РЕЦЕНЗІЯ

Кандидата технічних наук, доцента,
доцента кафедри захисту інформації
Совина Ярослава Романовича
Національного університету «Львівська політехніка»
на дисертацію
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»)

Актуальність теми дисертації.

Актуальність дисертаційної роботи Д.Ю. Журавчака "Удосконалення методів виявлення програм-вимагачів в режимі реального часу" обумовлена постійно зростаючою загрозою з боку програм-вимагачів, які завдають значних фінансових та репутаційних збитків організаціям усіх видів. Особливо на тлі зростаючої кіберзлочинності та активного використання програм-вимагачів у кібервійнах, проблема їхнього своєчасного виявлення та нейтралізації набуває особливої актуальності.

У дисертації запропоновано інноваційний підхід до вирішення цієї проблеми шляхом інтеграції технології eBPF (розширений фільтр пакетів Берклі) та моделей машинного навчання. Цей комплексний підхід дозволяє здійснювати моніторинг системних подій у режимі реального часу, виявляти підозрілу активність на ранніх стадіях та оперативно реагувати на загрози, що є критично важливим для забезпечення цілісності та доступності інформаційних систем.

З огляду на те, що програми-вимагачі постійно вдосконалюються, використовуючи нові техніки обфускації та шифрування, традиційні антивірусні засоби часто не здатні вчасно виявити та запобігти атакам. Тому дослідження нових методів виявлення, заснованих на аналізі поведінки програм та використанні сучасних технологій, таких як eBPF та машинне навчання, є надзвичайно важливим.

Актуальність дисертації також підтверджується її практичною цінністю. Розроблені автором методи та інструменти можуть бути використані для створення ефективних систем захисту від програм-вимагачів, що допоможе зменшити ризики та наслідки кібератак для організацій та користувачів.

Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри

Дисертаційні дослідження виконувалися в межах держбюджетної науково-дослідної роботи «Розроблення та удосконалення методів та засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах» (№ державної реєстрації 0119U101690; терміни виконання - 2019-2022 рр.); Окремі частини роботи виконано в межах держбюджетної науково-дослідної роботи: «Дослідження стійкості біометричних систем автентифікації до атак із застосуванням технології клонування голосу на основі глибинних нейронних мереж» (№ держреєстрації 0124U000407).

Наукова новизна основних результатів дисертації

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 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.

Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна.

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.

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

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».

1. **Практичне значення** 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.

Основні результати дисертаційної роботи використано і впроваджено з метою покращення захищеності комп'ютерної мережі та систем в компанії ТОВ "ЕПАМ СИСТЕМЗ", реагування на інциденти кібербезпеки, компанією ТзОВ "ВІП СТУДІЯ" що підтверджено актами впровадження.

Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дисертаційної роботи Журавчака Даниїла Юрійовича викладено у п'ятнадцяти 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.

Зауваження по дисертації.

1. У розділі 1.5, де розглядаються SIEM та EDR рішення, автор не проводить порівняння цих систем з іншими засобами виявлення програм-вимагачів, такими як антивірусне програмне забезпечення або системи виявлення вторгнень. Це ускладнює розуміння місця запропонованого підходу в контексті існуючих рішень.

2. У розділі 3.3, присвяченому машинному навчанню, автор перераховує різні моделі та алгоритми, але не надає достатньо глибокого аналізу

їх переваг та недоліків у контексті виявлення програм-вимагачів. Більш детальний розгляд допоміг би краще зрозуміти, чому були обрані саме ці моделі, і як вони взаємодіють з даними, отриманими від eBPF.

3. У розділі 3.1, де описана архітектура інтегрованої системи виявлення вірусів-вимагачів, згадується про інтеграцію з SIEM, SOAR, Threat Intel та антивірусним програмним забезпеченням, але не надається достатньо деталей щодо того, як саме ця інтеграція відбувається та які переваги вона надає. Більш детальний опис цього аспекту був би корисним для розуміння практичної цінності розробленої системи.

4. У розділі 4.3.2, де розглядається споживання системних ресурсів, автор надає деякі дані про продуктивність моделей машинного навчання, але не проводить детального аналізу впливу запропонованої системи на загальну продуктивність системи у різних сценаріях використання. Було б корисно дослідити, як система впливає на продуктивність при обробці великих обсягів даних або при одночасному запуску інших ресурсоємних процесів.

5. У дисертації відсутній розділ або підрозділ, присвячений етичним аспектам використання технології eBPF та машинного навчання у контексті кібербезпеки. Враховуючи потенційні ризики для конфіденційності та безпеки даних, було б важливо розглянути ці питання більш детально, наприклад, у розділі 1, присвяченому аналізу проблеми.

Слід відзначити, що визначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновок

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 рецензент
Кандидат технічних наук, доцент,
Доцент кафедри захисту інформації
Національного університету
“Львівська політехніка” Ярослав СОВИН

Підпис к.т.н, доцента Совина Я.Р. засвідчую
Вчений секретар
Національного університету
“Львівська політехніка” Роман БРИЛИНСЬКИЙ
к.т.н., доцент