ВІДГУК

офіційного опонента на дисертаційну роботу
Міщенка Максима Валерійовича
на тему «Прогнозування та виявлення загроз для корпоративних комп'ютерних мереж засобами експертних систем»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 122 Комп'ютерні науки

Актуальність теми дисертації.

Вирішення проблем кібербезпеки є актуальним завданням в умовах цифровізації інформаційних процесів. Останнім часом спостерігається стрімке збільшення кількості кібератак, які виконуються як індивідуальними зловмисниками, так і угруповуваннями, що здійснюють напади кібертероризму та ведуть кібервійни. Корпоративні мережі, зокрема, часто стають ціллю кібернападів і завдають великих збитків бізнесу. Зловмисники постійно вдосконалюють свої напади та використовуване шкідливе програмне забезпечення, що створює різноманітність у типах загроз та ускладнює їх виявлення. Для ефективної протидії існуючим загрозам необхідно вдосконалювати моделі виявлення загроз методами, які здатні виявляти відомі загрози, а також виявляти знайомі шаблони в модифікованих та нових загрозах. Перспективними для виявлення нових загроз є методи машинного навчання.

Одним з важливих факторів надійного кіберзахисту є швидкість реакції на загрози, що спонукає до розробки спеціалізованих експертних систем. Застосування ефективного рушію висновків експертної системи дозволяє визначати ймовірності виникнення загроз та відповідно розробляти заходи кібербезпеки. Дисертаційне дослідження, подане до захисту Міщенком М.В., використовує поєднання засобів експертних систем та виявлення загроз методами машинного навчання для підвищення точності виявлення загроз та визначення ймовірностей загроз в майбутньому для оперативного прийняття рішень щодо заходів безпеки. Оскільки своєчасне виявлення загроз в інформаційній системі та прийняття рішень щодо їх усунення надає можливість зменшити негативний вплив діяльності зловмисників, тема дослідження є надзвичайно актуальною.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

– вперше запропоновано метод визначення секції Linux ELF файлу UNIX-подібних операційних систем, який, на відміну від існуючих, містить процеси семантичного аналізу та ідентифікації шкідливого програмного забезпечення для підвищення точності та оперативності виявлення загроз;

– удосконалено метод ідентифікації шкідливих Windows PE файлів операційних систем сімейства Windows, який, на відміну від існуючих, використовує секцію таблиці імпортів у поєднанні з моделями word2vec та ансамблю дерева рішень, що надає можливість підвищити точність ідентифікації;

– удосконалено метод виявлення DDoS атак, який, на відміну від існуючих, містить поєднання моделей Isolation Forest та EWMA-статистики, що надає

можливість враховувати часові характеристики рядів спостережень мережевих параметрів для підтримки прийняття рішення щодо існування загрози;

– набула подальшого розвитку модель інформаційної технології виявлення та аналізу кіберзагроз для корпоративної комп'ютерної мережі, яка, на відміну від існуючих, надає можливість комплексного використання модулів ідентифікації шкідливого ПЗ та рушія висновків для підтримки прийняття рішень щодо заходів кібербезпеки.

Основні наукові результати дослідження полягають у розробці та удосконаленні методів виявлення та прогнозування загроз для корпоративних мереж засобами експертної системи на основі моделей машинного навчання, що дозволило підвищити точність виявлення загроз та зменшити час їх виявлення, зокрема, шкідливого програмного забезпечення та DDoS атак.

Практичне значення дисертаційного дослідження полягає у розробці інформаційної технології, що може бути використана фахівцями з кібербезпеки або системними адміністраторами корпоративної мережі для прийняття рішень щодо її захисту.

Отже, в дисертаційній роботі поставлене наукове завдання виконане повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Міщенка М.В. повністю відповідає Стандарту вищої освіти зі спеціальності 122 Комп'ютерні науки та напрямам досліджень відповідно до освітньо-наукової програми третього (освітньо-наукового) рівня «Комп'ютерні науки».

Дисертація є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям розробки методів та моделей для експертної оцінки кіберзагроз.

Розглянувши звіт подібності та перевірки роботи на текстові співпадіння з існуючими роботами, можна зробити висновок, що дисертаційна робота Міщенка Максима Валерійовича є результатом самостійних досліджень, не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані в даному дослідженні ідеї, результати та тексти інших авторів мають посилання на відповідне джерело. Принципи академічної доброчесності не були порушені.

Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою, складається з анотації, написаної українською та англійською мовами, вступу, 4 розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 188 сторінок.

Текст дисертації викладений логічно та послідовно, має належну редакторську якість та відповідає чинним вимогам до оформлення дисертацій, автор дотримується наукового стилю та використовує загальноприйняту термінологію.

У вступі обґрунтовано актуальність теми дослідження, наведені його мета і завдання, визначено об'єкт і предмет дослідження, наведено наукову новизну результатів дисертаційного дослідження та їх практичне значення, вказано апробацію та публікації.

У першому розділі проведено аналіз існуючих кіберзагроз для корпоративних комп'ютерних мереж, методів їх виявлення та прогнозування. На основі аналізу існуючих досліджень та розрбок у сфері кібербезпеки сформовано модель кіберзагрози для корпоративної мережі та модель процесу її виявлення та прогнозування. Для процесу виявлення кіберзагроз виділено кроки: виявлення вектору вразливості, оцінки вразливості, визначення протидії та прогнозування ймовірності експлуатації загрози. Для визначення найбільш розповсюджених загроз проаналізовано актуальні звіти кіберінцидентів.

У другому розділі викладені запропоновані автором дослідження методи виявлення загроз та метод визначення вразливостей. Метод визначення секції Linux ELF файлу розроблений для ідентифікації шкідливого програмного забезпечення і використовує NLP моделі та методи машинного навчання. Метод ідентифікації шкідливого ПЗ для операційних систем Windows та метод виявлення DDoS атак розроблені з використанням поєднання EWMA статистики та моделі Isolation Forest. Для визначення ймовірностей загроз автор використовує баєсову мережу. Наведено обчислення F-міри для запропонованих та існуючих методів на експериментальному наборі даних та доведено статистичну значимість різниці в отриманих результатах, що свідчать про більшу точність класифікації у випадку застосування запропонованих автором методів. Запропоновані методи комплексно використовуються в розробленій інформаційній технології виявлення загроз та визначення вразливостей для наповнення бази даних, яку використовує рушій висновків для визначення ймовірностей виникнення загроз та підтримки процесу прийняття рішень щодо захисту корпоративної мережі.

У третьому розділі наведено моделювання інформаційної технології з використанням діаграм IDEF0 та UML, що деталізує функціональні процеси в запропонованій інформаційній технології та надає розуміння варіантів використання запропонованої технології.

У четвертому розділі представлено розробку інформаційної системи виявлення загроз та визначення вразливостей методами, описаними у другому розділі. Виконано моделювання корпоративної мережі у віртуальному середовищі GNS3 та експериментально досліджено на моделі перевагу запропонованих рішень у порівнянні з антивірусним програмним забезпеченням Microsoft Defender та ClamAV.

Дисертаційна робота оформлена у відповідності до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи.

Наукові результати дисертації висвітлені у 8 наукових публікаціях автора, з них 4 статті опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України, 1 стаття опублікована у періодичному науковому виданні, що індексується у базі даних Scopus. Результати дослідження доповідались на 3 наукових конференціях.

У наведених публікаціях достатньо повно представлено результати дисертаційної роботи. Порушення академічної доброчесності в них не виявлено.

Особистий внесок здобувача у публікаціях, зазначений у дисертації, свідчить про його авторство у відповідних наукових досягненнях.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. Підрозділ 1.3 названий «Аналіз методів для виявлення та прогнозування кіберзагроз», проте він містить тільки невеличкий перелік методів, які можуть бути застосовані без указування умов, за яких вони можуть бути успішно застосовані.

2. У тексті дисертації автор використовує термін «прогнозування ймовірностей» там, де йдеться про визначення ймовірності виникнення певної події. Якби йшлося про прогнозування ймовірностей, то тоді автор мав би визначати ймовірності в певні майбутні моменти часу. Проте ймовірності визначені незалежно від контексту моменту часу.

3. У підрозділі 1.4 «Постановка задачі…» постановки задачі в термінах дано-знайти немає, є тільки визначений перелік завдань дисертаційного дослідження.

4. У функціональній моделі виявлення та передбачення загроз використовують в одному блоці, хоч вони спираються на використання різних методів та даних. Можна також уявити ситуацію, коли потрібно провести виявлення загроз без передбачення загроз та навпаки, тому не ясно, чому автор вирішив використовувати тільки в комплексі ці методи.

5. Запропоновані інформаційні процеси потребують більш детального дослідження, у тому числі їх швидкодії. Швидкодія окремих методів досліджена в роботі, але не системи в цілому. Яких витрат ресурсів потребує підтримка діяльності запропонованої інформаційної системи також не досліджено.

6. Немає у процесах запропонованої інформаційної системи перенавчання або донавчання нейромережі. Яким чином розроблена інформаційна система буде адаптуватись до нових загроз, які з’являються?

7. Зауваження до оформлення:

- пишемо «проєктування» за новим Українським правописом 2019 року замість «проектування» (перехідний період, коли можна було використовувати обидва варіанти написання слова завершився у 2024 році);
- у таблиці 1.3 деякі комірки порожні;
- у переліку публікацій слід вказувати чи є видання індексованим у Scopus, фаховим;
- загальновідомі формули розрахунки F1-міри наводяться в дисертації двічі на стор. 80 та на стор. 101 (достатньо зробити посилання на джерело, де наведені ці формули);
- на рис. 2.7, 2.15 не зазначено одиниці вимірювання часу;
- термін «ймовірність змінної» на стор.110 слід замінити на «ймовірність події»;
- у висновках не зазначено наукове завдання, яке вирішено.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу.

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Міщенка Максима Валерійовича на тему «Прогнозування та виявлення загроз для корпоративних комп'ютерних мереж засобами експертних систем» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для інформаційних технологій.

Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в 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», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач Міщенко Максим Валерійович заслуговує на присудження наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент:
професор кафедри
інформатики та програмної інженерії
КПІ ім. Ігоря Сікорського,
доктор технічних наук, професор Інна СТЕЦЕНКО

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Відділ кадрів архівної справи № 6

М.П.

«20» 03 2025 року

Підпис Ст. ЗАСВІДЧУЮ Відділ кадрів архівної справи