ВІДГУК

офіційного опонента

завідувача кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, доктора технічних наук, професора, академіка Української академії наук Хлапоніна Юрія Івановича
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

Протягом останніх років, в умовах ведення кібервійни та кібертероризму, підприємства та корпорації часто стають жертвами кібератак, що завдають їм великих збитків та стають причиною переривання їх діяльності на певний час. Такі атаки все частіше спрямовуються на корпоративні мережі, що належать підприємствам, адже саме вони відіграють ключову роль у функціонуванні підприємств. У зв'язку із постійним розвитком кіберзлочинців та їх технік зламу, а також з наявністю людського фактору при роботі з корпоративними мережами, на даний час існує велика кількість різних загроз для безпеки компанії, які пов'язані з функціонуванням її корпоративної мережі. Тому своєчасне виявлення таких загроз та прогнозування ймовірностей їх експлуатації є ключовим елементом сучасних систем захисту від вторгнень.

Прийняття рішень при розподілі ресурсів щодо захисту корпоративних комп'ютерних мереж потребує оцінки типу та рівня критичності загрози, що зумовлює актуальність використання засобів експертних систем, зокрема методів експертних оцінок в інформаційних системах виявлення загроз. Для забезпечення кібербезпеки організації, необхідно реалізувати процес підтримки прийняття рішень захисту мереж, враховуючи інформацію про наявні вразливості, їх тип та критичність, а також активи мережі, що є цілями зловмисника . Таким чином, розробка інформаційної технології прогнозування та виявлення загроз для корпоративних комп'ютерних мереж засобами експертних систем є актуальним науковим завданням.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконана в рамках визначених задач міжнародного науково-дослідного проекту «Cyber Rapid Analysis for Defense Awareness of Realtime Situation – CyRADARS» відповідно грантової програми NATO SPS, (grant 21 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).

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 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 імпортів 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 модулей ідентифікації шкідливого ПЗ та рушій висновків, що дозволяють виконати прогнозування ймовірності реалізації визначених векторів вразливостей для підтримки прийняття рішень щодо реагування на загрози.

Основні результати дослідження полягають у розробці інформаційної технології, яка містить засоби експертних систем та комплексно враховує результати застосування запропонованих методів виявлення та прогнозування загроз на основі моделей машинного навчання та статистичних моделей, що дозволило підвищити точність, F1-міру та зменшити час виявлення загроз, зокрема шкідливого ПЗ та DDoS атак.

Практичним результатом дисертації є інформаційна система виявлення та прогнозування загроз, що містить модулі експертної системи та моделі виявлення загроз. Система побудована на основі інформаційної технології, запропонованої в дисертаційному дослідженні, та може бути використана спеціалістами з кіберзахисту організації для забезпечення процесу підтримки прийняття рішень щодо захисту корпоративних комп'ютерних мереж.

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій підтверджується глибоким аналізом наукових праць українських та закордонних дослідників у відповідних сферах, нормативно-правових актів, міжнародних кібербезпекових стандартів та інформаційних ресурсів мережі Internet. Наукові результати дисертації були опробовані, доповідались на

міжнародних та всеукраїнських конференціях та підтверджуються довідками про впровадження. Це загалом підтверджує достатній рівень практичної значимості та обґрунтованості дослідження.

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 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 та перевірки роботи на текстові співпадіння з існуючими роботами, можна зробити висновок, що дисертаційна 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 вказані посилання) та використанням загальноприйнятої наукової термінології. Використані ідеї, результати і тексти інших авторів мають належні посилання та відповідне джерело.

Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою.

Текст дисертації викладено логічно та послідовно та оформлено відповідно до чинних норм. Автор дотримується наукового стилю та використовує загальноприйняту термінологію.

Структура та зміст дисертації

Дисертаційна робота складається зі вступу, 4 розділів, переліку умовних скорочень зі 143 джерел та 4 додатків. Загальний обсяг дисертації 188 сторінок.

У вступі дисертації обґрунтовано актуальність теми дослідження, сформульовано мету, завдання та методологію дослідження, а також наведено наукову новизну та розкрито зв’язок з науковими програмами кафедри.

У першому розділі проведено аналіз основних кіберзагроз для корпоративних комп’ютерних мереж, методів їх виявлення та прогнозування, а також їх характеристику. Автор проаналізував підходи до виявлення та прогнозування загроз з використанням моделей машинного навчання, засобами експертних систем та статистичних моделей. Також було надано розгорнутий порівняльний аналіз існуючих досліджень у сфері виявлення та прогнозування загроз для корпоративних мереж та для окремих їх вузлів. На основі аналізу існуючих досліджень, стандартів та фреймворків в сфері кібербезпеки, було сформовано модель кіберзагрози для корпоративної комп’ютерної мережі та

модель процесу її виявлення та прогнозування. Було виділено основні сутності, що входять до моделі та кроки процесу виявлення та прогнозування ймовірності експлуатації загрози.

У другому розділі було запропоновано методи виявлення та прогнозування загроз, а також інформаційну технологію для забезпечення підтримки прийняття рішень щодо захисту корпоративних мереж. Було запропоновано метод вибору та обробки секції Linux ELF файлів з використанням методів NLP та моделей машинного навчання, що дає найкращу точність класифікації файлових загроз. Метод було порівняно з існуючим методом інших авторів, в результаті чого було підтверджено статистичну значущість покращення точності та F1 міри з використанням запропонованого в даному дисертаційному дослідженні методу. Було запропоновано удосконалений метод виявлення DDoS атак з використанням поєднання EWMA статистики та моделі Isolation Forest, що дозволяє виявляти як DDoS атаки з періодичним однаковим інтервалом, так і атаки з різним інтервалом. Здатність методу виявляти DDoS було підтверджено експериментально. Також автором удосконалено метод ідентифікації шкідливих Windows PE файлів з використанням моделі word2vec та ансамблю дерев рішень, що дозволило отримати покращену точність та F1-міру класифікації файлових загроз, порівняно з існуючими методами. Новизна запропонованих методів була обґрунтована та підкріплена порівнянням з існуючими дослідженням у сфері кібербезпеки. Для прогнозування ймовірностей загроз запропоновано метод на основі побудови мережі Баєса для різних параметрів мережевого трафіку, ефективність якого експериментально підтверджена на наборі даних CSE-CIC-IDS2018. Результати роботи запропонованих у дисертаційному дослідженні методів комплексно враховуються в інформаційній технології виявлення та прогнозування загроз. Технологія містить модуль введення експертних оцінок для оцінки виявлених та прогнозованих загроз на основі стандарту CVSS та рушій висновків для пошуку можливих стратегій зловмисника з експлуатації виявлених загроз та оптимальних стратегій протидії загрозам. Для рушія висновків було запропоновано використання теорії ігор з використанням ітераційного методу вирішення антагоністичних ігор між кіберзлочинцем та спеціалістом з кібербезпеки та формування ймовірних стратегій експлуатації загроз та захисту.

В третьому розділі автор виконав моделювання інформаційної технології з використанням діаграм IDEF0, надавши 3 рівні деталізації процесів виявлення, прогнозування загроз та підтримки прийняття рішень щодо забезпечення захисту корпоративних комп’ютерних мереж. Також було створено UML діаграму для візуалізації взаємодії експертів та користувачів з розробленою технологію, що дозволяє більш чітко зрозуміти сценарії її використання.

В четвертому розділі було імплементовано запропоновану інформаційну технологію у вигляді MVP інформаційної системи виявлення та прогнозування загроз. Було представлено інтерфейс системи. У віртуальному середовищі GNS3 створено корпоративну комп’ютерну мережу, що дозволило реалізувати та експериментально підтвердити ефективність запропонованих у другому розділі методів виявлення та прогнозування загроз. Точність, час реагування та F1-міру

запропонованих методів було порівняно з існуючим антивірусним ПЗ, що показало покращення показників існуючих методів.

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

Оприлюднення результатів дисертаційної роботи

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 у періодичному науковому журналі, що індексуються у базі даних Scopus.

Також результати дослідження були представлені на 3 наукових фахових конференціях.

У наведених публікаціях у повній мірі представлено результати, отримані в дисертаційній роботі. Порушень академічної доброчесності в них не виявлено. Особистий внесок здобувача у публікаціях свідчить про його авторство у наукових досягненнях, зазначених в результатах дисертаційної роботи.

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

Недоліки та зауваження до дисертаційної роботи

1. В дисертаційній роботі для досягнення мети дослідження поставлене наступне завдання: «Розробка методу виявлення мережевих аномалій з можливістю детекції DDoS атак з використанням статистичних методів». За змістом роботи, не зовсім зрозуміло, який метод розроблений в рамках цього завдання. Всі описані методи мають інші назви.
2. Реалізація завдання «Розробка методу прогнозування виникнення загроз з використанням мереж Баєса для корпоративної комп'ютерної мережі» не міститься у наведеній науковій новизні, хоча сам метод представлений в розділі 2 дисертаційної роботи. Не зовсім зрозуміло, для чого було поставлене таке завдання і чи виконано воно в повному обсязі, оскільки в розділі 2 міститься тільки обмежений опис його реалізації.
3. Не зовсім зрозуміло, чи розроблена модель комплексної інформаційної системи (рисунок 2.28), являє собою модель інформаційної технології виявлення та прогнозування загроз для корпоративної комп'ютерної мережі яка заявлена в науковій новизні. Відмінність полягає в тому, що інформаційна система являє собою реалізацію інформаційної технології.
4. В роботі недостатньо обґрунтовано, чому дослідження велись саме для корпоративних комп'ютерних мереж. Які їх особливості враховані? Не зрозуміло, чи будуть результати прийнятними для інших видів комп'ютерних мереж.
5. При розробці методу визначення секції Linux ELF файлу для ідентифікації шкідливого ПЗ недостатньо обґрунтованим є використання методу TF-IDF

для векторизації дизасембльованих програмних секцій бінарних файлів. Можна було б використати інші методи, такі як bert, glove, word2vec, тощо та порівняти їх ефективність для вирішення даної задачі.

Висловлені зауваження не впливають на загальну позитивну оцінку наукової новизни, теоретичного рівня та прикладної цінності дисертаційного дослідження Міщенка Максима Валерійовича.

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» є завершеною науковою працею, в якій отримані обґрунтовані наукові результати.

Дисертація відповідає вимогам, які висуваються до дисертаційних робіт, зокрема зміст загалом відповідає галузі знань 12 "Інформаційні технології", спеціальності 122 "Комп'ютерні науки", та «Вимогам до оформлення дисертації», затвердженим Наказом Міністерства освіти і науки України від 12.01.2017 р. № 40 (із змінами, внесеними згідно з Наказом Міністерства освіти і науки України від 31.05.2019 № 759) та «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 (в редакції постанови Кабінету Міністрів України від 19 травня 2023 р. № 502).

Здобувач Міщенко Максим Валерійович заслуговує на присудження наукового ступеню доктора філософії зі спеціальності «Комп'ютерні науки».

Офіційний опонент:

завідувач кафедри кібербезпеки та
комп'ютерної інженерії Київського
національного університету
будівництва і архітектури
доктор технічних наук, професор Юрій ХЛАПОНІН

«01» квітня 2025 року

Підпис Хлапоніна Ю.І. засвідчую:
Секретар вченої Ради
Київського національного університету будівництва і архітектури

М.П.

Микола КЛИМЕНКО