ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного університету
«Львівська політехніка»

"30" квітня 2024 р.

Висновок
про наукову новизну, теоретичне та практичне значення результатів дисертації «Удосконалення методів виявлення програм-вимагачів в режимі реального часу»
здобувача наукового ступеня доктора філософії за спеціальністю
125 Кібербезпека* (галузь знань *12 Інформаційні технології
Журавчака Даниїла Юрійовича
наукового семінару кафедри захисту інформації

1. Актуальність теми дисертації

Розробка та вдосконалення методів виявлення програм-вимагачів у 2024 році є надзвичайно актуальними, враховуючи постійне зростання та ускладнення кіберзагроз у глобальному масштабі. Це вимагає від бізнесу та державних установ впровадження передових методів захисту інформаційних активів.

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

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 керуються в головних управління розвідки. У перші місяці після вторгнення зріс масштаб та напрям програм-вимагачів та інших кіберзлочинів, у сторону урядового сегменту.

У зв'язку з цим, дослідження та розробка нових методів виявлення та протидії вірусам-вимагачам є надзвичайно важливим завданням 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.

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

Тема дисертації відповідає науковому напрямку кафедри захисту інформації Національного університету "Львівська політехніка": дослідження систем технічного захисту інформації, каналів зв'язку та комп'ютерних мереж, фізичного захисту інформації та криптографії.

Удосконалення інформаційної безпеки держави, контррозвідувальних методів протидії та техніки.

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.);

3. Особистий внесок здобувача в отриманні наукових результатів

У даній дисертації здійснено розробку та удосконалення методів виявлення та моніторингу програм-вимагачів у реальному часі, включаючи детальний технічний аналіз вірусів-вимагачів, оцінку наявних методик нейтралізації загроз, та дослідження можливостей eBPF для кіберзахисту. Було розроблено нові алгоритми та машинно-навчальні моделі, що дозволяють аналізувати великі обсяги даних і ефективно виявляти потенційні загрози, проведено експериментальні дослідження для підтвердження ефективності цих методів. Науковий внесок охоплює розробку інтегрованих систем збору даних, ефективних моделей класифікації та методів ідентифікації шаблонів даних, що значно підвищують швидкість і точність виявлення кіберзагроз та забезпечують надійний захист комп'ютерних систем.

4. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій базується на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванню прийнятих допущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується результатами комп'ютерного моделювання і практичною реалізацією модулів моніторингу на базі eBPF, моделей машинного навчання, а також збіжністю з результатами експериментальної верифікації.

5. Ступінь новизни основних результатів дисертації порівняно з відомими дослідженнями аналогічного характеру

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.

1. *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.
2. *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.
3. *Вперше запропоновано комплексну модель* класифікації вірусів-вимагачів з використанням ансамблю дерев рішень та випадкового лісу, що дозволяє з високою

наука, техніка", вип. 3, вип. 19, Березень 2023, с. 69-82, doi:10.28925/2663-4023.2023.19.6982. *Особистий внесок здобувача: проведено аналіз систем забезпечення безпеки endpoint detection and response, класифікація функціональних та нефункціональних властивостей задля створення такої системи у контексті виявлення програм-вимагачів у режимі реального часу.*

4. Піскозуб, А. З., Журавчак, Д. Ю., і Толкачова, А. Ю. "Дослідження Вразливостей у Чатботах з Використанням Великих Мовних Моделей." Безпека Інформації, том 29, № 3, 2023, с. 111–117. *Особистий внесок здобувача: проведено аналіз моделей машинного навчання, їхніх переваг та недоліків, а також аналіз вразливостей.*
5. Журавчак, Д., П. Глущенко, М. Опанович, В. Дудикевич, і А. Піскозуб. "КОНЦЕПЦІЯ НУЛЬОВОЇ ДОВІРИ ДЛЯ ЗАХИСТУ ACTIVE DIRECTORY ДЛЯ ВИЯВЛЕННЯ ПРОГРАМ-ВИМАГАЧІВ". Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", вип. 2, вип. 22, Грудень 2023, с. 179-90, doi:10.28925/2663-4023.2023.22.179190. *Особистий внесок здобувача: проведено аналіз використання концепції нульової довіри для виявлення вірусів-вимагачів у середовищі windows active directory.*
6. Журавчак, Даниїл, Едуард Кійко, і Валерій Дудикевич. "Використання EBPF для Ідентифікації Вірусів-Вимагачів, що Використовують DNS-Запити DGA." Information Technology and Security, vol. 11, no. 2 (21), 2023, pp. 166–174. *Особистий внесок здобувача: представлено розробку модуля опрацювання dns трафіку для виявлення активності вірусів-вимагачів.*
7. Журавчак, Д. Ю. "Моніторинг Вірусів-Вимагачів за Допомогою Розширеного Берклійського Пакетного Фільтра (eBPF) та Машинного Навчання." Наукоємні Технології, том 60, № 4, 2023, с. 352–363. *Особистий внесок здобувача: представлено модуль моніторингу мережі та моделей машинного навчання для виявлення вірусів-вимагачів.*

Статті у наукових періодичних виданнях інших держав, що включені до міжнародної наукометричної бази даних (Scopus):

8. Zhuravchak, D., Tolkachova, A., Piskozub, A., Dudykevych, V., і Korshun, N. "Monitoring Ransomware with Berkeley Packet Filter." CEUR Workshop Proceedings, vol. 3550, Cybersecurity Providing in Information and Telecommunication Systems II 2023. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II co-located with the International Conference on Problems of Infocommunications. Science and Technology (PICST 2023), Kyiv, Ukraine, October 26, 2023 (online), 2023, pp. 95–106. *Особистий внесок здобувача: представлено інтегровану систему виявлення вірусів-вимагачів за допомогою модулів моніторингу активності на операційній системі.*

Наукові публікації у збірниках матеріалів та тез конференцій:

9. Zhuravchak, D., Ustyianovych, T., Dudykevych, V., Venny, B., і Ruda, K. "Ransomware Prevention System Design Based on File Symbolic Linking Honeypots." 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 2021, pp. 284-287. IEEE. *Особистий внесок здобувача: представлено систему на базі програмних-приманок для виявлення вірусів-вимагачів.*
10. Журавчак Д.Ю. , Опанович М. Ю. Аналіз атак вірусів-шифрувальників на системи типу Active Directory за допомогою кореляції закономірностей в кіберзлочинах та аномальної активності // "Технічні засоби захисту інформації", семінар при вченій раді НАН України,

Київ, Україна, 2022 р.*Особистий внесок здобувача: представлено систему виявлення закономірностей у кіберзлочинах типу вірусів-вимагачів.*

11. Журавчак Д.Ю, проф. Дудикевич В.Б. Аналіз методів Threat Hunting для проактивного виявлення програм-вимагачів // "Технічні засоби захисту інформації", семінар при вченій раді НАН України, Київ, Україна, 2023 р. *Особистий внесок здобувача: представлено метод проактивного виявлення програм-вимагачів за допомогою Threat Hunting.*
12. Журавчак Д.Ю, проф. Дудикевич В.Б. Аналіз мережевого трафіку з використанням eBPF/XDP для ефективного виявлення програм-вимагачів // "Технічні засоби захисту інформації", семінар при вченій раді НАН України, Київ, Україна, 2024 р.*Особистий внесок здобувача: представлено систему моніторингу мережевого трафіку з метою виявлення вірусів-вимагачів на базі eBPF/XDP.*
13. Журавчак Д. Ю., Дудикевич В. Б., Опанович М. Ю., Піскозуб А. З. СТВОРЕННЯ СИСТЕМИ БЕЗПЕРЕРВНОГО РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФІКУВАННЯ ВІРУСАМИ-ВИМАГАЧАМИ В ACTIVE DIRECTORY // Збірник тез доповідей підготовлено за матеріалами Міжнародної наукової інтернет-конференції (випуск 70) 22-23 вересня 2022 р. на сайті www. konferenciaonline. org. ua. - 2022. - С. 25. *Особистий внесок здобувача: представлено систему безперервного реагування на інциденти кіберзлочинів типу вірусів-вимагачів.*
14. Журавчак, Даниїл, і Дудикевич Валерій. "Виклики Та Перспективи Впровадження Машинного Навчання Для Виявлення Програм-Вимагачів В Режимі Реального Часу." Захист Інформації І Безпека Інформаційних Систем: Матеріали IX Міжнародної Науково-Технічної Конференції, Львів, 25–26 травня 2023 р., 2023, с. 141–143. *Особистий внесок здобувача: представлено аналіз впровадження математичного апарату на базі моделей машинного навчання для виявлення програм-вимагачів.*

7. Апробація основних результатів дослідження на конференціях, симпозіумах, семінарах тощо

Основні результати дисертаційного дослідження апробовано на міжнародних наукових та науково-практичних конференціях, наукових школах та консорціумах, семінарах:

- Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II co-located with the International Conference on Problems of Infocommunications. Science and Technology (PICST 2023), Kyiv, Ukraine, October 26, 2023 (online)
- 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 2021
- Міжнародна наукова інтернет-конференція 22-23 вересня 2022 р. на сайті www. konferenciaonline. org. ua.
- IX Міжнародна Науково-Технічна Конференція, Львів, 25–26 травня 2023 р.
- Міжвідомчому міжрегіональному семінар Наукової Ради НАН України "Технічні засоби захисту інформації" (2022, 2023, 2024 років, Київ, Україна);
- Наукові семінари кафедри захисту інформації (2020-2024 рр.).

8. 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 для покращення процесів виявлення та управління інцидентами інформаційної безпеки в державних та приватних організаціях, що значно підвищує їхню здатність протистояти сучасним кіберзагрозам.

Також їх можна впровадити у навчальний процес у курсі "Міжнародні стандарти з кібербезпеки" для студентів спеціальності 125 "Кібербезпека".

9. Практична цінність результатів дослідження із зазначенням конкретного підприємства або галузі народного господарства, де вони можуть бути застосовані

Методи виявлення та моніторингу програм-вимагачів, розроблені в межах даного дослідження, значно покращують системи активного та пасивного захисту інформації в державних та приватних організаціях. Використання інноваційних технологій, таких як eBPF та методи машинного навчання, дозволяє ефективно ідентифікувати та класифікувати кіберзагрози, забезпечуючи швидкий та точний аналіз безпекових інцидентів. Розроблені моделі дозволяють зменшити час на аналіз та реагування на кіберзлочини, одночасно підвищуючи захищеність систем і забезпечуючи глибший аналіз вразливостей на різних рівнях інформаційної інфраструктури. Це робить результати дослідження особливо цінними для секторів, де критично важливо забезпечити надійний захист даних, таких як фінансові установи, охорона здоров'я, урядові служби та електронна комерція.
Основні результати дисертаційної роботи використано та впроваджено з метою покращення захищеності комп'ютерної мережі та систем в компанії ТОВ "ЕПАМ СИСТЕМЗ", реагування на інциденти кібербезпеки, компанією ТзОВ "ВІП СТУДІЯ".

10. Оцінка структури дисертації, її мови та стилю викладення

Дисертаційна робота викладена на 233 сторінках та складається з анотації, змісту, переліку скорочень, вступу, чотирьох основних розділів, в яких міститься 41 рисунок та 19 таблиць, списку використаних джерел з 210 найменувань, а також 4 додатки. За структурою, мовою та стилем викладення дисертація відповідає вимогам МОН України. Робота написана грамотною українською мовою з використанням сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним.

У ході обговорення дисертації до неї не було висунуто жодних зауважень щодо самої суті роботи.

11. З врахуванням зазначеного, **на науковому семінарі кафедри захисту інформації ухвалили:**

11.1. Дисертація Журавчака Даниїла Юрійовича на тему "Удосконалення методів виявлення програм-вимагачів" є завершеною науковою працею, у якій розв'язано конкретне наукове завдання – в режимі реального часу ідентифікувати та класифікувати кіберзагрози типу програм-вимагачів, забезпечуючи швидкий та точний аналіз безпекових інцидентів, що має важливе значення для галузі знань 12 "Інформаційні технології".

11.2. Основні наукові положення, методичні розробки, висновки та практичні рекомендації, викладені у дисертаційній роботі, логічні, послідовні, аргументовані, достовірні, достатньо обґрунтовані. Дисертація характеризується єдністю змісту.

11.3. У 14 наукових публікаціях відображені основні результати дисертації (з них 7 статей у наукових фахових виданнях України, 1 стаття у науковому виданні іншої держави, що входить до міжнародної наукометричної бази (Scopus), та 6 матеріалів конференцій).

11.4. Дисертація відповідає вимогам наказу МОН України № 40 від 12.01.2017р. «Про затвердження вимог до оформлення дисертації», Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти,

11.4. Дисертація відповідає вимогам наказу МОН України № 40 від 12.01.2017р. «Про затвердження вимог до оформлення дисертації», Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії (Постанова Кабінету Міністрів України від 12 січня 2022 р. № 44, зі змінами).

11.5. Дисертація є результатом самостійних досліджень, не містить елементів фальсифікації, компіляції, плагіату та запозичень, що констатує відсутність порушення академічної доброчесності. Використання текстів інших авторів мають належні посилання на відповідні джерела.

11.6. З урахуванням наукової зрілості та професійних якостей Журавчака Даниїла Юрійовича дисертаційна робота "Удосконалення методів виявлення програм-вимагачів в режимі реального часу" рекомендується для подання до розгляду та захисту у разовій спеціалізованій вченій раді.

За затвердження висновку проголосували:

"за"	*55*	*(п'ятдесят п'ять)*
"проти"	*–*	*(немає)*
"утримались"	*–*	*(немає)*

Головуючий на засіданні фахового семінару, д.т.н., професор, завідувач кафедри захисту інформації — Іван ОПІРСЬКИЙ

Рецензенти:

к.т.н., доцент, доцент кафедри захисту інформації — Ярослав СОВИН

к.т.н., старший викладач кафедри захисту інформації — Андрій ПАРТИКА

Відповідальний в ІКТА за атестацію PhD, д.т.н., професор, професор кафедри захисту інформації — Любомир ПАРХУЦЬ

"23" квітня 2024 р.