РЕЦЕНЗІЯ

рецензента Ахрамович В.М., доктора технічних наук, професора
на дисертаційну роботу Марченка Віталія Вікторовича
«Метод виявлення шкідливих процесів в інформаційній системі підприємства
на основі ідентифікації та діагностування станів логічних об'єктів»
представлену на здобуття наукового ступеня доктора філософії з галузі знань
12 Інформаційні технології за спеціальністю 125 Кібербезпека

1. Актуальність обраної теми.

Тема «Виявлення шкідливих процесів в інформаційній системі підприємства» є актуальною в сучасному світі, оскільки інформаційні технології є невід'ємною частиною бізнесу та повсякденного життя.

У світі, де обмін інформацією здійснюється за допомогою комп'ютерів та Інтернету, інформаційна безпека стає все більш важливою. У разі порушення безпеки даних можуть виникнути серйозні наслідки, такі як втрата конфіденційної інформації, пошкодження даних, витік особистих даних та інші Окрім того, такі події можуть призвести до збитків у грошовому виразі, порушення репутації та недовіри клієнтів.

Захист інформації від шкідливих процесів, таких як хакерські атаки, віруси та шкідливі програми, стає все важливішим для забезпечення безпеки та успішності діяльності підприємств та організацій. Тому дисертаційного дослідження «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів» є важливим етапом у забезпеченні інформаційної безпеки, що дозволяє швидко виявляти та усувати загрози для інформаційних систем та даних. Крім того, застосування методів виявлення шкідливих процесів дозволяє

підвищити рівень безпеки та знизити ризики порушення правил та норм у сфері інформаційної безпеки.

2. Обґрунтованість наукових положень, висновків і рекомендацій дисертації.

Обґрунтованість наукових положень, висновків і рекомендацій базуються на отриманих результатах здійсненого здобувачем аналізу широкого кола наукових праць вітчизняних та зарубіжних авторів. Слід зазначити належний ступінь наукової обґрунтованості висунутих автором теоретичних положень, розрахунків та висновків, що забезпечується застосуванням існуючих інструментів дослідження, що базуються на теорії скінченних автоматів, машинного навчання, методів обробки великих даних, вибору компонент та навчання моделей для виявлення шкідливих процесів в інформаційній системі підприємства.

3. Оцінка новизни наукових результатів дисертаційного дослідження.

У процесі дослідження, моделювання та розрахунків у дисертаційній роботі одержані наступні наукові результати, а саме:

1) вперше розроблено модель ідентифікації та діагностування станів логічних об'єктів, наукова новизна якого полягає в тому, що вона ґрунтується на теорії скінченних автоматів на основі протоколу TCP, що дозволяє на стадії створення з'єднання ідентифікувати порушення пакету зі встановленими параметрами та діагностувати роботу транспортного протоколу;

2) удосконалено метод вибору критеріїв логічних об'єктів, які підлягають ідентифікації та діагностуванню, щодо виявлення шкідливих процесів, в якому на відміну від існуючих, на основі методу основних компонентів обґрунтовано вибір параметрів вхідних даних логічного об'єкту моделі розширеного скінченного автомату TCP протоколу. Такий підхід

дозволяє прискорити обробку даних при виявленні шкідливих процесів в інформаційній системі організації в реальному часі;

3) удосконалено метод виявлення шкідливих процесів в інформаційній системі організації, який на відміну від існуючих, базується на алгоритмах машинного навчання та враховує обрані параметри які підлягають ідентифікації та діагностуванню. Такий метод дозволяє підвищити ефективність ідентифікації та діагностування станів логічних об'єктів в інформаційній системі організації в реальному часі.

Наукові положення, висновки та рекомендації, які викладені в дисертаційній роботі, є обґрунтованими і містять наукову новизну, проведені дослідження є внеском у вирішення поставленого завдання.

4. Практична цінність отриманих результатів.

Наукові результати, отримані в дисертації, можуть бути використані для вирішення проблеми вразливості систем виявлення шкідливих процесів у режимі реального часу. Практична цінність отриманих результатів полягає в ефективності виявлення шкідливих процесів у реальному часі на 65-99% порівняно з існуючими сучасними методами та зменшенні кількості помилкових спрацьовувань на 13% -14%, що дає можливість інтегрування даного методу в системи виявлення вторгнень та підвищенні функціонування інформаційних систем підприємства.

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

Результати дисертаційної роботи реалізовано в науково-дослідних роботах на тему «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах кібернетичних атак» (№ 0114U000391 м. Київ) та «Методологія виявлення шкідливих процесів в

інформаційних системах (№ 0121U113613, м. Київ) та в навчальному процесі Державного університету телекомунікацій.

Також результати наукових досліджень прийняті до впровадження в ТОВ «Смартс» та в ТОВ «ЄВРОТЕЛЕКОМ».

6. Повнота викладу основних результатів дисертації в публікаціях.

Основні наукові положення дисертації викладено та опубліковано в 12 наукових праць серед яких: 8 наукових статей, з яких: 5 – в фахових виданнях України, у яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора й кандидата наук, 1 – в закордонних виданнях (Франція), 1 – індексується в Scopus (Категорія А), 1- в інших та в 4 тезах і матеріалах доповідей на 4 конференціях, 1 – в закордонному виданні.

7. Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення.

Зміст та обсяг дисертаційної роботи Марченка В.В. та анотація до неї характеризуються цілісністю та логічністю викладу матеріалів і відповідає діючим вимогам щодо дисертацій на здобуття наукового ступеня доктора філософії передбаченим чинним «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженим постановою Кабінету Міністрів України від 12 січня 2022 р. №44.

8. Зауваження до проведеного дисертаційного дослідження.

Ознайомлення зі змістом дисертаційної роботи Марченка В.В., при загальній позитивній її оцінці дозволило визначити наступні зауваження:

1. В роботі використовується метод головних компонент для методу виявлення шкідливих процесів, проте не наведено обґрунтування вибору даного методу.

2. При оцінці ефективності розробленого методу виявлення шкідливих процесів доцільно було б порівняти його з машинним навчанням без вчителя.

3. Наявні нечіткі формулювання в роботі, наприклад, протиріччя зменшення хибно-позитивних спрацювань, а вирішує завдання розробки методу виявлення шкідливих процесів у реальному часі і т.д., що не дозволяє чітко аналізувати роботу.

Визначені зауваження не зменшують наукової цінності поданої на захист дисертаційної роботи Марченка Віталія Вікторовича, в якій представлено результати вирішення актуальної наукової задачі, що має теоретичне та практичне значення та оцінюється позитивно.

9. Висновок.

Дисертація Марченка В.В. є завершеним науковим дослідженням, що містить наукові результати, що дозволяють вирішити актуальне наукове завдання, спрямоване на розробку методу виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів.

За рівнем наукової новизни, якістю досліджень, достовірністю та обґрунтованістю висновків дисертація Марченка В.В. на тему «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів» відповідає спеціальності 125 Кібербезпека та задовольняє чинним вимогам п. 6-9 «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, які висуваються до дисертації, а її автор, Марченко Віталій Вікторович, заслуговує присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Рецензент
Доктор технічних наук, професор,
професор кафедри систем інформаційного та кібернетичного захисту
Державного університету телекомунікацій
МОН України

Володимир АХРАМОВИЧ

Підпис професора кафедри систем інформаційного та кібернетичного захисту засвідчую,
учений секретар Державного університету телекомунікацій А.М. Тямшина

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 13:20:50 20.04.2023

Назва файлу з підписом: Відгук рецензента Ахрамович.pdf.p7s
Розмір файлу з підписом: 2.3 МБ

Перевірені файли:
Назва файлу без підпису: Відгук рецензента Ахрамович.pdf
Розмір файлу без підпису: 2.3 МБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: АХРАМОВИЧ ВОЛОДИМИР МИКОЛАЙОВИЧ
П.І.Б.: АХРАМОВИЧ ВОЛОДИМИР МИКОЛАЙОВИЧ
Країна: Україна
РНОКПП: 1875912050
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 13:20:49 20.04.2023
Сертифікат виданий: АЦСК АТ КБ «ПРИВАТБАНК»
Серійний номер: 248197DDFAB977E5040000009BA60001D53D1604
Алгоритм підпису: ДСТУ-4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в CMS-файлі (CAdES)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований