РЕЦЕНЗІЯ

офіційного рецензента, кандидата фізико-математичних наук, доцента кафедри інформаційних технологій та програмної інженерії Національного університету «Чернігівська політехніка» Акименка Андрія Миколайовича
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.

Кібератаки є однією з найбільш розповсюджених загроз функціонування сучасних організацій, оскільки більшість з них використовують корпоративні мережі для зберігання та обміну конфіденційними даними та ведення підприємницької діяльності. Процес захисту корпоративних мереж стає складнішим з кожним роком, тому що зловмисники вдаються до пошуків нових вразливостей та якісного розвитку кібератак. Це зумовлює необхідність та актуальність створення нових методів виявлення та прогнозування кіберзагроз.

Для виявлення кіберзагроз значний інтерес представляє застосування експертних систем та методів, що здатні виявляти відомі шаблони в існуючих загрозах. Засоби експертних систем можуть бути поєднані з методами машинного навчання або статистичними методами для підвищення точності виявлення загроз, а застосування методів експертних оцінок та рушія висновків дозволяє здійснювати прогнозування ймовірності експлуатації виявлених загроз.

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

Представлена дисертаційна робота запланована та виконана в рамках міжнародного наукового проекту «Cyber Rapid Analysis for Defense Awareness of Realtime Situation – CyRADARS» за грантом NATO SPS (grant agreement number G5286)» та відповідно до плану науково–дослідної роботи Національного університету «Чернігівська політехніка» «Розробка моделей та методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931).

Наукова новизна та практичне значення дослідження.

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 вибору моделі класифікації і 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 імпорту в поєднанні з моделями word2vec та ансамблю дерева рішень, що забезпечує більшу точність виявлення загроз та F-міру класифікації;

– удосконалено метод виявлення DDoS атак, який, на відміну від існуючих, містить поєднання моделей Isolation Forest та EWMA-статистики, що дозволяє враховувати часовий контекст рядів спостережень мережевих параметрів для підтримки прийняття рішення про існування загрози;

– набула подальшого розвитку модель інформаційної технології виявлення та прогнозування загроз для корпоративної комп'ютерної мережі, яка, на відміну від існуючих, враховує комплексне використання модулів ідентифікації шкідливого ПЗ та рушій висновків, що дозволяють виконати прогнозування ймовірності реалізації визначених векторів вразливостей для підтримки прийняття рішень щодо реагування на загрози.

Практичним результатом дисертації є створена комплексна інформаційна технологія, що поєднує застосування засобів експертних систем, методів машинного навчання та статистичного аналізу для вирішення завдання виявлення та прогнозування загроз для корпоративних мереж. Створена технологія дозволяє забезпечити процес підтримки прийняття рішень при забезпеченні захисту корпоративних мереж спеціалістами з кібербезпеки.

Ступінь обґрунтованості наукових положень, висновків, сформульованих у дисертації.

Наукові положення та висновки, сформульовані у дисертаційному дослідженні є достовірними та обґрунтованими з використанням глибокого аналізу існуючих досліджень українських та зарубіжних науковців, нормативно-правових актів, звітів з кібербезпеки організацій та інформаційних ресурсів мережі Internet.

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

Повнота викладення основних результатів дисертації в опублікованих працях.

Наукові результати дисертації представлені у 8 наукових публікаціях автора. З них: 4 статті опубліковані у наукових виданнях, які входять до переліку наукових фахових видань України; 1 стаття вийшла у періодичному науковому журналі, що індексуються у базі даних Scopus. Крім того,

результати дослідження були представлені на 3 наукових фахових конференціях.

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

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 напрямкам досліджень відповідно до освітньої програми «Комп'ютерні науки». Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям «Комп'ютерні науки». Розглянувши звіт подібності за результатами перевірки роботи на текстові співпадіння, можна зробити висновок, що робота Міщенка М.В. є результатом самостійних досліджень та не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Виявлений відсоток співпадінь пояснюється наведенням у дисертації фрагментів з опублікованих статей автора (на які вказане посилання) та використанням загальноприйнятої наукової термінології. Використані ідеї, результати та тексти інших авторів, які використані в даному дослідженні, процитовані та мають належне посилання на відповідне джерело.

Зміст дисертації.

Робота складається зі вступу, чотирьох розділів, переліку умовних скорочень, переліку джерел та додатків.

У першому розділі автор зосереджується на дослідженні найбільш розповсюджених існуючих кіберзагроз для корпоративних комп’ютерних мереж. У якості джерел досліджуються кібербезпекові звіти відомих технологічних компаній, роботи інших авторів та найновіші кіберінциденти. Но основі проаналізованої інформації та існуючих кібербезпекових фрейморків побудована модель кіберзагрози та процесу виявлення і прогнозування кіберзагроз з використанням засобів експертних систем, а також моделей машинного навчання та статистичних моделей.

У другому розділі представлено методи визначення секції Linux ELF файлів, що містить процеси семантичного аналізу та вибору моделі класифікації для ідентифікації шкідливого ПЗ. Ефективність методу оцінена з використанням метрик точності та F-міри. Також проведено статистичну оцінку отриманих результатів та підтверджено їх статистичну значущість. Запропоновано метод ідентифікації шкідливих Windows PE файлів та проведено порівняння їх ефективності з існуючими методами, що показало статистично значущі покращення в точності та F-мірі класифікації. Удосконалено метод виявлення DDoS атак з використанням моделей EWMA та Isolation Forest. Запропоновано

інформаційну технологію, що містить композицію запропонованих методів та елементи експертної системи для здійснення прогнозування ймовірності експлуатації виявлених загроз.

У третьому розділі представлено загальну функціональну модель розробленої інформаційної технології виявлення та прогнозування загроз для корпоративних комп'ютерних мереж. Визначено вхідні та вихідні параметри, обмеження та ресурси. Також змодельовані варіанти використання системи та діаграму баз даних.

В четвертому розділі наведені результати дослідження роботи інформаційної технології у віртуальному середовищі, що моделює корпоративну комп'ютерну мережу. Були проведені оцінки ефективності системи та порівняні з існуючими антивірусними ПЗ, що показало зменшення часу виявлення та збільшення F-міри класифікації загроз.

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

Ідентичність анотації та основних положень дисертаційної роботи.

Анотація в повному обсязі відображає основні положення дисертаційної роботи.

Недоліки та зауваження до дисертаційної роботи.

1. Не зовсім зрозуміло чому наведена в 2-му розділі модель Баєса не була включена до наукових результатів. Сама модель, наведена на рисунку 2.26, містить 2 вершини, які залежні від інших змінних. Хоча, відповідно до завдання, що вирішує метод, залежна вершина має бути одна.
2. Наведена у 4-му розділі на рисунку 4.1 корпоративна комп'ютерна мережа створена в середовищі GNS3 для експериментального аналізу створеної інформаційної системи, є замалою та має спрощену структуру, що не завжди відповідає реальним умовам.
3. Модель кіберзагрози для корпоративної комп'ютерної мережі, наведена на рисунку 1.1, позначена як модель «сутність-зв'язок», хоча насправді має ознаки різних моделей, зокрема діаграми композитної структури та діаграми класів.
4. Метод ідентифікації шкідливих Windows PE файлів на перший погляд, має невелике покращення точності та F-міри порівняно з іншими методами. Можливо було б доцільно також інші характеристики, які б показали кращу ефективність методу.
5. Для методу виявлення мережевих аномалій з використанням Isolation Forest та EWMA статистики не зрозуміло як вимірюється ефективність.

В роботі приведено тільки графічні результати роботи методу, що не дає уявлення про його ефективність у порівнянні з існуючими.

6. В роботі наявні стилістичні та орфографічні помилки.

Усі наведені зауваження не зменшують цінність результатів роботи. Отримані в роботі результати є новими, відповідають поставленим цілям і задачам та мають теоретичне і практичне значення.

Висновок про дисертаційну роботу.

Дисертаційна робота здобувача ступеня доктора філософії Міщенка Максима Валерійовича на тему «Прогнозування та виявлення загроз для корпоративних комп'ютерних мереж засобами експертних систем» є повністю завершеним науковим дослідженням, що виконане на високому професійному рівні.

Дисертаційна робота повністю відповідає вимогам наказу МОН України № 40 від 12.01.2017 р. «Про затвердження Вимог до оформлення дисертації» (зі змінами) та Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 19 травня 2023 року № 502 «Про внесення змін до деяких постанов Кабінету Міністрів України з питань підготовки та атестації здобувачів наукових ступенів», та змін до 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 року № 44.

Вважаю, що Міщенко Максим Валерійович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю «Комп'ютерні науки».

Офіційний рецензент:

кандидат фізико-математичних
наук, доцент кафедри інформаційних
технологій та програмної інженерії
Національного університету
«Чернігівська політехніка» Андрій АКИМЕНКО