

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U004826

Особливі позначки: відкрита

Дата реєстрації: 24-08-2026

Статус: Захищена

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Карпюк Роман Валентинович

2. Roman V. Karpiuk

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0001-0053-1608

Вид дисертації: доктор філософії

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 25-08-2026

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Львівський національний університет імені Івана Франка

Код за ЄДРПОУ: 02070987

Місцезнаходження: вул. Університетська, Львів, 79000, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 15540

Повне найменування юридичної особи: Львівський національний університет імені Івана Франка

Код за ЄДРПОУ: 02070987

Місцезнаходження: вул. Університетська, Львів, 79000, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Львівський національний університет імені Івана Франка

Код за ЄДРПОУ: 02070987

Місцезнаходження: вул. Університетська, Львів, 79000, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56, 20.56.01, 20.60

Тема дисертації:

1. Застосування машинного навчання для виявлення та дослідження загроз в комп'ютерних мережах.
2. Application of Machine Learning for Detection and Investigation of Threats in Computer Networks.

Реферат/анотація:

1. У дисертаційній роботі розв'язано актуальне наукове завдання підвищення ефективності функціонування центрів протидії кіберзагрозам (CSOC) шляхом розроблення методу формування кореляційних правил у системах SIEM на основі машинного навчання. На відміну від наявних підходів, метод застосовується не до низькорівневих журналів подій і не для покращення окремого засобу захисту, а як аналітична надбудова над готовими спрацюваннями різнорідних контролів кібербезпеки: систем виявлення вторгнень, засобів захисту кінцевих точок, підсистем автентифікації, поштового та мережевого моніторингу, служб каталогів. Проаналізовано сучасний стан систем виявлення аномалій і показано, що доступні на ринку рішення обмежені доменом конкретного виробника, закриті для модифікації та коштовні у володінні. Обґрунтовано архітектурні підходи до побудови системи моніторингу подій кібербезпеки, збирання телеметрії з кінцевих пристроїв, її агрегації та кореляції; сформовано перелік параметрів, придатних для виявлення аномалій; запропоновано методику експертного оцінювання ефективності архітектурного підходу. Здійснено класифікацію алгоритмів пошуку аномалій та обґрунтовано вибір DensityFunction як базового. Розроблено

п'ятиетапний метод: постановка задачі та збирання початкової статистики; відокремлення штатного «шуму» з опрацюванням винятків; розрахунок додаткових корисних параметрів, зокрема грануляризації за часовими мітками; навчання базового алгоритму на очищеній вибірці; застосування навченої моделі до нових даних. Як компенсуючий контроль на випадок неспрацювання окремого кореляційного правила запропоновано механізм risk-based alerting. Розроблене програмне забезпечення впроваджено та функціонує на реальних даних у центрі протидії кіберзагрозам компанії SoftServe Inc., а також використовується в навчальному процесі Львівського національного університету імені Івана Франка. Результати впровадження підтверджують зниження кількості хибно-позитивних спрацювань і керованість показників часу на тріаж (TTT) та часу на закриття інцидентів (TTC). Ключові слова: аномалія, ризик, хибно-позитивні спрацювання, машинне навчання, функція густини, CSOC, SIEM, кореляційні правила, модель даних, додаткові корисні параметри.

2. The dissertation solves the relevant scientific task of improving the efficiency of Cybersecurity Operation Centres (CSOC) by developing a method for creating correlation rules in SIEM systems based on machine learning. Unlike existing approaches, the method is applied neither to low-level event logs nor to the improvement of an individual security control, but as an analytical layer over ready-made alerts produced by heterogeneous cybersecurity controls: intrusion detection systems, endpoint protection tools, authentication subsystems, mail and network monitoring, and directory services. The current state of anomaly detection systems is analysed; it is shown that market solutions are limited to a particular vendor's domain, closed to modification and expensive to own. Architectural approaches to building a cybersecurity event monitoring system, collecting telemetry from endpoints, aggregating and correlating it are substantiated; a set of parameters suitable for anomaly detection is formed, and a technique for expert evaluation of the architectural approach is proposed. Anomaly detection algorithms are classified and the choice of DensityFunction as the base algorithm is justified. A five-stage method is developed: problem statement and collection of initial statistics; separation of regular noise with exception handling; calculation of additional useful parameters, including granularisation by timestamps; training of the base algorithm on the cleaned sample; application of the trained model to new data. As a compensating control for cases when an individual correlation rule fails, a risk-based alerting mechanism is proposed. The developed software has been implemented and operates on real data in the Cybersecurity Operation Centre of SoftServe Inc. and is used in the educational process of Ivan Franko National University of Lviv. The implementation results confirm a reduction in false-positive alerts and manageability of Time To Triage (TTT) and Time To Closure (TTC). Keywords: anomaly, risk, false positives, machine learning, density function, CSOC, SIEM, correlation rules, data model, additional useful parameters.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 1. Karpiuk R., Kokovska Ya., Venherskyi P., Development of a Universal High-Performance Machine Learning Framework for Finding Cybersecurity Anomalies in Big Data, Lecture Notes in Electrical Engineering., 2024, Vol. 1198, P. 289-300, https://doi.org/10.1007/978-3-031-61221-3_14.
- 2. Roman Karpiuk, Petro Venherskyi, Using Machine Learning (ML) To Detect Threat Anomalies For Reducing False-Positives On The Daily Cybersecurity Operation Centre Routine, Вісник Львівського університету, серія прикладна математика та інформатика, Львів, 2021, <http://dx.doi.org/10.30970/vam.2021.29.11339>
- 3. Karpiuk R., Intelligent Monitoring For Distributed Systems: Leveraging Machine Learning To Detect And Adapt To Evolving Cyber Threats, Вісник Львівського університету. Серія прикладна математика та

інформатика, Львів, 2024, № 33, С. 69–72, <http://dx.doi.org/10.30970/vam.2024.33.12791>

- 4. Корченко А., Карпюк Р., Парашук Т., Мацюк С., Метод Формування Параметрів Та Оцінювання Загроз У Соціотехнічних Системах, Information Technology: Computer Science, Software Engineering and Cyber Security, 2023, Vol. 2, P. 3-11, <https://doi.org/10.32782/IT/2023-2-1>
- 5. Karpiuk Roman, Venherskyi Petro, Using Machine Learning (ML) to Detect Cybersecurity Anomalies, IXth International Scientific and Technical Conference «Information protection and information systems security», 25-26 May 2023, pp. 107-109, ISBN 978-966-941-829-6
- 6. Венгерський П., Карпюк Р., Використання Машинного Навчання Для Визначення Загроз З Кібербезпеки, Колективна монографія «Актуальні питання забезпечення кібербезпеки та захисту інформації», 2023, ст. 132-141, ISBN 978-966-301-259-9
- 7. Karpiuk R., Venherskyi P., Korchenko A, Khokhlachova Yu., Machine Learning as One of the Highly Effective Methods of Reducing the Load on CSOC's Analysts, IEEE ELIT, 2023, Vol. 13th., P. 132–136, DOI: 10.1109/ELIT61488.2023.10310808
- 8. Karpiuk R., Venherskyi P., Extraction, integration and data processing in the SIEM «Splunk» using «Nessus» vulnerability scanner, Conference proceeding «Behind the Digital Curtain Civil Society vs. State Sponsored Cyber Attacks», Brussels, 25 June 2019, DOI 10.34054/bdc002
- 9. Karpiuk Roman, Venherskyi Petro, Using Machine Learning (ML) to Detect Threat Anomalies for Reducing False-Positives on the Daily Cybersecurity Operation Centre Routine, The 12th International Scientific Conference «ITSEC», 2-4 May 2023, pp. 62-64, УДК [003.26+004+519.816]:004.056:65(063)
- 10. Karpiuk R., Kokovska Ya., Venherskyi P., Investigation of False Positives Notable Events by Processing of the SOC Team Using Machine Learning Methods, In Problems of Scientific, Technical and Legal Support for Cybersecurity in the Modern World, Krakow, Poland, 2024.
- 11. Venherskyi P., Karpiuk R., The Use of Machine Learning (ML) as One of the Highly Effective Methods of Reducing the Load on CSOC's Analysts, XXVII Всеукраїнська наукова конференція «Сучасні проблеми прикладної математики та інформатики (APAMCS-2023)», Львів, 7-9 Листопада 2023., ст. 71-75.
- 12. Karpiuk R., Venherskyi P., Kropyva, M., Detection of LDAP Reconnaissance or Kerberoasting Attacks Using Machine Learning, The 13th International Scientific Conference «ITSEC», Lviv, 9-11 May 2024.
- 13. Karpiuk R.V., Venherskyi P.S., Using Machine Learning in Cybersecurity to Detect Some Threat Anomalies, IEEE TCSET, Online, 22-26 February 2022
- 14. Karpiuk R., Venherskyi P., Built strong vulnerability analytics with Nessus and SIEM Splunk, Міжнародна наукова конференція “Сучасні проблеми прикладної математики та інформатики” (APAMCS-2019), 24 – 27 вересня 2019 року, Львів, ст. 76-82.
- 15. Karpiuk R., Venherskyi P., Using machine learning (ML) to detect threat anomalies for reducing false-positives on the daily cybersecurity operation centre routine, Зб. наук. праць "Сучасні проблеми прикладної математики та комп'ютерних наук", Львів, 2021, ст. 42-46.

Наукова (науково-технічна) продукція: методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: підвищення автоматизації виробничих процесів; забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0123U101815

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Венгерський Петро Сергійович
2. Petro S. Venherskyi

Кваліфікація: д. ф.-м. н., професор, 01.05.02**Ідентифікатор ORCID ID:** 0000-0001-9808-7404**Додаткова інформація:** Web of Science Researcher ID: F-7499-2019; Scopus Author ID: 55225981100;
<https://scholar.google.com/citations?user=1E6bnCoAAAAJ>**Повне найменування юридичної особи:** Львівський національний університет імені Івана Франка**Код за ЄДРПОУ:** 02070987**Місцезнаходження:** вул. Університетська, Львів, 79000, Україна**Форма власності:** Державна**Сфера управління:** Міністерство освіти і науки України**Ідентифікатор ROR:****VII. Відомості про офіційних опонентів та рецензентів****Офіційні опоненти****Власне Прізвище Ім'я По-батькові:**

1. Корченко Олександр Григорович
2. Oleksandr H. Korchenko

Кваліфікація: д. т. н., професор, 05.13.21**Ідентифікатор ORCID ID:** 0000-0003-3376-0631**Додаткова інформація:** Scopus Author ID: 57217960494;
<https://scholar.google.com.ua/citations?user=nGJEeNIAAAAAJ>**Повне найменування юридичної особи:** Державний університет інформаційно-комунікаційних технологій**Код за ЄДРПОУ:** 38855349**Місцезнаходження:** вул. Солом'янська, Київ, 03110, Україна**Форма власності:** Державна**Сфера управління:** Міністерство освіти і науки України**Ідентифікатор ROR:****Власне Прізвище Ім'я По-батькові:**

1. Гільгурт Сергій Якович
2. Serhii Y. Hilhurt

Кваліфікація: д. т. н., старший науковий співробітник, 05.13.05

Ідентифікатор ORCID ID: 0000-0003-1647-1790

Додаткова інформація: Web of Science Researcher ID: Q-6850-2018; Scopus Author ID: 57373650100;
<https://scholar.google.com.ua/citations?user=L4JS3tQAAAAJ>

Повне найменування юридичної особи: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України

Код за ЄДРПОУ: 05516949

Місцезнаходження: вул. Генерала Наумова, Київ, 03164, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Пелешко Дмитро Дмитрович
2. Dmytro D. Peleshko

Кваліфікація: д. т. н., професор, 05.13.23

Ідентифікатор ORCID ID: 0000-0003-4881-6933

Додаткова інформація: Scopus Author ID: 27867946500; Web of Science Researcher ID: S-2980-2018;
<https://scholar.google.com.ua/citations?user=gYqXHWEEAAAAJ>

Повне найменування юридичної особи: Львівський національний університет імені Івана Франка

Код за ЄДРПОУ: 02070987

Місцезнаходження: вул. Університетська, Львів, 79000, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Павлишенко Богдан Михайлович
2. Bohdan M. Pavlyshenko

Кваліфікація: д. т. н., професор, 05.13.23

Ідентифікатор ORCID ID: 0000-0001-9515-3488

Додаткова інформація: Scopus Author ID: 8521299600;
https://scholar.google.com/citations?user=Ld4m_aIAAAAJ&hl

Повне найменування юридичної особи: Львівський національний університет імені Івана Франка

Код за ЄДРПОУ: 02070987

Місцезнаходження: вул. Університетська, Львів, 79000, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Дияк Іван Іванович

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Дияк Іван Іванович

**Відповідальний за підготовку
облікових документів**

Жак Ольга Володимирівна

Реєстратор

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Тетяна Анатоліївна