ВИСНОВОК

Національного університету «Чернігівська політехніка» про наукову новизну, теоретичне та практичне значення результатів дисертації Міщенка Максима Валерійовича на тему: «Прогнозування та виявлення загроз для корпоративних комп'ютерних мереж засобами експертних систем» поданої на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 - Комп'ютерні науки

1. Актуальність теми дослідження та її зв'язок з науково-дослідними роботами

У сучасному світі кібербезпека займає провідне місце у захисті цифрових даних організацій. Більшість сучасних компаній, як приватних, так і державних, використовують корпоративні комп'ютерні мережі у своїй діяльності, які часто стають об'єктами атак, що завдають значних фінансових та репутаційних збитків організаціям-жертвам. Ефективний захист корпоративних мереж залежить від своєчасного виявлення та прогнозування можливих загроз, і зумовлює необхідність розвитку моделей та методів захисту корпоративних мереж.

Одним із головних викликів кібербезпеки є оперативне реагування як на відомі, так і на нові загрози. У разі, коли загрози вже ідентифіковані, їхні хеш-суми зберігаються у базах даних сигнатур антивірусного програмного забезпечення та IDS-систем, що полегшує їхнє виявлення і нейтралізацію. Проте зловмисники постійно модифікують існуючі загрози, додаючи нову логіку. Це зумовлює необхідність використання методів, які можуть виявляти мережеві аномалії, самонавчатись та ідентифікувати знайомі шаблони у нових загрозах. До таких методів належать статистичні моделі та алгоритми машинного навчання.

Прийняття рішень щодо розподілу ресурсів для захисту вимагає оцінки рівня критичності загроз. Це зумовлює важливість використання експертних систем, зокрема методів експертної оцінки в системах виявлення загроз. Більшість досліджень у цій галузі зосереджені на використанні нечіткої логіки або нейронних мереж для створення рушіїв висновків. Як

альтернативу, в роботі запропоновано застосування моделей теорії ігор у якості рушія експертних систем. Такий підхід дозволяє оцінювати ймовірності експлуатації загроз зловмисниками, генерувати рекомендації з кіберзахисту та пропонувати оптимальні стратегії для фахівців із кібербезпеки.

Таким чином, актуальним науковим завданням є розробка моделей та методів для виявлення та прогнозування загроз у корпоративних комп'ютерних мережах із використанням експертних систем, що сприятиме підвищенню оперативності прийняття рішень щодо реагування на існуючі та потенційні загрози.

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

2. Мета і задачі дослідження

Метою дисертаційного дослідження є підвищення оперативності виявлення загроз та забезпечення підтримки прийняття рішень щодо реагування на наявні та можливі вразливості корпоративних комп'ютерних мереж.

Для досягнення мети дослідження в дисертації сформульовані та вирішені наступні завдання:

1. Аналіз існуючих кіберзагроз для корпоративних комп'ютерних мереж і методів їх виявлення та прогнозування.

2. Розробка методів ідентифікації шкідливого програмного забезпечення для UNIX-подібних систем та систем сімейства Windows на основі семантичного аналізу та моделей машинного навчання.

3. Розробка методу виявлення мережевих аномалій з можливістю детекції DDoS атак з використанням статистичних методів.

4. Розробка методу прогнозування виникнення загроз з використанням мереж Басса для корпоративної комп'ютерної мережі.

5. Розробка моделі комплексної інформаційної технології для виявлення кіберзагроз та формування рекомендацій щодо вибору оптимальних стратегій кіберзахисту з використанням експертних систем.

6. Підтвердження ефективності запропонованих методів та комплексної технології в розробленій системі виявлення та прогнозування кіберзагроз для корпоративної комп'ютерної мережі.

3. Наукові положення, розроблені особисто здобувачем, та їх новизна.

Дисертаційна робота виконана здобувачем особисто, містить наукові положення і результати, які характеризуються як науково значущі з урахуванням потреб теорії та практики за спеціальністю 122–Комп'ютерні науки.

Основні результати дослідження, які становлять його наукову новизну, полягають у наступному:

Вперше:

- 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.

- 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;

Набуло 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 дисертаційної роботи, що характеризують новизну дослідження, полягають у наступному:

1) Запропонований метод визначення секції Linux ELF файлу UNIX-подібних операційних систем містить процес семантичного аналізу та ідентифікації шкідливих Linux ELF фалів. Метод полягає у вибору секції файлу та розміру n-gram, що дає найвищу точність класифікації. Метод протестовано з використанням набору шкідливих та безпечних файлів розміром 6804 файлів та отримано найкращу точність 97% та F1-score 0.97 для моделі опорних векторів з градієнтним спуском.
2) Розроблений метод ідентифікації шкідливих Windows PE файлів з використаням секції Import Table та методу word2vec. Векторизовані дані передаються для класифікації за допомогою моделей опорних векторів, ансамблю дерев рішень та багатошарового перцептрону. Виконане тестування методу на наборі даних шкідливих та нешкідливих файлів розміром 16862 файли показало, що найкращу точність, F1-міру показала модель ансамблю дерев рішень. Порівняння отриманих результатів з результатами існуючих досліджень виявили покращення показників F1-міри та часу класифікації.

3) Розроблений метод виявлення загроз з використанням EWMA-статистики та Isolation Forest. Застосування даного методу дозволяє виявляти як контекстні так і точкові аномалії. Дієвість методу експериментально перевірено та підтверджено в ході симуляцій декількох послідовних DDoS атак
4) Запропонована модель інформаційної технології виявлення та прогнозування загроз для корпоративної комп'ютерної мережі містить модулі експертної системи. Такі модулі забезпечують прогнозування ймовірностей експлуатації загроз та формування рекомендацій щодо вибору оптимальних стратегій кіберзахисту.
5) Для прогнозування ймовірностей виникнення загроз для корпоративної комп'ютерної мережі використано мережі Баєса, що забезпечує підтримку прийняття рішень щодо стратегій реагування на можливі кіберзагрози.
6) Виконано проектування інформаційної системи з використанням діаграм IDEF0 та розробкою функціональної моделі та її декомпозиції. Проведені в роботі експерименти показали зменшення часу виявлення загроз для Linux ELF та Windows PE файлів, а також підвищення F1-міри виявлення шкідливих Linux ELF файлів.

4. Обґрунтованість та достовірність наукових положень, висновків рекомендацій

Зміст дисертаційної роботи побудовано на відповідному первинному матеріалі, аналіз та узагальнення якого дозволили сформулювати основні наукові положення, висновки та рекомендації.

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій підтверджується глибоким аналізом наукових досягнень українських та зарубіжних науковців у відповідній сфері, нормативно-правових актів, аналітичних матеріалів міжнародних організацій, інформаційних ресурсів мережі Internet, що дозволило компетентно виконати завдання, поставлені у дослідженні.

Основні положення, висновки та практичні рекомендації базуються на матеріалах власних досліджень автора, логічно випливають із матеріалів дисертації та є науково обґрунтованими і чітко сформульованими.

Для досягнення поставлених в дисертаційному дослідженні завдань було використано як загально наукові, так і спеціальні методи, а саме: методи моделювання функціональних діаграм IDEF0 для проектування інформаційної системи виявлення та прогнозування загроз для корпоративних комп'ютерних мереж, діаграми UML для моделювання варіантів використання системи експертами з кібербезпеки та інженерами з кіберзахисту. Для оцінки значення кількісної метрики CVSS для загроз корпоративним компютерним мережам, використано метод експертних оцінок. Також застосовано методи статистичного аналізу для виявлення аномалій мережевого трафіку, методи машинного навчання та методи NLP для ідентифікації шкідливих файлів.

5. Теоретичне та практичне значення результатів дисертаційного дослідження.

Науково-практичні розробки та рекомендації автора було впроваджено у практичну діяльність:

– у навчальному процесі Національного університету «Чернігівська політехніка» при проведенні лекцій та лабораторних робіт з дисципліни «Системи штучного інтелекту» – в процесі навчання бакалаврів спеціальності 121 – «Інженерія програмного забезпечення» на кафедрі інформаційних технологій та програмної інженерії (довідка про впровадження від 13.01.2025);

– в ТОВ "ДП «ЗАВОД РАПІД»" при виявленні існуючих файлових загроз на комп'ютерах в корпоративній комп'ютерній мережі та виконанні прогнозування ймовірності реалізації зловмисниками виявлених загроз (довідка про впровадження від 27.12.2024).

6. Апробація результатів дослідження.

Основні положення, результати та висновки дисертації доповідались на

3 наукових конференціях зокрема: XV міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем МОДС 2020», Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених «Новітні технології у науковій діяльності і навчальному процесі», XIV Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Юність науки – 2024».

7. Повнота викладення основних наукових результатів дисертації в публікаціях таособистий внесок у них автора.

Аналіз кількості наукових публікацій, повноти опублікування результатів дисертації та особистого внеску здобувача до всіх наукових публікацій, опублікованих самостійно й у співавторстві та зараховані за темою дисертації, засвідчив, що результати дослідження, викладені у дисертаційній роботі, отримані автором самостійно та повною мірою відображені в публікаціях, доповідалися та обговорювалися на науково-практичних конференціях.

Основні результати дисертаційного дослідження опубліковано здобувачем самостійно та в співавторстві в 8 наукових працях загальним обсягом 2,8 друк. Арк, з яких автору належить 2,4 друк.арк. Серед них 4 статті у наукових фахових виданнях України, обсягом 2,2 друк. арк., 1 з них включена до міжнародної наукометричної бази Scopus, обсягом 0,6 друк. арк., 3 праці апробаційного характеру обсягом 0,4 друк.арк. Результати роботи доповідалися на 3 всеукраїнських та міжнародних наукових конференціях.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. А.Г. Гребенник, О.В. Трунова, В.В. Казимир, М.В. Міщенко «Виявлення та прогнозування загроз для корпоративної комп'ютерної мережі.» *Технічні науки та технології, 2020. - № 2 – с.175–184.* (0,5 ум. друк. арк.)

(Особистий внесок здобувача: загальна архітектура системи прогнозування та виявлення загроз ККМ, аналіз методу виявлення кіберзагроз з використанням EWMA-статистики) (0,3 ум. друк. арк.)

2. Mishchenko M.V., Dorosh M.S.. "Semantic analysis and classification of malware for UNIX-like operating systems with the use of machine learning methods". Applied Aspects of Information Technology. 2022; Vol. 5, No. 4: 371-386, DOI: https://doi.org/10.15276/aait.05.2022.25. (0,6 ум. друк. арк.) (Особистий внесок здобувача: метод семантичного аналізу та класифікації шкідливого програмного забезпечення для UNIX-подібних систем) (0,5 ум. друк. арк.)
3. Mishchenko, M. V., Dorosh, M. S.. (2024). «An expert system of recommendations for combating cyber threats using CVSS metrics and game theory.» Вісник сучасних інформаційних технологій, 7(3), 284–295. https://doi.org/10.15276/hait.07.2024.20 (0,6 ум. друк. арк.) (Особистий внесок здобувача: експертна система рекомендації протидії загрозам з використанням метрик CVSS та теорії ігор) (0,5 ум. друк. арк.)
4. Міщенко, М. «Функціональна модель системи виявлення та прогнозування кіберзагроз для корпоративних комп'ютерних мереж з використанням експертних оцінок.» Технічні науки та технології – 2024. № 3 (37), - с. 143–152. https://doi.org/10.25140/2411-5363-2024-3(37)-143-152 (0,6 ум. друк. арк.)
5. Міщенко М.В., Гребенник А.Г., Трунова О.В.. "Прогнозування рівня загроз з використанням мереж Байєса" XV міжнародна науково-практична конференція математичне та імітаційне моделювання систем МОДС 2020. С. 120-123. Тези доповідей. (0,2 ум. друк. арк.) (Особистий внесок здобувача: дослідження існуючих методів прогнозування загроз з використанням мережі Баєса) (0,1 ум. друк. арк.)
6. Міщенко М.В. «Створення сервісу для виявлення шкідливих elf файлів за допомогою машинного навчання з використанням хмарних технологій aws» Всеукраїнська науково-практична конференція

студентів, аспірантів та молодих учених НОВІТНІ ТЕХНОЛОГІЇ У НАУКОВІЙ ДІЯЛЬНОСТІ І НАВЧАЛЬНОМУ ПРОЦЕСІ. – 2023 – с.107-108. Тези доповідей. (0,1 ум. друк. арк.)

7. Міщенко М.В. «Створення експертної системи генерації рекомендацій з протидії кібератакам з використанням теорії ігор.» XIV Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених ЮНІСТЬ НАУКИ – 2024 – с. 1175-1176. Тези доповідей. (0,1 ум. друк. арк.)

Статті у наукових фахових виданнях та виданнях, внесених до наукометричних баз:

1. Mishchenko, M., & Dorosh, M. (2025). Detection of Windows Portable Executable Malware using NLP Techniques and Proxy-server. International Journal of Computing, 23(4), 663-672. https://doi.org/10.47839/ijc.23.4.3765 (0,6 ум. друк. арк.) (Особистий внесок здобувача: метод ідентифікації шкідливих Windows PE файлів) (0,5 ум. друк. арк.) (SCOPUS)

8. Загальний висновок.

Дисертаційна робота Міщенка Максима Валерійовича на тему «Прогнозування та виявлення загроз для корпоративних комп'ютерних мереж засобами експертних систем» є оригінальним, самостійним, завершеним науковим дослідженням, що стосується актуальної проблематики і містить оригінальні підходи до розв'язання теоретичних та практичних завдань підтримки прийняття рішень щодо захисту корпоративних комп'ютерних мереж від кіберзагроз.

Основні положення, висновки та рекомендації дисертації містять елементи наукової новизни, є повністю обґрунтовані та аргументовані і отримали необхідну апробацію на науково-практичних конференціях. У публікаціях здобувача знайшли відображення всі положення дисертаційного дослідження. Зміст дисертації відповідає визначеній меті, поставлені здобувачем наукові завдання вирішені повною мірою, мету дослідження

досягнуто. Роботу виконано державною мовою.

За актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Міщенка Максима Валерійовича відповідає спеціальності 122-Комп'ютерні науки та вимогам «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)», затвердженого Постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (в редакції постанови Кабінету Міністрів України від 19 травня 2023 р. № 502), наукові публікації здобувача відповідають пункту 8 постанови Кабінету Міністрів України від 12 січня 2022 року № 44 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії».

Дисертація Міщенка Максима Валерійовича на тему «Прогнозування та виявленн загроз для корпоративних комп'ютерних мереж засобами експертних систем» може бути рекомендована до захисту у спеціалізовану вчену раду.

Головуючий
завідувач кафедри інформаційних
та комп'терних систем, к.т.н., доцент Роговенко А.І.

29.01.2025

Підпис Роговенка А.І. засвідчую
Начальник відділу кадрів Т.Ч. Ткаченко
«29» 01 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Чернігівська політехніка»
ВІДДІЛ КАДРІВ