи, яке продемонструвало відповідність результатів теоретичних досліджень з реальними результатами застосування.

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. Особливістю розробленої частково централізованої розподіленої системи є складність в розумінні її функціонування зловмисниками, автоматичне та гнучке забезпечення переміщення центру між компонентами в процесі функціонування системи, автоматичне 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 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.

5. Використання результатів роботи

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. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі Савенка Б. О.

Дисертаційна робота виконана на кафедрі комп'ютерної інженерії та інформаційних систем,

(назва кафедри (відділу), назва установи)

науковий керівник д.т.н., професор, професор каф. КІІС Лисенко С. М.

(науковий ступінь, вчене звання, посада, прізвище, ініціали)

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Савенко Б. О.

(прізвище, ініціали здобувача)

є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідне джерело.

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано 11 наукових праць, у тому числі 4 статті у наукових фахових виданнях (з них 2 статті у періодичному науковому фаховому виданні України категорії «А» та виданні, що входить до Scopus), 6 тез доповідей в збірниках матеріалів конференцій.

Наукові праці, в яких опубліковані основні наукові результати дисертації

1. Lysenko S., Savenko B. Distributed Discrete Malware Detection Systems Based on Partial Centralization and Self-Organization. *International Journal of Computing*. 2023. Vol. 22. Pp. 117-139. DOI: https://doi.org/10.47839/ijc.22.2.3082 - *Scopus*

Розроблено модель архітектури частково централізованих розподілених систем та математичні моделі характеристичних показників значень рівнів безпеки компонентів.

2. Kashtalian A., Lysenko S., Savenko B., Sochor T., Kysil T. Principle and method of deception systems synthesizing for malware and computer attacks

detection. *Radioelectronic and Computer Systems.* 2023. Vol. *0*(4). Pp. 112-151. DOI: https://doi.org/10.32620/reks.2023.4.10 - *Scopus*

Розроблено метод організації функціонування частково централізованих розподілених систем.

3. Савенко Б. О. Метод синтезу математичних моделей рівнів безпеки для частково централізованих розподілених систем виявлення зловмисного програмного забезпечення. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки.* 2023. № 3. Ч. 1. С. 217-227. DOI: https://doi.org/10.32782/2663-5941/2023.3.1/34

4. Савенко Б. О. Метод виявлення worm-вірусів згідно багатокласової класифікації. *Вісник Хмельницького національного університету. Серія: Технічні науки.* 2024. № 1 (331). С. 18-28. DOI: https://doi.org/10.31891/2307-5732-2024-331-2

Праці, які засвідчують апробацію матеріалів дисертації

5. Савенко Б. О. Розподілена частково централізована система виявлення зловмисного програмного забезпечення в комп'ютерних мережах. *Актуальні проблеми комп'ютерних наук АПКН-2022* : матеріали XIV всеукр. наук.-практ. конф., м. Хмельницький, 18-19 лист. 2022 р. / Хмельницький національний університет. Хмельницький, 2022. С. 251–253. URL: https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn2022_corpuspaper.pdf

6. Савенко Б. О. Самоорганізована розподілена система виявлення зловмисного програмного забезпечення в комп'ютерних мережах. *Математичне та програмне забезпечення інтелектуальних систем (МПЗІС-2022)* : тези доповідей XX міжнар. наук.-практ. конф., м. Дніпро, 23-25 лист. 2022 р. / під заг. ред. О.М. Кісельової. Дніпро, ДНУ, 2022. С. 172–173. URL: http://mpzis.dnu.dp.ua/wp-content/uploads/2022/12/MPZIS-2022-1.pdf

7. Савенко Б. О. Розподілені системи виявлення зловмисного програмного забезпечення. *2022 International Conference on Innovative Solutions in Software Engineering (ICISSE-2022)* : Conference Proceedings, Ivano-Frankivsk, Ukraine, November 29-30, 2022 / Kuz M., Kozenko M. eds. Ivano-Frankivsk, VSPNU, 2022. Pp. 22–25. URL: https://kit.pnu.edu.ua/wp-content/uploads/sites/70/2023/01/2022_International_Conference_on_Innovative_Solutions_in_Software.pdf

8. Савенко Б. О. Модель архітектури частково розподілених систем та їх компонентів в комп'ютерних мережах. *2023 Інформаційні технології та інженерія*: Тези доп. Всеукраїнської науково-практичної конференції молодих вчених, аспірантів і студентів, м. Миколаїв, 7–10 лютого 2023 р. / ЧНУ імені Петра Могили, м. Миколаїв, 2023. С. 81-82. https://dspace.chmnu.edu.ua/jspui/handle/123456789/875

9. Савенко Б., Каштальян А., Петляк Н. Розподілені системи виявлення worm-вірусів. *2023 ITSec: Безпека інформаційних технологій:* матеріали XII Міжнар. наук.-техн. конф., м. Ужгород, 2-4 трав. 2023 р. / НАУ, м. Київ, 2023. С. 37-39. http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf

Розроблено реалізацію частково централізованої розподіленої системи.

10. Savenko B., Kashtalian A., Lysenko S., Savenko O. Malware Detection By Distributed Systems with Partial Centralization. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems:*

Technology and Applications (IDAACS), Dortmund, Germany, 2023 / Pp. 265-270. DOI: https://doi.org/10.1109/IDAACS58523.2023.10348773 - *Scopus*

Розроблено метод синтезу математичних моделей рівнів безпеки компонентів системи.

Публікації, які додатково відображають наукові результати дисертації

11. Савенко Б. О. А. с. 124840, Україна. Комп'ютерна програма «Проміжне програмне забезпечення частково централізованих розподілених систем виявлення зловмисного програмного забезпечення в комп'ютерних мережах». Дата реєстрації 07.03.2024.

Розроблено реалізацію частково централізованої розподіленої системи.

ВВАЖАТИ, що дисертаційна робота __ *Савенко Б. О.* ___

(прізвище, ініціали здобувача)

«Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах»,

(назва)

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, та відповідає напрямку наукового дослідження освітньо-наукової програми Хмельницького національного університету зі спеціальності 123 Комп'ютерна інженерія .

(шифр, назва)

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «_Метод та частково централізовані системи __

назва роботи

виявлення зловмисного програмного забезпечення в комп'ютерних мережах»,

подану __ *Савенко Богданом Олеговичем* _____

прізвище, ім'я, по батькові

на здобуття ступеня доктора філософії, до захисту.

Головуюча публічної презентації:

доктор технічних наук

(науковий ступінь

професор, завідувач кафедри КІІС _____ *Тетяна ГОВОРУЩЕНКО*

вчене звання, посада) *підпис* *Ім'я ПРІЗВИЩЕ*

МІНІСТЕРСТВО ОСВІТИ І НАУКИ ... ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ВІДДІЛ КАДРІВ

Ідентифікаційний код 02071234

Підпис дійсний

Засвідчую

Начальник відділу кадрів

І.С.Мартинюк