ВІДГУК

офіційного опонента – доктора технічних наук, професора Радівілової Тамари Анатоліївни, на дисертацію Марченка Віталія Вікторовича «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.

Ступінь актуальності обраної теми дисертації

Тема «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностики стану логічних об'єктів» є актуальною в сьогоденні, оскільки інформаційні технології стали невід'ємною частиною бізнесу та повсякденного життя. Сьогодні компанії активно використовують інформаційні системи для підтримки своєї діяльності, тому надійність і безпека цих систем є дуже важливою. Однак інформаційні системи вразливі до різноманітних шкідливих процесів, таких як хакерські атаки, віруси, апаратні та програмні збої тощо. Ці шкідливі процеси можуть призвести до втрати даних, порушення роботи інформаційних систем і завдати значної шкоди бізнесу.

Крім того, як показують щорічні звіти провідних організацій, зловмисники постійно вдосконалюють свої механізми атак, і будь-яка організація, яка нехтує своєю безпекою, у майбутньому може стати жертвою кібернетичної атаки. Ще одним важливим фактором, який слід враховувати, є «неминуча людська помилка», як під час налаштування та використання інформаційних систем, так і під час їх захисту. Можливе рішення цих проблем – використання методів та технологій виявлення шкідливих процесів. Таким чином, тема «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностики стану логічних об'єктів» дисертації Марченка Віталія Вікторовича є актуальною і присвячена вирішенню важливого для науки і практики завдання.

Актуальність теми дисертаційного дослідження додатково підтверджується її безпосереднім зв'язком із Стратегією кібербезпеки України від 26 серпня 2021 року №447/2021.

Ступінь обґрунтованості наукових результатів, висновків і рекомендацій, сформульованих в дисертації

Достовірність наукових положень та висновків, сформульованих у дисертації, забезпечена теоретичною обґрунтованістю вихідних положень,

кількісним та якісним дослідженням фактичного матеріалу, який отримав автор у процесі дослідження.

Слід зазначити, що дисертація Марченка В.В. відзначається як за своїм змістом, так і характером викладу основних теоретичних положень. Текст дисертації характеризується науковим викладом, смисловою завершеністю, цілісністю, що є свідченням високої загальної культури автора, вмінням здобувача правильно добирати слова, точно і ясно висловлювати наукову думку.

Наукова новизна та достовірність одержаних результатів

Ознайомлення зі змістом дисертації, основними публікаціями та анотацією дозволяє визнати, що мету дослідження досягнуто. Це знайшло відображення в основних положеннях роботи, які сформульовані автором особисто і характеризуються певною науковою новизною.

Зокрема, автором:

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.

Достовірність дисертаційних досліджень підтверджується проведенням коректного експерименту та отримання достовірних розрахунків.

Повнота викладу основних положень дисертації в опублікованих працях

Основні наукові положення, результати і висновки дисертаційної роботи отримані автором самостійно. Проведений аналіз наукових праць здобувача

показав, що основні результати дисертаційної роботи повноцінно відображені в публікаціях автора. Повнота викладення отриманих результатів дослідження та їх оформлення можуть оцінюватись як достатні. Робота має завершений характер, висновки і пропозиції достатньою мірою розкриті і обґрунтовані у текстовій частині дисертації.

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.

Кількість, обсяг та зміст друкованих праць відповідають вимогам МОН України щодо публікацій основного змісту дисертації на здобуття наукового ступеня доктора філософії та надають авторові право публічного захисту дисертації.

Практичне значення одержаних автором наукових результатів

Здобуті в дисертації наукові результати можуть бути використані для розв'язання часткової задачі виявлених вразливостей функціонуючих систем в реальному часі.

Реалізація запропонованого методу виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів дозволяє підвищити ефективність виявлення шкідливих процесів в режимі реального часу на 65-99% на відміну від існуючих сучасних методів та зменшити кількість хибно-позитивних спрацювань на 13-14%.

Оцінка змісту дисертації, її завершеності та відповідності встановленим вимогам

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

Робота виконана на належному науковому рівні, є завершеною науковою працею, має практичне значення та відображає розв'язання актуального науково завдання. Робота характеризується цілісністю та логічністю викладу матеріалів.

Дисертація оформлена відповідно до вимог Міністерства освіти і науки України, що висуваються до такого роду наукових робіт.

Зауваження та дискусійні положення щодо змісту дисертації

1. При викладенні матеріалу другого розділу автором описано роботу TCP-протоколу на основі специфікації стандартних документів, таких як Інтернет стандарт RFC, на основі якого показано перехід на розширенні скінчені автомати. Однак автором не відображено яким чином відбувається виявлення аномальних процесів на транспортному рівні, а показано тільки можливі атаки, які можуть бути виявлені на даному рівні.

2. З дисертаційної роботи не зовсім зрозуміло, чому саме виявлення шкідливих процесів повинно бути розглянуто на транспортному рівні моделі OSI і з використанням яких механізмів це вирішується.

3. В підрозділі 3.4 запропонований алгоритм роботи методу виявлення шкідливих процесів узагальнено, доречно було б деталізувати блоки збору, обробки та діагностування системи.

Разом із тим, вказані зауваження не знижують загальної високої оцінки проведеної роботи, наукової та практичної цінності дисертації.

Загальна оцінка роботи та висновки

Дисертаційна робота Марченка Віталія Вікторовича є завершеним науковим дослідженням, що спрямоване на вирішення актуального наукового завдання щодо розробки методу виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностуванні станів логічних об'єктів.

Дисертаційна робота за актуальністю вибраної теми, обсягом і рівнем теоретичних та експериментальних досліджень, достовірністю та обґрунтованістю висновків, науковою новизною, значенням отриманих результатів для науки і практики 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 дисертацій, а її автор, Марченко Віталій Вікторович, заслуговує присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Професор кафедри Інфокомунікаційної інженерії ім. В.В. Поповського Харківського національного університету радіоелектроніки

доктор технічних наук, професор Т.А. Радівілова

«_04_»_квітня_2023 р.

Підпис засвідчено
Начальник відділу

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 16:13:21 08.04.2023

Назва файлу з підписом: Відгук опонента (Радівілова).pdf.p7s
Розмір файлу з підписом: 685.8 КБ

Перевірені файли:
Назва файлу без підпису: Відгук опонента (Радівілова).pdf
Розмір файлу без підпису: 667.0 КБ

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

Підписувач: РАДІВІЛОВА ТАМАРА АНАТОЛІЇВНА
П.І.Б.: РАДІВІЛОВА ТАМАРА АНАТОЛІЇВНА
Країна: Україна
РНОКПП: 2913916026
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 16:13:20 08.04.2023
Сертифікат виданий: АЦСК АТ КБ «ПРИВАТБАНК»
Серійний номер: 248197DDFAB977E504000000AFC0DF008DAE0E04
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