ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА

Завідувача кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету, доктора технічних наук, професора Казмірчук Світлани Володимирівни

на дисертаційну роботу Марченка Віталія Вікторовича на тему:

«МЕТОД ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОЦЕСІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА НА ОСНОВІ ІДЕНТИФІКАЦІЇ ТА ДІАГНОСТУВАННЯ СТАНІВ ЛОГІЧНИХ ОБ'ЄКТІВ»

подану на здобуття наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 125 Кібербезпека.

1. Актуальність теми дисертації

Виявлення шкідливих процесів в інформаційній системі підприємства є надзвичайно актуальною темою в сучасному світі. У зв'язку зі збільшенням кількості даних, що зберігаються в такій системі, з'являється необхідність в ефективному моніторингу та виявленні ненормальних станів логічних об'єктів, які можуть бути зумовлені не тільки спрямованими атаками, але й відмовами обладнання, неправильним програмним забезпеченням або відсутністю досвідчених адміністраторів. Крім того, інформаційна система є однією з ключових складових ефективного управління підприємством, яка зберігає велику кількість конфіденційної інформації про підприємство, його клієнтів, робітників і партнерів, тому її захист від шкідливих процесів є критично важливим.

Шкідливі процеси можуть мати різні форми і проявлятися на різних рівнях інформаційної системи. Захист від таких процесів у інформаційних системах є ключовим елементом забезпечення безпеки інформації, зменшення ризиків втрати конфіденційної інформації та захисту бізнесу від можливих фінансових втрат.

Виявлення шкідливих процесів в інформаційній системі підприємства дає змогу ідентифікувати можливі загрози безпеці даних та самій системі на ранніх стадіях їх появи, а також дозволяє зменшити час, необхідний для виявлення та усунення несправності в роботі інформаційної системи, що може зменшити затрати на її підтримку та позитивно позначитися на діяльності підприємства в цілому.

Тому, виявлення шкідливих процесів в інформаційній системі підприємства є дуже важливою задачею, яка дозволяє забезпечити безпеку та надійність системи. А тема дисертації «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностики стану логічних об'єктів» є актуальною в сучасних умовах.

2. Аналіз основного змісту, наукової новизни і практичної цінності, достовірності та обґрунтованості результатів.

Аналіз основного змісту, наукової новизни та практичної цінності

Дисертація складається з анотації, вступу, трьох розділів, висновків, списку використаних джерел та додатків. Повний обсяг, якої становить 160 сторінок друкованого тексту, з них 126 сторінок основного матеріалу. Матеріали дисертації містять 22 рисунки та 15 таблиць. Загальний список використаних джерел становить 111 найменувань. Додатки подано на 6 сторінках.

За своїм змістом дисертаційна робота Марченка В.В. відповідає чинним вимогам щодо оформлення дисертацій на здобуття наукового ступеня доктора філософії. Зміст роботи відповідає поставленим у ній задачам.

Новизна одержаних результатів. В рамках проведених досліджень для досягнення мети автором особисто отримані наступні нові наукові результати:

1) вперше розроблено модель ідентифікації та діагностування станів логічних об'єктів, яка 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, що дозволяє прискорити обробку даних при виявленні шкідливих процесів в інформаційній системі організації в режимі реального часу;

3) удосконалено метод виявлення шкідливих процесів в інформаційній системі організації, що дозволяє підвищити ефективність ідентифікації та діагностування станів логічних об'єктів в інформаційній системі організації в режимі реального часу.

Практичне значення одержаних автором наукових результатів підтверджується результатами дослідження з використанням спеціально створеного тестового стенду, у результаті чого було отримано визначені показники для кількісної оцінки якості роботи методу виявлення шкідливих процесів в інформаційній системі підприємства. Отримані результати свідчать, що застосування запропонованого автором методу виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів дозволяє підвищити ефективність виявлення таких процесів в режимі реального часу в середньому на 50% на відміну від існуючих сучасних методів та зменшення кількості хибно-позитивних спрацювань на 13-14%.

Ступінь достовірності й обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

Обґрунтованість наукових результатів, одержаних здобувачем, обумовлюється застосуванням відомих підходів та методів, зокрема теорії скінченних автоматів, методи кореляційної теорії, методи мета-аналізу, системного аналізу, методів машинного навчання.

Додатково достовірність отриманих результатів підтверджено їх використанням у виробничому процесі, що відображено у відповідних актах впровадження, а саме впровадження у діяльності ТОВ «Смартс» та в ТОВ «ЄВРОТЕЛЕКОМ» (довідка про впровадження від 16.01.23).

Оцінка мови, стилю та змісту дисертації, відповідність встановленим вимогам щодо оформлення.

Оформлення дисертації відповідає вимогам Державних стандартів України. Текст дисертації написано грамотною технічною мовою, ясно та зрозуміло. Дисертація являє собою одноосібно написану наукову працю, яка містить сукупність наукових результатів, виставлених автором для публічного захисту, має внутрішню єдність і свідчить про особистий внесок автора у науку.

Повнота викладу наукових результатів дисертації в публікаціях. Основні результати дисертаційної роботи Марченка В.В. повністю викладені у 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, 1 – індексується в Scopus, 1- в інших та в 4 тезах і матеріалах доповідей на 4 конференціях, 1 – в закордонному виданні, що входять до переліку видань, дозволених МОН України для публікацій результатів досліджень з технічних наук.

Зазначені публікації в повній мірі висвітлюють основні наукові результати дисертації.

Зауваження та недоліки до тексту дисертації

1. У дисертаційні роботі автор зазначає, що практичне значення одержаних результатів полягає в розроблені методу виявлення шкідливих процесів і аналогічний результат заявлено у п. 3 наукової новизни. Таким чином не зрозуміло до чого автор зараховує зазначений результат.

2. В роботі предметом дослідження заявлено метод виявлення шкідливих процесів в інформаційній системі підприємства, який корелюється з метою роботи, але не в повній мірі відповідає проведеному аналізу відомих розробок. Автор проаналізував механізми захисту інформаційної системи підприємства, підходи машинного навчання щодо виявлення шкідливих процесів в інформаційній системі організації, науково-методичні підходи виявлення аномалії. Але за правилами в дисертації підлягає аналізу предмет дослідження, що зазначається в першій задачі. Тобто, за визначеними позиціями - це аналіз відомого методу виявлення шкідливих процесів в інформаційній системі підприємства.

3. У дисертаційні роботі автор використовує поняття «логічний об'єкт», але не надає вичерпного визначення його сутності, бажано б додати певні описи формальної логіки та логічних правил, які саме використовуються.

4. Наукова новизна сформульована не за правилами. Потрібно чітко зазначати які конкретні елементи (величини) запропонованої моделі чи кроки

розробленого методу відрізняють його від відомих та забезпечують заявлений ефект. Наприклад, в п. 1 наукової новизни автор констатує що новизна моделі «… ґрунтується на теорії скінченних автоматів …», але ця теорія не є елементом моделі, вона є лише інструментом створення елемента з необхідними властивостями, що дає моделі можливість досягнення заявленого ефекту.

5. У п. 2 наукової новизни відповідно заявлено, що метод «… дозволяє прискорити обробку даних …», але у п. 3 висновку (що стосується цього методу), відповідно до правил, необхідно зазначати конкретний кількісний ефект. Тобто, не зрозуміло на скільки прискорилась обробка даних.

6. В роботі часто використовується термін «в реальному часі», але за контекстом це є не коректним, тому слід застосовувати «… в режимі реального часу …».

Проте, зазначені недоліки не є визначальними і тому не знижують цінності дисертаційної роботи, її науково-теоретичного і практичного значення та загальної позитивної оцінки.

3. Загальний висновок по роботі.

Дисертаційна робота Марченка Віталія Вікторовича є завершеною кваліфікаційною працею та свідчить про особистий внесок автора в науку. Робота містить нове вирішення актуального наукового завдання щодо методу виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів.

Дисертаційна робота має зазначену наукову новизну та практичну значимість, відповідає 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 дисертацій, а її автор, Марченко Віталій Вікторович, заслуговує присудження наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 125 Кібербезпека.

Офіційний опонент:
Завідувач кафедри
комп'ютеризованих систем захисту інформації
Національного авіаційного університету

доктор технічних наук, професор

«19» 04 2023 р. С. В. Казмірчук

Підпис гр. Казмірчук С.В.
з а с в і д ч у ю
Вчений секретар
Національного авіаційного університету
М. Лежнький

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
01132330
МІСТО КИЇВ

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 09:32:59 19.04.2023

Назва файлу з підписом: Відгук_Казмірчук.pdf.p7s
Розмір файлу з підписом: 13.4 МБ

Перевірені файли:
Назва файлу без підпису: Відгук_Казмірчук.pdf
Розмір файлу без підпису: 13.4 МБ

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

Підписувач: КАЗМІРЧУК СВІТЛАНА ВОЛОДИМИРІВНА
П.І.Б.: КАЗМІРЧУК СВІТЛАНА ВОЛОДИМИРІВНА
Країна: Україна
РНОКПП: 3108614400
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 09:32:58 19.04.2023
Сертифікат виданий: АЦСК АТ КБ «ПРИВАТБАНК»
Серійний номер: 248197DDFAB977E5040000004C1C000163C81404
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