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

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

кандидата технічних наук, доцента, Соколова Володимира Юрійовича,
доцента кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету імені Бориса Грінченка
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.

Розробка та вдосконалення методів виявлення програм-вимагачів у 2024 році є надзвичайно актуальними, враховуючи постійне зростання та ускладнення кіберзагроз у глобальному масштабі. У сучасному світі, де інформаційні технології займають центральне місце у всіх сферах життя, захист інформаційних активів стає пріоритетним завданням для будь-якої організації. Це вимагає від бізнесу та державних установ впровадження передових методів захисту інформаційних активів.

За останні кілька років спостерігається стрімке зростання кількості атак вірусів-вимагачів на різні організації, включаючи компанії, установи, медичні заклади, освітні установи та державні інституції. Наприклад, у 2020 році велика

кількість лікарень, що працювали з пацієнтами з COVID-19, були атаковані вірусами-вимагачами, що призвело до тимчасової недоступності медичної допомоги, що у окремих випадках призвело до летального результату. Цей випадок підкреслює критичну важливість наявності ефективних засобів захисту від кіберзагроз.

Екосистема кіберзлочинності продовжує стрімко розвиватися. Одним із визначальних факторів ландшафту програм-вимагачів у 2022-23 роках є триваюча війна в Україні, яка має особливий вплив з огляду на високу концентрацію кіберзлочинних угруповань з Росії, що куруються в головних управліннях розвідки. У перші місяці після вторгнення зріс масштаб та напрям програм-вимагачів та інших кіберзлочинів, у сторону урядового сегменту. Це створює додаткові виклики для національної безпеки та вимагає розробки нових ефективних засобів протидії.

Крім того, сучасні операційні системи та комп'ютерні мережі щодня стають все складнішими, що ускладнює захист від кіберзагроз. Зростання складності корпоративних мереж та широке використання хмарних технологій створює нові виклики для забезпечення мережевої безпеки. Віруси-вимагачі часто розповсюджуються через мережеві з'єднання, використовуючи слабкі місця у мережевій інфраструктурі. Ефективний захист вимагає комплексного підходу до мережевої безпеки, включаючи сегментацію мережі, шифрування трафіку та застосування сучасних систем виявлення та запобігання вторгненням.

Розробка та впровадження нових методів виявлення та протидії вірусам-вимагачам у режимі реального часу є надзвичайно важливими завданнями для забезпечення безпеки інформації та захисту комп'ютерних систем. Вдосконалення методів виявлення та протидії вірусам-вимагачам у режимі реального часу може допомогти зменшити ризик втрати даних та забезпечити швидку реакцію на потенційні загрози. Запропоновані у дисертаційній роботі методи виявлення з використанням технології eBPF та моделей машинного навчання мають значний потенціал для підвищення ефективності захисту інформаційних систем.

Таким чином, тема дисертації Журавчака Д. Ю. «Удосконалення методів виявлення програм-вимагачів в режимі реального часу» є надзвичайно актуальною та важливою для сучасного суспільства. Впровадження результатів дослідження сприятиме підвищенню рівня кібербезпеки, забезпеченню захисту критичної інфраструктури та мінімізації втрат від кіберзагроз.

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 **вступі** автором обґрунтовано актуальність теми, сформульовано цілі та завдання дослідження, визначено наукову новизну та практичну цінність результатів дослідження, презентовано дані про апробацію та публікацію результатів дисертаційної роботи.

У першому розділі «Аналіз проблеми виявлення та протидії програмам-вимагачам» автор детально аналізує віруси-вимагачі. Розглянуто класифікацію, історію розвитку, методи розповсюдження та вплив на інформаційні системи цих шкідливих програм. Проведено аналітичний огляд сучасного стану кіберзлочинності з акцентом на вплив вірусів-вимагачів, із особливою увагою до тенденцій та потенційних загроз. У цьому розділі також обґрунтовується вибір напряму дослідження та постановка завдань дисертації.

У другому розділі «Використання eBPF для виявлення програм-вимагачів» здійснено глибокий аналіз технології eBPF (Extended Berkeley Packet Filter) та її можливостей у контексті боротьби з програмами-вимагачами. Розглянуто архітектуру eBPF, її ключові можливості та потенціал для ефективного виявлення та нейтралізації загроз. Особлива увага приділена інтеграції алгоритмів машинного навчання з eBPF для підвищення ефективності виявлення зловмисних дій. Розділ завершується формулюванням комплексного підходу до використання eBPF для виявлення програм-вимагачів в режимі реального часу, включаючи детальний розгляд методології розробки та імплементації модулів на основі eBPF для моніторингу системних викликів, файлової та мережевої активності.

У третьому розділі «Створення інтегрованого методу аналізу вірусів-вимагачів на базі моделей машинного навчання» розглянуто розробку та впровадження ефективних методів аналізу даних для виявлення програм-вимагачів, зосереджуючись на використанні моделей машинного навчання. Детально досліджено архітектуру інтегрованої системи виявлення вірусів-вимагачів, яка базується на використанні модулів eBPF та аналізу даних за допомогою машинного навчання. Особлива увага приділена оптимізації алгоритмів для підвищення точності виявлення та зменшення хибних спрацьовувань.

У четвертому розділі «Аналіз ефективності запропонованих рішень» представлено результати експериментальних досліджень, які підтверджують високу ефективність запропонованих методів виявлення програм-вимагачів. Проведено порівняльний аналіз з традиційними методами виявлення, що показав значне покращення в точності та швидкості реагування на загрози. Також розглянуто питання інтеграції розроблених методів з існуючими системами безпеки, такими як SIEM та EDR, що дозволить підвищити рівень захисту від програм-вимагачів.

У висновках дисертаційної роботи викладено основні результати та рекомендації 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.

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.

Наведені в дисертації результати базуються на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванню прийнятих припущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується практичною реалізацією методології виявлення та протидії програмам-вимагачам.

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.

В цілому, позитивно оцінюючи дисертаційне дослідження, необхідно зробити певні зауваження та вказати на окремі положення роботи, що викликають дискусію:

– у розділі 1.4 проведено аналіз кількох популярних методів виявлення та протидії програмам-вимагачам. Однак, бракує більш детального обґрунтування вибору саме цих методів та критеріїв, за якими вони були обрані. Доцільно було б розширити цей перелік за рахунок інших популярних підходів, щоб зробити розроблену методологію ще більш універсальною. Наприклад, можна було б використати методи, що враховують різні аспекти атак та різноманітні шляхи розповсюдження програм-вимагачів;

– у розділі 2.1 проведено дослідження і порівняння технології eBPF та інших методів моніторингу. Однак, не надається конкретних рекомендацій для проведення переходу до нових технологій. Наявна таблиця порівнянь демонструє відповідність між підходами, проте бракує конкретних рекомендацій щодо дій, які необхідно здійснити для ефективного впровадження нових технологій у існуючі системи. Варто було б навести ці рекомендації для полегшення практичного застосування результатів;

– у розділі 4.3 наведено показники ефективності методології, що базуються на часі виявлення загроз у реальних умовах. При обчисленні цього показника доцільності порівняння з існуючими методами, наведені дані мають певну суб'єктивність, що ускладнює надання більш детального кількісного обґрунтування. Процес виявлення загроз у різних організаціях має певні відмінності через контекст організацій, їх розмір, наявну матеріально-технічну базу тощо. Тому обчислення даного показника є досить приблизним і певною мірою суб'єктивним. Разом з тим, він все ж таки демонструє ефективність запропонованих методів у порівнянні з традиційними;

– у розділі 4.4 проведено аналіз практичної реалізації запропонованих методів у реальних умовах. Однак, наведені результати базуються переважно на прикладах з окремих організацій, що може обмежити репрезентативність даних. Вартим було б збільшити кількість прикладів практичного застосування методів у різних умовах для підвищення рівня довіри до результатів дослідження;

– розроблені методи моніторингу та виявлення програм-вимагачів на базі eBPF та машинного навчання мають значний потенціал, проте відсутня детальна оцінка впливу цих методів на продуктивність систем. У роботі не наведено конкретних даних щодо використання процесорних та пам'яттєвих ресурсів при впровадженні розроблених методів у реальних умовах експлуатації. Це ускладнює оцінку практичної доцільності застосування методів у високонавантажених системах. Доцільно було б надати детальні результати тестування продуктивності розроблених методів у різних сценаріях використання для забезпечення балансу між ефективністю виявлення загроз та оптимальним використанням системних ресурсів.

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.

Дисертаційна робота Журавчака Даниїла Юрійовича «Удосконалення методів виявлення програм-вимагачів в режимі реального часу» є завершеним, самостійним та цілісним науковим дослідженням, що містить наукову новизну та

практичну цінність отриманих результатів. Робота дозволяє значно підвищити ефективність виявлення та протидії програмам-вимагачам у сучасних інформаційних системах.

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
доцент кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка
к.т.н., доцент Володимир СОКОЛОВ

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
Соколова В.
(ПІБ)
ЗАСВІДЧУЮ
Відділ. справ. В.К.
(посада)