Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U001823

Особливі позначки: відкрита

Дата реєстрації: 19-05-2026

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Опанович Максим Юрійович
2. Maksym Opanovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: кібербезпека

Дата захисту: 11-06-2026

Спеціальність за освітою: кібербезпека

Місце роботи здобувача: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, Львів, 79013, 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 13119

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, Львів, 79013, 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: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.01, 20.56.02

Тема дисертації:

1. Вдосконалення виявлення кіберзагроз в Active Directory за допомогою кореляції закономірностей в кіберзлочинах та аномальної активності

2. Improving the detection of cyber threats in Active Directory using the correlation of patterns in cyberattacks and anomalous activity

Реферат/анотація:

1. Дисертаційна робота присвячена вирішенню актуальної науково-практичної задачі підвищення рівня захищеності інформаційно-комунікаційних систем побудованих на Active Directory (AD). Робота зосереджена на розробленні та дослідженні методу виявлення кіберзагроз, що базується на аналізі закономірностей в атаках та їх кореляції з поведінковими аномаліями. Актуальність теми зумовлена невпинним зростанням кількості, складності та масштабу кіберзагроз, особливу небезпеку серед яких становлять розвинені стійкі загрози (APT). Метою роботи є вдосконалення захисту Active Directory від кіберзагроз шляхом розроблення методу виявлення, який інтегрує поведінковий аналіз на базі машинного навчання та кореляцію закономірностей атак для мінімізації хибних спрацювань. У першому розділі «АНАЛІЗ ПІДХОДІВ ТА ЗАСОБІВ ДЛЯ ВИЯВЛЕННЯ ТА ПРОТИДІЇ КІБЕРЗАГРОЗАМ» здійснено комплексний аналіз сучасних інструментів та підходів до виявлення кіберзагроз в контексті зростання активності APT-груп. Встановлено критичну роль

інфраструктури AD як пріоритетної цілі зловмисників та визначено ключові фактори успішності кібератак, зокрема масове використання технік LOTL. На основі порівняльного аналізу методів захисту обґрунтовано перспективність підходу виявлення аномалій для ідентифікації нових та модифікованих загроз. Визначено необхідність вдосконалення даного методу для нівелювання високого рівня хибних спрацювань, притаманного його класичній реалізації. У другому розділі «ДОСЛІДЖЕННЯ ЗАКОНОМІРНОСТЕЙ В КІБЕРАТАКАХ ТА ВИЯВЛЕННЯ АНОМАЛІЙ» досліджено закономірності кібератак APT-груп та підтверджено тенденцію до використання легітимних інструментів ОС Windows для маскування зловмисної активності. Визначено критичність компонентів AD та доведено неефективність підходів на основі індикаторів компрометації проти технік LOTL. За результатами порівняльного аналізу методів машинного навчання обґрунтовано вибір LSTM-автокодувальників для обробки нерозмічених даних командного рядка. Запропоновано використання вузькоспеціалізованих мікро-моделей для окремих системних інструментів, для забезпечення мінімізації хибних спрацювань та високу точність виявлення аномалій. У третьому розділі «РОЗРОБЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ СКЛАДНИХ КІБЕРЗАГРОЗ ЗА ДОПОМОГОЮ ЗАКОНОМІРНОСТЕЙ АТАК APT-ГРУП ТА ЇХ КОРЕЛЯЦІЇ З АНОМАЛІЯМИ» представлено етапи реалізації запропонованого рішення. Розроблено методику формування політик безпеки та аудиту для забезпечення збору релевантних даних. Описано метод виявлення аномальної поведінки, реалізований через вузькоспеціалізовані мікро-моделі на базі LSTM-автокодувальників для окремих процесів. Представлено механізм багаторівневої кореляції подій, який забезпечує валідацію аномалій через порівняння зі зловмисними патернами та техніками MITRE ATT&CK. Формалізовано архітектуру програмного комплексу. Впроваджено алгоритм ризик-орієнтованої агрегації, що динамічно розраховує рівень небезпеки інцидентів з урахуванням критичності активів. Розроблено загальну математичну модель, яка описує взаємодію всіх компонентів методу. У четвертому розділі «РЕАЛІЗАЦІЯ ТА ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ДІЄВОСТІ МЕТОДУ ВИЯВЛЕННЯ СКЛАДНИХ КІБЕРЗАГРОЗ ЗА ДОПОМОГОЮ ЗАКОНОМІРНОСТЕЙ В КІБЕРАТАКАХ ТА ЇХ КОРЕЛЯЦІЇ З АНОМАЛІЯМИ» описано практичну імплементацію розробленого рішення та виконано всебічне тестування. Експериментально підтверджено високу точність розроблених мікро-моделей на базі LSTM-автокодувальників, де досягнуто середнього показника F1-Score на рівні 90,95%.. Загальна точність методу, реалізованого у формі правил ADR, підтверджується коректною класифікацією 99,1% легітимних та 95,9% зловмисних подій. Підтверджено стійкість методу до обфускації з показником повноти 98,3%, що перевершує найкращі аналоги до 61,9%. Доведено здатність алгоритму ризик-орієнтованої агрегації виявляти комплексні багатоетапні атаки, шляхом кореляції розрізнених подій в єдиний інцидент. Розроблені політики аудиту дозволили скоротити обсяг вхідних даних приблизно у 12 і підвищити співвідношення сигналу до шуму до 44 разів. У висновках узагальнено основні наукові та практичні результати роботи, які підтверджують досягнення поставленої мети та вирішення науково-практичної задачі. Обґрунтовано ефективність розробленого методу виявлення аномалій, реалізованого у формі правил ADR на базі вузькоспеціалізованих мікро-моделей LSTM-автокодувальників, що забезпечують високу точність та стійкість до обфускації, а також представлено та охарактеризовано кількісні та метрики запропонованого рішення.

2. The dissertation is dedicated to solving the urgent scientific and practical problem of increasing the level of security of information and communication systems built on Active Directory (AD). The work focuses on the development and research of a method for detecting cyber threats, based on the analysis of patterns in attacks and their correlation with behavioral anomalies. The relevance of the topic is due to the constant increase in the number, complexity and scale of cyber threats, among which advanced persistent threats (APT) are of particular danger. The aim of the work is to improve the protection of Active Directory against cyber threats by developing a detection method that integrates behavioral analysis based on machine learning and correlation of attack patterns to minimize false positives. In the first section, “ANALYSIS OF APPROACHES AND MEANS FOR DETECTION AND COUNTERACTION OF CYBER THREATS”, a comprehensive analysis of modern tools and approaches to detecting cyber threats in the context of the growth of APT groups’ activity was carried out. The critical role of the AD infrastructure as a priority target for attackers was established and key factors for the success of cyber attacks

were identified, in particular the massive use of LOTL techniques. Based on a comparative analysis of protection methods, the prospects of the anomaly detection approach for identifying new and modified threats were substantiated. The need to improve this method to eliminate the high level of false positives inherent in its classical implementation was identified. In the second section "STUDY OF CYBERATTACKS AND ANOMALIES DETECTION", the patterns of cyberattacks by APT groups are investigated and the tendency to use legitimate Windows OS tools to mask malicious activity is confirmed. The criticality of AD components is determined and the ineffectiveness of approaches based on indicators of compromise against LOTL techniques is proven. Based on the results of a comparative analysis of machine learning methods, the choice of LSTM autoencoders for processing unlabeled command line data is justified. The use of highly specialized micro-models for individual system tools is proposed to ensure the minimization of false positives and high accuracy of anomaly detection. The third section, “DEVELOPMENT OF A METHOD FOR DETECTION OF COMPLEX CYBERTHREATS USING APT GROUP ATTACK PATTERNS AND THEIR CORRELATION WITH ANOMALIES,” presents the stages of implementation of the proposed solution. A methodology for forming security and audit policies to ensure the collection of relevant data has been developed. A method for detecting anomalous behavior, implemented through highly specialized micro-models based on LSTM autoencoders for individual processes, is described. A mechanism for multi-level event correlation is presented, which ensures the validation of anomalies through comparison with malicious patterns and MITRE ATT&CK techniques. The architecture of the software complex is formalized. A risk-oriented aggregation algorithm is implemented, which dynamically calculates the level of incident danger taking into account the criticality of assets. A general mathematical model is developed that describes the interaction of all components of the method. The fourth section, “IMPLEMENTATION AND EXPERIMENTAL STUDY OF THE EFFECTIVENESS OF THE METHOD FOR DETECTION OF COMPLEX CYBERTHREATS USING PATTERNS IN CYBERATTACKS AND THEIR CORRELATIONS WITH ANOMALIES,” describes the practical implementation of the developed solution and performs comprehensive testing. The high accuracy of the developed micro-models based on LSTM autoencoders was experimentally confirmed, where the average F1-Score was achieved at the level of 90.95%. The overall accuracy of the method, implemented in the form of ADR rules, is confirmed by the correct classification of 99.1% of legitimate and 95.9% of malicious events. The resistance of the method to obfuscation with a completeness index of 98.3% was confirmed, which surpasses the best analogues by 61.9%. The ability of the risk-based aggregation algorithm to detect complex multi-stage attacks by correlating disparate events into a single incident has been proven. The developed audit policies have allowed to reduce the volume of input data by approximately 12 times and increase the signal-to-noise ratio by up to 44 times. The conclusions summarize the main scientific and practical results of the work, which confirm the achievement of the set goal and the solution of the scientific and practical problem. The effectiveness of the developed anomaly detection method, implemented in the form of ADR rules based on highly specialized micro-models of LSTM autoencoders, which provide high accuracy and resistance to obfuscation, is substantiated, and the quantitative and metrics of the proposed solution are presented and characterized.

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. 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.

- 2. Журавчак, Д., Глущенко , П., Опанович , М., Дудикевич , В., & Піскозуб , А. (2023). КОНЦЕПЦІЯ НУЛЬОВОЇ ДОВІРИ ДЛЯ ЗАХИСТУ ACTIVE DIRECTORY ДЛЯ ВИЯВЛЕННЯ ПРОГРАМ-ВИМАГАЧІВ. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 2(22), 179–190.
- 3. Опанович, М. (2024). АНАЛІЗ КІБЕРАТАК ТА ДІЯЛЬНОСТІ АРТ ГРУП В УКРАЇНІ. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 4(24), 172–184.
- 4. Опанович М. Ю. Аналіз способів обходу інструментів для запобіганням загроз та дослідження методів протидії цьому // Наукоємні технології. – 2024. – Т. 62, № 2. – С. 116–125.
- 5. Opanovych, M. (2025). ANOMALY DETECTION IN ACTIVE DIRECTORY FOR APT ATTACK DETECTION: METHODS, EFFECTIVENESS, AND LIMITATIONS. Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 2(30), 752–765.
- 6. Opanovych M. Y., Zhuravchak D. Y., Tolkachova A., Piskozub A., Dudykevych V. Design of an integrated defense-in-depth system with an artificial intelligence assistant to counter malware // Східно-Європейський журнал передових технологій. – 2024. – № 6/2(132). – С. 64–73.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Піскозуб Андріян Збігнєвич

2. Andrian Piskozub

Кваліфікація: к. т. н., доцент, 05.13.13

Ідентифікатор ORCID ID: 0000-0002-3582-2835

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, Львів, 79013, 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. Смірнов Олексій Анатолійович

2. Oleksii Smirnov

Кваліфікація: д.т.н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0001-9543-874X

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Складанний Павло Миколайович

2. Pavlo M. Skladannyi

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-7775-6039

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Коробейнікова Тетяна Іванівна

2. Tetyana I. Korobeynikova

Кваліфікація: к. т. н., доц., 05.13.06

Ідентифікатор ORCID ID: 0000-0003-2487-8742

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Партика Андрій Ігорович

2. Andrii Partyka

Кваліфікація: к.т.н., доцент, 05.27.01

Ідентифікатор ORCID ID: 0000-0003-3037-8373

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Опірський Іван Романович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Опірський Іван Романович
Відповідальний за підготовку облікових документів	Пархуць Любомир Теодорович
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна