РЕЦЕНЗІЯ

офіційного рецензента, доктора технічних наук, професора кафедри інформаційних та комп'ютерних систем Національного університету «Чернігівська політехніка» Зайцева Сергія Васильовича 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.

У сучасному світі питання кібербезпеки є дуже актуальним, адже кількість та складність кібератак постійно зростає, що робить необхідним застосування методів їх виявлення, що здатні самонавчатись та знаходити схожі шаблони в нових загрозах, базуючись на знаннях про відомі кіберзагрози. Також, враховуючи активне ведення кібервійни та здійснення кібертероризму проти приватних та державних організацій України, досить актуальним є питання захисту корпоративних комп'ютерних мереж, які належать таким організаціям.

Методи, засновані на використанні експертних систем, дозволяють виявляти як відомі, так і нові або модифіковані кіберзагрози, засновуючись на експертних знаннях та різних механізмах формування висновків. Застосування експертних систем є доцільним не тільки для виявлення існуючих загроз, а й для прогнозування загроз, зокрема за рахунок поєднання з іншими методами виявлення загроз для наповнення бази знань.

Розробка технологій виявлення та прогнозування загроз для корпоративних комп'ютерних мереж засобами експертних систем підвищує захищеність та сприяє розвитку застосування сучасних технологій для забезпечення кібербезпеки організацій, що робить це дослідження актуальним в сучасних умовах.

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:

1. 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.

2. Удосконалено метод ідентифікації шкідливих Windows PE файлів операційних систем сімейства Windows, який, на відміну від існуючих, використовує секцію таблиці імпортів в поєднанні з моделями word2vec та ансамблю дерева рішень, що забезпечує більшу точність виявлення загроз та F-міру класифікації.

3. 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.

4. Набула подальшого розвитку модель інформаційної технології виявлення та прогнозування загроз для корпоративної комп'ютерної мережі, яка, на відміну від існуючих, враховує комплексне використання модулей 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 інформаційна технологія виявлення та прогнозування загроз для корпоративних комп'ютерних мереж, що може бути використана спеціалістами з кібербезпеки або системними адміністраторами організації для підтримки прийняття рішень щодо захисту комп'ютерних мереж. Також запропоновано нові та удосконалені методи виявлення шкідливого ПЗ та DDoS атак, результати роботи яких слугують для наповнення бази знань створеної технології.

Ступінь обґрунтованості наукових положень, висновків, сформульованих у дисертації.

Обґрунтованість та достовірність наукових положень підтверджується ретельним дослідницьким аналізом наукових робіт українських та зарубіжних науковців, а також експериментів, проведених автором особисто. Обчислювальні досліди детально описані та можуть бути відтворені, що підтверджує достовірність результатів. Це загалом підтверджує достатній рівень практичної значимості та обгрунтованості дослідження.

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 були представлені у 8 наукових публікаціях автора. З них: 4 статті опубліковані у наукових виданнях, які на момент публікації входили 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». В результаті розгляду звіту подібності та перевірки роботи на текстові співпадіння з існуючими роботами, 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. Ідеї, результати та тексти інших авторів, які використані в даному дослідженні, процитовані та мають посилання на першоджерело. Робота складається зі вступу, чотирьох розділів, переліку умовних скорочень, переліку джерел та додатків.

У першому розділі автор досліджує існуючі кіберзагрози для корпоративних комп’ютерних мереж, методи їх виявлення та прогнозування, а також виконує порівняльний аналіз існуючих систем кіберзахисту. У результаті проведеного аналізу літератури, аналітичних звітів компаній з кібербезпеки та інформації про найновіші кіберінциденти з відкритих джерел мережі Internet, автор виділив найбільш поширені сучасні загрози для корпоративних комп’ютерних мереж, механізми їх потрапляння та дії в мережі, а також шляхи їх виявлення. На основі отриманих даних та існуючих безпекових фреймворків, було запропоновано модель кіберзагрози, яка використовується для побудови методів виявлення та прогнозування загроз. Також у першому розділі автор проаналізував підходи виявлення та прогнозування загроз з використанням експертних систем, методів штучного інтелекту та статистичних моделей, базуючись на наукових дослідженнях у сфері кібербезпеки, в результаті чого було сформовано набір методів, що були запропоновані та вдосконалені у дисертаційному дослідженні.

У другому розділі сформульовано та детально описано методи, що слугують для виявлення та прогнозування загроз, та у своїй сукупності об’єднані у

інформаційну технологію, що містить модулі експертної системи . Над розробленими методами проведені експерименти та порівняльний аналіз з існуючими методами та моделями, який показав статистично значущі покращення в точності та f-мірі виявлення загроз.

В третьому розділі виконується моделювання інформаційної технології засобами IDEF0 та UML, що надає розуміння функціональних процесів та варіантів використання запропонованої технології.

В четвертому розділі проведені експерименти у віртуальному середовищі виявлення шкідливого ПЗ та DDoS атак методами у складі запропонованої інформаційної технології. Експерименти підтвердили ефективність методів та показали покращення часу реагування та F-міри методів виявлення шкідливого ПЗ порівняно з антивірусними ПЗ Microsoft Defender та ClamAV.

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

Ідентичність анотації та основних положень дисертаційної роботи.

Анотація в повному обсязі відображає основні положення дисертацій ної роботи.

Недоліки та зауваження до дисертаційної роботи.

1. У другому розділі дисертаційної роботи наведено 4 методи і 1 модель, при чому до наукової новизни віднесено тільки 4 наукових результати. Не зовсім зрозуміло чому модель Баєса наведена в другому розділі, оскільки другий розділ в основному містить пункти наукової новизни.
2. Доцільно було б об’єднати семантичні методи ідентифікації шкідливих файлів для Windows PE і Linux ELF файлів в один і навести у вигляді алгоритму.
3. Наведені в роботі методи також бажано було б представити у вигляді алгоритмів, що покращило б їх цілісне сприйняття.
4. Бажано було б навести порівняння ефективності запропонованих методів крім табличного, ще й у графічному вигляді.
5. 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 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:

доктор технічних наук, професор,
професор кафедри інформаційних та
комп'ютерних систем
Національного університету
«Чернігівська політехніка» Сергій ЗАЙЦЕВ