Голові разової спеціалізованої
вченої ради
Національного університету
«Львівська політехніка»
д.т.н., професору
Опірському Івану Романовичу

ВІДГУК
офіційного опонента
доктора технічних наук, професора Смірнова Олексія Анатолійовича,
завідувача кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
на дисертаційну роботу

Журавчака Даниїла Юрійовича
«Удосконалення методів виявлення програм-вимагачів
в режимі реального часу»
подану до захисту на здобуття наукового ступеня доктора філософії за
спеціальністю 125 «Кібербезпека»
(галузь знань 12 «Інформаційні технології»)

1. Актуальність теми дисертаційної роботи.

Актуальність теми дисертаційної роботи Д.Ю. Журавчака "Удосконалення методів виявлення програм-вимагачів в режимі реального часу" є безсумнівною та підтверджується кількома факторами.

По-перше, програми-вимагачі стали однією з найпоширеніших та найнебезпечніших кіберзагроз останніх років. Вони завдають значних фінансових та репутаційних збитків організаціям усіх галузей, включаючи державні установи, медичні заклади, підприємства та освітні установи. Швидкий розвиток та еволюція програм-вимагачів роблять їх особливо небезпечними, оскільки традиційні методи захисту часто не встигають за новими загрозами.

По-друге, зростаюча кіберзлочинність, особливо в контексті війни в Україні, вимагає розробки та впровадження нових, більш ефективних методів виявлення та протидії програмам-вимагачам. Використання цих програм у кібервійні підкреслює їх потенційну небезпеку для національної безпеки та вимагає негайної реакції з боку наукової спільноти та фахівців з кібербезпеки.

По-третє, сучасні інформаційні системи стають все більш складними, що ускладнює їх захист від кіберзагроз. Програми-вимагачі використовують різноманітні вектори атак, включаючи фішинг, експлуатацію вразливостей програмного забезпечення та мережеві атаки. Для ефективної протидії цим загрозам необхідні комплексні підходи, які враховують усі аспекти кібербезпеки, від моніторингу системних подій до аналізу мережевого трафіку та поведінки процесів.

У дисертаційній роботі запропоновано інноваційний підхід до виявлення програм-вимагачів, що базується на використанні технології розширеного фільтра пакетів Берклі (eBPF) та моделей машинного навчання. Цей підхід дозволяє здійснювати моніторинг системних подій у режимі реального часу та

виявляти підозрілу активність на ранніх стадіях, що є критично важливим для запобігання атакам та мінімізації їх наслідків.

Таким чином, актуальність теми дисертаційної роботи підтверджується її спрямованістю на вирішення нагальної проблеми кібербезпеки, важливістю розробки нових методів захисту від програм-вимагачів та потенційним внеском у підвищення рівня кібербезпеки як в Україні, так і в світі.

2. Аналіз змісту дисертаційної роботи.

Дисертація Журавчака Д. Ю. є завершеною дослідницькою роботою, що містить анотацію, вступ, 4 розділи, висновки, список використаних джерел та додатки.

У **першому розділі** автор проводить глибокий аналіз проблеми, розглядаючи різні аспекти програм-вимагачів, їх класифікацію, історію розвитку, методи поширення та вплив на інформаційні системи. Особливу увагу приділено аналізу сучасного стану кіберзлочинності та використанню програм-вимагачів у кібервійнах.

Другий розділ присвячено використанню технології eBPF (extended Berkeley Packet Filter) для виявлення програм-вимагачів. Автор детально описує архітектуру eBPF, його можливості та переваги у контексті кібербезпеки. Зокрема, розглянуто використання eBPF для моніторингу системних викликів, файлової системи, мережевого трафіку та показників продуктивності.

У **третьому розділі** представлено створення інтегрованого методу аналізу вірусів-вимагачів на базі моделей машинного навчання. Автор розглядає різні моделі, такі як дерева рішень, метод опорних векторів та глибокі нейронні мережі, та обґрунтовує їх вибір для вирішення поставлених завдань. Детально описано процес формування наборів даних, навчання моделей та їх інтеграцію з eBPF.

У **четвертому розділі** представлено аналіз ефективності запропонованих рішень. Автор проводить експерименти з використанням розробленого симулятора атак програм-вимагачів та оцінює ефективність різних моделей машинного навчання. Результати експериментів підтверджують високу точність та швидкість виявлення загроз запропонованим методом.

У **висновках** дисертаційної роботи викладено основні результати та рекомендації щодо застосування створеної інтегрованої системи виявлення вірусів-вимагачів у режимі реального часу. Представлено та охарактеризовано кількісні та якісні метрики ефективності запропонованого рішення, а також надано рекомендації щодо впровадження запропонованих методів у практичних комп'ютерних системах.

Загалом, дисертаційна робота Д.Ю. Журавчака є вагомим внеском у галузь кібербезпеки. Запропонований метод виявлення програм-вимагачів має значний потенціал для практичного застосування та може бути використаний для підвищення рівня захисту інформаційних систем.

3. Наукова новизна одержаних результатів.

Науковою новизною роботи є розробка нових методів виявлення та протидії вірусам-вимагачам у режимі реального часу на основі сучасних технологій машинного навчання, а також інтеграція різних методів захисту для підвищення ефективності захисту комп'ютерних систем від цих шкідливих програм:

– **вперше розроблено методологію** дослідження кіберзлочинів, що використовує моделі Ізоляційного лісу, GPT та DevSecOps підхід. Дана

методологія, на відміну від існуючих, виявляє кібератаки на різні рівні інфраструктури інформаційної системи, включно з атаками сканування, ін'єкціями шкідливого коду, атаками типу Directory Traversal та виявленням аномалій з порушенням логіки додатків, які можуть залишатися непоміченими класичними SIEM системами за відсутності поведінкових сигнатур, гарантуючи високий рівень безпеки;

– **вперше розроблено модель** інтегрованої системи збору даних для виявлення вірусів-вимагачів, що об'єднує застосування eBPF для моніторингу системних викликів, файлової та криптографічної активності, аналізу мережевого трафіку та процесів. Ця система забезпечує унікальний набір даних (features), які використовуються для ефективного ідентифікування потенційних загроз в режимі реального часу;

– **вперше запропоновано комплексну модель** класифікації вірусів-вимагачів з використанням ансамблю дерев рішень та випадкового лісу, що дозволяє з високою точністю розрізняти «безпечні» та «небезпечні» програми на основі аналізу складних поведінкових шаблонів та криптографічної активності;

– **вперше запропоновано методологію** застосування глибоких нейронних мереж для ідентифікації складних шаблонів у даних, зібраних модулями eBPF, що представляють поведінку вірусів-вимагачів, забезпечуючи новий рівень точності виявлення невідомих або еволюціонованих загроз;

– **отримали подальший розвиток методи** виявлення кіберзагроз за допомогою аналізу мережевого трафіку з використанням eBPF, що значно підвищує швидкість та точність ідентифікації потенційних атак вірусів-вимагачів у порівнянні з традиційними підходами;

– **удосконалено метод** симуляції кібератак за допомогою моделі емуляцій дій шахрая для тестування та оцінки ефективності розроблених моделей, одночасно, включаючи запуск вірусів-вимагачів у контрольованому лабораторному середовищі. Це дозволило детально аналізувати реакцію моделей на різноманітні сценарії атак та оптимізувати їх для максимальної ефективності;

– **отримали подальший розвиток методики** порівняльного аналізу та оцінки ефективності математичних апаратів виявлення та протидії програмам-вимагачам, за допомогою метрики MCC (коефіцієнту кореляції Метью), що виявився ефективним для оцінювання моделей, які працюють з незбалансованими даними, характерними для сценаріїв кіберзагроз типу вірусів-вимагачів.

4. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати.

Наукові результати, отримані автором, можуть бути використані при розробці, побудові та впровадження систем та платформ менеджменту інформаційної безпеки. Розроблені методи можуть бути використані для підвищення ефективності систем моніторингу та виявлення загроз у реальному часі. Запропоновані підходи дозволяють підвищити точність і швидкість виявлення загроз, що сприяє покращенню кібербезпеки інформаційних систем.

Результати дисертаційної роботи Журавчака Д. Ю. впроваджені у навчальний процес кафедри «Захист інформації» Національного університету «Львівська політехніка» при вивченні дисципліни «Міжнародні стандарти з

кібербезпеки» для студентів першого рівня вищої освіти напрямку підготовки 125 «Кібербезпека», спеціалізації «Управління інформаційною безпекою».

5. Ступінь обґрунтованості наукових положень дисертації, їх достовірність та новизна.

Наукові положення дисертації є добре обґрунтованими та підтверджуються результатами експериментів, проведених автором. Використання сучасних методів машинного навчання та технології eBPF для виявлення програм-вимагачів є інноваційним підходом, що підтверджує новизну дослідження.

Дисертант детально описує процес розробки та реалізації запропонованих методів, включаючи збір та підготовку даних, вибір та навчання моделей, а також їх інтеграцію з eBPF. Він також надає результати експериментів, які демонструють високу ефективність запропонованого підходу у виявленні та протидії програмам-вимагачам.

Автор обговорює обмеження свого дослідження та пропонує напрямки для подальшої роботи, що свідчить про його наукову доброчесність та розуміння складності проблеми.

Загалом, наукові положення дисертації є обґрунтованими, достовірними та новими, що підтверджується детальним описом методів дослідження, результатами експериментів та аналізом отриманих даних.

6. Практичне значення одержаних результатів полягає у можливості використання розроблених методів та інструментів для ефективного виявлення та протидії вірусам-вимагачам у режимі реального часу, що дозволить підвищити рівень захисту комп'ютерних систем від цих загроз. Результати дослідження можуть бути корисними для фахівців з інформаційної безпеки, розробників антивірусного програмного забезпечення, а також для широкого кола користувачів комп'ютерних систем:

– використання розробленого комплексного методу аналізу даних на рівні ядра та ідентифікації програм-вимагачів із використанням фільтру eBPF, що значно підвищує швидкість та точність виявлення кіберзагроз. Впровадження цього методу у системи кібербезпеки дозволяє оперативно відслідковувати та реагувати на підозрілі зміни в системних викликах, файловій активності та мережевому трафіку, сприяючи своєчасному виявленню атак;

– використання розробленої моделі класифікації на основі ансамблю дерев рішень та випадкового лісу продемонструвало підвищену точність у виявленні шкідливих програм, досягаючи в середньому точності вище 95,0% і F1-метрики 97,7%, що є значним внеском у розвиток інструментів кібербезпеки;

– застосування методології глибоких нейронних мереж для аналізу складних шаблонів даних демонструє передовий підхід до виявлення новітніх кіберзагроз. Розроблені моделі забезпечили точність ідентифікації на рівні 97,8%, прецизійність 96,9% та F1-метрику 97,7%, значно покращуючи аналітичні можливості комп'ютерних систем і забезпечуючи надійне виявлення невідомих раніше загроз та вірусів-вимагачів, що еволюціонують;

– проведені експерименти у контрольованому лабораторному середовищі підтвердили високу точність розроблених моделей, де модель на базі глибоких нейронних мереж продемонструвала точність до 97,8% і коефіцієнт кореляції Метьюса 0,95, що вказує на високий рівень адекватності та надійності виявлення кіберзагроз.

7. Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дисертаційної роботи Журавчака Даниїла Юрійовича викладено у чотирнадцяти наукових публікаціях, а саме: семи статтях у наукових фахових виданнях України та восьми матеріалів конференцій, з яких три входить до міжнародної наукометричної бази Scopus.

Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів.

8. Оцінка структури дисертації, її мови та стилю викладення.

Дисертація за структурою, мовою та стилем викладення оформлена відповідно до вимог МОН України, що висуваються до подібного роду наукових робіт. Дисертація написана грамотною українською мовою з використанням сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним. Зміст наукових праць доповнює основні положення дисертації.

У дисертаційній роботі відсутні порушення академічної доброчесності. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Ознайомлення з текстом анотації дає змогу констатувати, що її зміст повною мірою відображає основні положення і висновки дисертації та не містить зайвої інформації.

9. Зауваження та дискусійні положення щодо змісту роботи.

Незважаючи на загальне позитивне враження від дисертаційної роботи, слід зазначити деякі зауваження та виділити окремі положення роботи, що викликають дискусії:

- У розділі 1.3 дисертаційної роботи представлено широкий огляд методів виявлення та протидії програмам-вимагачам, проте деякі з них описані недостатньо детально. Наприклад, методи статичного та динамічного аналізу згадані, але не розкриті повною мірою. Більш детальний опис цих методів, їх переваг та недоліків дозволив би краще зрозуміти контекст дослідження та обґрунтованість вибору eBPF та машинного навчання.
- Хоча автор у розділі 2.8 детально описує використання eBPF для моніторингу різних аспектів системи (системні виклики, файлові операції, мережевий трафік), недостатньо уваги приділено інтеграції цих даних. Зокрема, незрозуміло, як дані з різних модулів eBPF об'єднуються та аналізуються разом для виявлення складних патернів поведінки програм-вимагачів. Більш детальний опис цього процесу інтеграції та аналізу даних був би корисним.
- У розділі 4.3 представлено результати експериментів з використанням різних моделей машинного навчання, але бракує порівняння їх ефективності з іншими сучасними методами виявлення програм-вимагачів. Наприклад, було б цікаво порівняти запропонований підхід з методами, що базуються на аналізі поведінки користувачів або на використанні антивірусних баз даних.
- Автор у розділі 2.9 приділяє значну увагу використанню eBPF на платформі Linux, але розгляд можливості його застосування на інших операційних системах, таких як Windows або macOS є мінімальним. Автор лише описує процес міграції модулів, але не надає увагу їх тестування та роботи. Враховуючи поширеність цих систем, дослідження можливостей eBPF для виявлення програм-вимагачів на них могло б бути корисним доповненням до роботи.

• Хоча в дисертації в розділі 4.3 обговорюються питання оптимізації моделей машинного навчання та зменшення їх впливу на продуктивність системи, не надано конкретних рекомендацій щодо вибору оптимальної моделі для різних сценаріїв використання. Більш детальний аналіз компромісу між точністю виявлення та використанням ресурсів допоміг би практикам зробити обґрунтований вибір моделі для своїх потреб.

Водночас, висловлені зауваження та пропозиції мають дискусійний характер, є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової й практичної цінності.

Загальні висновки щодо дисертаційної роботи

Загальні висновки щодо дисертаційної роботи Д.Ю. Журавчака "Удосконалення методів виявлення програм-вимагачів в режимі реального часу" дозволяють стверджувати, що дана робота є актуальним та завершеним науковим дослідженням, яке має значний потенціал для вирішення нагальної проблеми кібербезпеки.

Отримані в ході дослідження наукові та практичні результати свідчать про високу ефективність запропонованого підходу. Розроблена автором система виявлення програм-вимагачів демонструє високу точність та швидкість виявлення загроз, що є критично важливим для мінімізації потенційних збитків від кібератак.

Зміст дисертаційної роботи «Удосконалення методів виявлення програм-вимагачів в режимі реального часу» відповідає обраній темі та забезпечує досягнення поставленої мети. Дослідження відповідає вимогам порядку присудження ступеня доктора філософії, а його автор, Журавчак Даниїл Юрійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Офіційний опонент:

доктор технічних наук, професор,
завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор,

Олексій СМІРНОВ

Підпис доктора технічних наук, професора, завідувача кафедрою кібербезпеки та програмного забезпечення, Центральноукраїнського національного технічного університету Смірнова Олексія Анатолійовича засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету
кандидат технічних наук, доцент

Андрій ТИХИЙ