Голові разової спеціалізованої вченої ради
ДФ 70.052.022
Хмельницького національного університету
д.т.н., професору Говорущенко Тетяні Олександрівній

Висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Стецюка М.В. «Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення», що подана на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія

Актуальність теми дослідження та її зв'язок з планами наукових робіт університету. Важливою умовою існування та ведення успішної економічної діяльності для будь-якої організації є забезпечення безпеки та неперервності технологічного процесу, що неможливо без підтримання постійної доступності та актуальності інформації, з якою оперує дана організація, її партнери та клієнти. Зловмисники для досягнення певних вигод прагнуть отримати доступ до такої інформації. Для досягнення цієї мети вони використовують різноманітні засоби, зокрема зловмисне програмне забезпечення (ЗПЗ). Тому, вирішення задачі підтримання постійної доступності та актуальності інформації в умовах впливів ЗПЗ, є однією із самих важливих наукових задач в сфері інформаційних технологій (ІТ), орієнтованих на побудову та подальшу експлуатацію спеціалізованих інформаційних систем (ІС). Незважаючи на великий обсяг виконаних в цьому напрямку наукових досліджень і, відповідно, отриманих наукових результатів та розробок, на сьогодні, надзвичайно актуальною, залишається задача покращення забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак.

Дослідження, результати яких викладено в дисертації, виконано в рамках науково-дослідних тематик Хмельницького національного університету: держбюджетної науково-дослідної теми «Агентно-орієнтована система підвищення безпеки та якості програмного забезпечення комп'ютерних систем» № 1Б-2019 (№ держреєстрації 0119U100662); держбюджетної науково-дослідної теми № 1Б-2021 «Самоорганізована розподілена система виявлення зловмисного програмного забезпечення в комп'ютерних мережах» (ДР № 0121U109936). Роль автора в НДР, в якій він є безпосереднім виконавцем, полягає у розробленні моделей, методів та засобів забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення.

Формулювання наукової задачі, мети і задач дослідження. Потреба у засобах забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення, а також відсутність методів для вирішення таких задач створюють актуальну науково-прикладну задачу, одним із шляхів розв'язання якої є розроблення методів та засобів забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення.

Здобувачем на початку дослідження коректно визначено об'єкт і предмет дослідження. Так, об'єктом дослідження є процес забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак. Предметом дослідження є методи і алгоритми забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак.

Метою дисертаційного дослідження є покращення ефективності забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак.

Для досягнення поставленої мети необхідно вирішити такі задачі:

- Провести аналіз методів забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ, типів ЗПЗ і комп'ютерних атак та їх потенційно можливі впливи на апаратно-програмні засоби комп'ютерних систем.

- Розробити абстрактну модель впливів ЗПЗ та комп'ютерних атак на об'єкти комп'ютерних систем для формалізованого представлення їх в якості процесів, що протікають в комп'ютерних системах і впливають на їх працездатність.

- Розробити метод забезпечення відмовостійкості спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак на об'єкти та процеси, що приймають участь у відновленні працездатності ІС та апаратно-програмних засобів після збоїв, які викликані внутрішніми нерегламентованими діями.

- Розробити метод забезпечення живучості спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак на об'єкти комп'ютерних систем та процеси, які використовують механізми забезпечення живучості для відновлення працездатності ІС та апаратно-програмних засобів після збоїв, які викликані зовнішніми нерегламентованими діями та впливами ЗПЗ і комп'ютерними атаками.

- Розробити метод забезпечення захисту інформації спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак на об'єкти комп'ютерних систем та процеси, які використовують механізми забезпечення збереження інформації в процесі одночасної її обробки та впливів.

- Розробити метод забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак на об'єкти комп'ютерних систем та процеси, в якому поєднати впливи та стани забезпечення відмовостійкості, живучості та захисту інформації до впливів.

- Розробити ІС з підсистемами забезпечення відмовостійкості, живучості та захисту інформації, провести з нею експериментальні дослідження щодо встановлення покращення її характеристик при впливах ЗПЗ і комп'ютерних атак та впровадити її у виробництво.

Наукова новизна одержаних автором результатів полягає у розробленні методів та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення, що забезпечило можливість підвищення відмовостійкості та живучості спеціалізованих інформаційних технологій.

Одержано такі наукові результати:

вперше розроблено:

1) метод забезпечення відмовостійкості ІТ згідно інтеграції компонентів надмірностей, який на відміну від відомих методів, надає змогу розширити можливості ІТ в частині їх адаптивності та відповідно автоматичної зміни апаратно-програмної конфігурації, що дозволяє створювати відмовостійкі ІТ щодо впливів ЗПЗ та комп'ютерних атак;

2) метод забезпечення живучості спеціалізованих ІТ згідно аналізу маркерів та збереженої інформації для самодослідження, який на відміну від відомих методів, зберігає інформацію про ключові процеси та здійснює їх самоаналіз, що дає можливість покращити забезпечення живучості ІТ в умовах впливів ЗПЗ та комп'ютерних атак;

3) метод забезпечення захисту інформації спеціалізованих ІТ, який на відміну від відомих, полягає в поєднані із організаційними заходами інтеграцію в ІТ методів сегментування мережі, криптографічного захисту, двофакторної автентифікації програмного забезпечення, створення хибних об'єктів атаки, резервного копіювання з територіальним розмежуванням місць зберігання копій, що дозволяє створювати засоби з покращеним захистом інформації в умовах впливів ЗПЗ та комп'ютерних атак;

4) метод забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ, який на відміну від відомих, полягає в інтеграції в ІТ методів забезпечення відмовостійкості, живучості та захисту інформації згідно їх збігів в станах при реагуванні на впливи ЗПЗ та комп'ютерних атак, що надало змогу створювати спеціалізовані ІС з покращеними характеристиками відмовостійкості, живучості та захисту інформації до цих впливів.

Практичне значення одержаних результатів. Практичне значення отриманих результатів полягає в розробленні методів, алгоритмів та засобів забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ, в яких поєднані та інтегровані механізми забезпечення відмовостійкості, живучості та захисту інформації згідно їх збігів в станах при реагуванні на впливи ЗПЗ та комп'ютерних атак. Це дало змогу створювати спеціалізовані ІС стійкі до таких впливів. В результаті проведених експериментальних досліджень з засобами, в які імплементовано розроблені методи, отримано покращені характеристики відмовостійкі, живучості та захисту інформації до впливів ЗПЗ та комп'ютерних атак, оціночні значення яких становлять окремо для спеціалізованої ІТ з імплементованим методом забезпечення відмовостійкості 76%, з імплементованим методом забезпечення живучості 72% та при інтеграції в спеціалізовану ІТ методу забезпечення відмовостійкості, живучості та захисту інформації 67%.

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій, які захищаються. Наукові положення, висновки і рекомендації дисертації обґрунтовані коректним та доцільним використанням математичного апарату, алгоритмами забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ, успішною програмною реалізацією розробленої ІС, ефективним практичним впровадженням результатів дисертаційного дослідження на підприємствах,

що експлуатують комп'ютерні системи, яке продемонструвало відповідність теоретичних досліджень з реальними результатами застосування.

Особистий внесок здобувача полягає в розробленні нових моделей, методів, елементів інформаційної технології та інструментальних засобів, що забезпечують вирішення поставлених у дисертації задач. Всі основні наукові положення, результати, висновки і рекомендації дисертаційної роботи отримані автором особисто. Основні результати дисертації опубліковані у 12 наукових працях, серед яких 6 статей у фахових наукових журналах України, 6 публікацій у матеріалах конференцій, де засвідчена апробація отриманих результатів, з яких дві праці індексовані у наукометричній базі Scopus. Крім того, отримано 1 свідоцтво про реєстрацію авторського права на твір (програму). При вивченні рукопису мною не були встановлені факти текстових запозичень без відповідних посилань на літературні джерела.

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 також на: Міжнародній науково-практичній конференції «Інформаційні технології та взаємодії» (м. Київ, 2018); 1st International Workshop on Intelligent Information Technologies & Systems of Information Security. - Khmelnytskyi, Ukraine, June 10-12, 2020; 2st International Workshop on Intelligent Information Technologies & Systems of Information Security. - Khmelnytskyi, Ukraine, March 24-26, 2021; XII всеукраїнської науково-практичній конференції «Актуальні проблеми комп'ютерних наук АПКН-2020» – Хмельницький: ХНУ, 2020; Proceedings of VII International conference "Information Technology and Interactions" (IT&I-2020) , 02-04 December 2020. – Taras Shevchenko National University, Kyiv; II Всеукраїнській науково-практичній конференції здобувачів вищої освіти й молодих учених "Комп'ютерна інженерія і кібербезпека: досягнення та інновації", м. Кропивницький, 25–27 листопада

2020 p.; 3st International Workshop on Intelligent Information Technologies & Systems of Information Security. - Khmelnytskyi, Ukraine, May 25-27, 2022.

Структура та обсяг дисертації. Дисертація складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та додатків. Повний обсяг роботи становить 249 сторінок друкованого тексту, з них анотація – на 12 стор., зміст – на 4 стор., перелік умовних скорочень – на 1 стор., основний текст – на 160 стор., список із 136 використаних джерел – на 19 стор., додатки – на 54 стор. Дисертація містить 55 рисунків та 4 таблиці.

Зауваження. В результаті вивчення рукопису мною сформовано наступні зауваження:

1. Недостатньо деталізовані вимоги до архітектури ІС при її реалізації із застосуванням спеціалізованої ІТ із застосуванням запропонованого методу забезпечення відмовостійкості в умовах впливів ЗПЗ.

2. Не забезпечена відкритість архітектури взаємодіючих процесів кроку один методу забезпечення відмовостійкості для врахування, поки що невідомих, не вивчених впливів ЗПЗ.

3. Не розкрито алгоритм двофакторної перевірки контролю легальності програмного забезпечення клієнтських робочих місць методу захисту інформації для випадку атаки із зовнішньої мережі.

4. На сторінці 121 вказано термін «швидкість реакції», хоча по тексту дисертації і в контексті роботи використовується термін «час реакції».

Зазначені зауваження суттєво не впливають на належний рівень і якість проведеного дослідження.

Загальний висновок. Вважаю, що дисертаційна робота Стецюка М.В. «Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення» містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі комп'ютерної інженерії, які в

сукупності забезпечують розв'язання актуальної науково-прикладної задачі забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення. Дисертаційна робота «Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення» відповідає вимогам наказу Міністерства освіти і науки України №40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації», а також відповідає вимогам, передбачених «Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (Постанова Кабінету Міністрів України №44 від 12.01.2022 р.), а її автор, Стецюк Микола Васильович, 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 Ю.П. Кльоца засвідчую»:
Проректор з наукової роботи Хмельницького
національного університету _____ Олег СИНЮК