Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії Журавчак Даниїл Юрійович 1996 року народження, громадянин України, освіта вища: закінчив у 2020 році Національний університет «Львівська політехніка» за спеціальністю Кібербезпека, спеціалізація системи технічного захисту інформації автоматизації та їх обробки, виконав акредитовану освітньо-наукову програму Кібербезпека.
Разова спеціалізована вчена рада, утворена наказом ректора Національного університету «Львівська політехніка» Міністерства освіти і науки України, м. Львів, від «28» травня 2024 року № 222-5-10 у складі:

Голови разової спеціалізованої вченої ради	Івана Опірського, д.т.н., професора, завідувача кафедри захисту інформації технологій Національного університету «Львівська політехніка».
Рецензентів	Ярослава Совина, к.т.н., доцента кафедри захисту інформації Національного університету «Львівська політехніка».
	Андрія Партики, к.т.н., старшого викладача кафедри захисту інформації Національного університету «Львівська політехніка».
Офіційних опонентів	Олексія Смірнова, д.т.н., професора, завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету
	Володимира Соколова, к.т.н., доцента кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського університету імені Бориса Грінченка

на засіданні «13» серпня 2024 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 – Інформаційні технології Даниїлу Журавчаку на підставі публічного захисту дисертації «Удосконалення методів виявлення програм-вимагачів в режимі реального часу» за спеціальністю 125 Кібербезпека.

Дисертацію виконано у Національному університеті «Львівська політехніка» Міністерства освіти і науки України, м. Львів.
Науковий керівник Валерій Дудикевич, д.т.н, професор кафедри захисту інформації Навчально-наукового інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка».
Дисертацію подано у вигляді спеціально підготовленого рукопису, що містить нові науково-обґрунтовані результати проведених здобувачем досліджень, а саме: 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; модель 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; розроблено 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 загроз, що еволюціонують, що має істотне значення для галузі знань 12 - Інформаційні технології.
Здобувач має 15 наукових публікацій за темою дисертації, зокрема: 6 статей наукових фахових виданнях України та 2 у періодичному виданні закордоном та 7 тез виступів на науково-практичних заходах; 3 публікацій проіндексовано в наукометричній базі Scopus:

1. Zhuravchak, D. “СТВОРЕННЯ СИСТЕМИ ЗАПОБІГАННЯ ПОШИРЕННЯ ВІРУСІВ ВИМАГАЧІВ ЗА ДОПОМОГОЮ МОВИ ПРОГРАМУВАННЯ PYTHON ТА УТИЛІТИ AUDITD НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX”. Електронне фахове наукове видання “Кібербезпека: освіта, наука, техніка”, вип. 4, вип. 12, Червень 2021, с. 108-16, doi:10.28925/2663-4023.2021.12.108116. *Особистий внесок здобувача: представлено метод виявлення вірусів-вимагачів а допомогою створення системи програмних-приманок на базі утиліти auditD та створення модуля моніторингу за допомогою мови програмування python.*

2. Zhuravchak Danyil, Opanovych Maksym, Dudykevych Valerii, Piskozub Andrian, (2022). Detection Method Of Credential Dumping Method Through Exploiting Vulnerable Windows Error Reporting Service In Windows Operating Systems. Сучасна спеціальна техніка, 2 (69), 38-52. https://doi.org/10.36486/mst2411–3816.2022.2(69).2. *Особистий внесок здобувача: проведено аналіз вразливостей операційної системи Windows, що експлуатуються програмами-вимагачами.*

3. Zhuravchak, D. ., V. Dudykevych, і A. Tolkachova. "ДОСЛІДЖЕННЯ СТРУКТУРИ СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ ВІРУСІВ-ВИМАГАЧІВ НА БАЗІ ENDPOINT DETECTION AND RESPONSE". Електронне фахове наукове видання "Кібербезпека: освіта, 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.

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

У дискусії взяли участь голова і члени спеціалізованої вченої ради:

1. Іван Опірський, доктор технічних наук, професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка», без зауважень.
2. Совин Ярослав Романович, кандидат технічних наук, доцент, доцент кафедри захисту інформації Національного університету «Львівська політехніка», без зауважень.
3. Андрій Партика, кандидат технічних наук, старший викладач кафедри захисту інформації Національного університету «Львівська політехніка», без зауважень.

4. Володимир Соколов, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського університету імені Бориса Грінченка, без зауважень.
5. Олексій Смірнов, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, без зауважень.

Результати відкритого голосування:

«За» 5 (*п'ять*) членів ради,
«Проти» 0 (*нуль*) членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує Даниїлу Журавчаку ступінь доктора філософії з галузі знань *12 Інформаційні технології* за спеціальністю *125 Кібербезпека*.

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої
вченої ради _____ Іван Опірський

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"
ЗКПО 02071010