

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U001820

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. Журавчак Анастасія Юріївна

2. Anastasiia Y. Zhuravchak

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: Товариство з обмеженою відповідальністю «Епам діджитал»

Код за ЄДРПОУ: 44420385

Місцезнаходження: вул. Прахових Сім'ї, Київ, 01033, Україна

Форма власності: Приватна/недержавна

Сфера управління:

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 13101

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, 20.56.01, 20.56.02

Тема дисертації:

1. Удосконалення методології автоматизації тестування на проникнення за допомогою методів машинного навчання

2. Improvement of the penetration testing automation methodology using learning methods

Реферат/анотація:

1. У сучасних умовах стрімкої цифрової трансформації суспільства та зростання залежності бізнесу, урядових і критичних інфраструктурних систем від інформаційних технологій питання забезпечення кібербезпеки набуває першочергового значення. Традиційні підходи до тестування на проникнення базуються на ручному аналізі, що виконується фахівцями з кібербезпеки з використанням наборів інструментів для сканування та експлуатації вразливостей. Сучасні тенденції розвитку штучного інтелекту (ШІ) відкривають нові можливості для підвищення ефективності процесів тестування на проникнення. Це зумовлює доцільність дослідження напрямку інтеграції технологій штучного інтелекту у процеси тестування на проникнення з метою підвищення швидкості, точності та відтворюваності результатів. Перший розділ "Аналіз сучасних методів тестування безпеки веб-застосунків" присвячений всебічному аналізу сучасного стану проблеми, починаючи з класифікації основних типів атак та вразливостей за стандартом OWASP Top 10. У розділі детально розглядаються методи виявлення, а також аналізуються провідні інструменти для автоматизації тестування.

Особливу увагу приділено аналізу ринку комерційних рішень, що виявив відсутність українських інструментів серед лідерів галузі. Обґрунтовано напрямки дослідження та доцільність розробки нової методології на основі методів машинного навчання. У другому розділі "Дослідження методів машинного навчання для автоматизації тестування на проникнення" здійснено дослідження класичних методів машинного навчання, спрямованих на автоматизацію процесів тестування на проникнення. Проведено порівняльний аналіз з метою визначення їх ефективності для виявлення вразливостей. Обґрунтовано необхідність переходу до моделей навчання з підкріпленням Reinforcement learning (RL), які дозволяють моделювати послідовність дій агента у динамічному середовищі. Особливу увагу приділено інтеграції великих мовних моделей (LLM) у ролі політики агента, здатної до контекстного планування, міркувань і генерації дій за принципом ReAct. Було розроблено концептуальну архітектуру методу агента з коротко- та довготривалою пам'яттю. Проведене дослідження сформуло теоретичну базу для подальшого дослідження. Третій розділ "Розробка методу автоматизованого тестування за допомогою моделі машинного навчання" присвячений розробці математичних та архітектурних основ методу автоматизованого тестування на проникнення з використанням марковських процесів прийняття рішень у поєднанні з великими мовними моделями. Було здійснено формалізацію параметрів веб-додатків, типів вразливостей та їхніх характеристик, що впливають на процес виявлення. Розроблено модель автоматизованого тестування у вигляді дискретного марковського ланцюга, у межах якого визначено множину станів системи, ймовірності переходів між ними та функції винагороди, що дозволило описати динаміку процесу з урахуванням природи середовища. На основі цієї моделі сформовано систему метрик, що забезпечила кількісну оцінку ефективності тестування. Вибрано архітектуру типу "LLM як політика", у якій велика мовна модель відповідала за генерацію стратегій, reasoning-ланцюгів та адаптивне планування дій агента. Розроблено архітектуру взаємодії між математичними моделями та інтелектуальними компонентами LLM, створюючи основу для автономного прийняття рішень у змінному середовищі. Четвертий розділ "Експериментальне дослідження організації та оцінки автоматизованого тестування на проникнення", що присвячений практичній перевірці розробленого методу. У цьому розділі здійснено практичну реалізацію та експериментальну перевірку розробленого методу автоматизованого тестування на проникнення із використанням штучного інтелекту. Було розгорнуто відтворюване лабораторне середовище на базі хмарної інфраструктури Amazon Web Services, що забезпечило масштабованість, ізоляцію та безпечне виконання експериментів. Створено дворівневу структуру, яка включала набір інструментів (Nmap, Burp Suite, SSlyze) та цільові веб-додатки (OWASP Juice Shop, DVWA, WebGoat), що дозволило змоделювати реальні сценарії тестування. Проведено серію експериментів із порівняння ручного та автоматизованого підходів до виявлення вразливостей у мережевих, веб- та TLS-конфігураціях. Отримані результати засвідчили підвищення точності та повноти виявлення вразливостей. Проведено кількісний аналіз результатів експериментів, сформовано метрики продуктивності та достовірності, а також розроблено методичні рекомендації щодо впровадження інструментарію в практику. У висновках дисертаційної роботи підсумовано вирішення науково-практичного завдання автоматизації тестування на проникнення шляхом інтеграції методів навчання з підкріпленням, марковських процесів прийняття рішень та великих мовних моделей.

2. In today's rapidly digital transformation of society and the growing dependence of business, government, and critical infrastructure systems on information technology, the issue of ensuring cybersecurity is becoming paramount. Traditional approaches to penetration testing are based on manual analysis performed by cybersecurity specialists using toolkits for scanning and exploiting vulnerabilities. Current trends in the development of artificial intelligence (AI) open up new opportunities for increasing the efficiency of penetration testing processes. This makes it appropriate to study the direction of integrating artificial intelligence technologies into penetration testing processes in order to increase the speed, accuracy, and reproducibility of results. The first section, "Analysis of Modern Web Application Security Testing Methods," is devoted to a comprehensive analysis of the current state of the problem, starting with the classification of the main types of attacks and vulnerabilities according to the OWASP Top 10 standard. The section discusses detection methods in detail, as well as analyzes leading tools for testing automation. Special attention is paid to the analysis of the commercial solutions market,

which revealed the absence of Ukrainian tools among the industry leaders. Research directions and the feasibility of developing a new methodology based on machine learning methods are substantiated. In the second section "Research on machine learning methods for penetration testing automation", a study of classical machine learning methods aimed at automating penetration testing processes was carried out. A comparative analysis was conducted to determine their effectiveness for detecting vulnerabilities. The need to transition to Reinforcement learning (RL) models was justified, which allow modeling the sequence of agent actions in a dynamic environment. Special attention was paid to the integration of large language models (LLM) as an agent policy capable of contextual planning, reasoning, and generating actions according to the ReAct principle. A conceptual architecture of the agent method with short- and long-term memory was developed. The conducted research formed a theoretical basis for further research. The third section "Development of an automated testing method using a machine learning model" is devoted to the development of the mathematical and architectural foundations of the automated penetration testing method using Markov decision processes in combination with large language models. The parameters of web applications, types of vulnerabilities and their characteristics that affect the detection process were formalized. An automated testing model was developed in the form of a discrete Markov chain, within which a set of system states, transition probabilities between them and reward functions were defined, which made it possible to describe the dynamics of the process taking into account the nature of the environment. Based on this model, a system of metrics was formed that provided a quantitative assessment of the effectiveness of testing. An architecture of the "LLM as a policy" type was chosen, in which the large language model was responsible for the generation of strategies, reasoning chains and adaptive planning of agent actions. An architecture of interaction between mathematical models and intelligent components of LLM was developed, creating the basis for autonomous decision-making in a changing environment. The fourth section, "Experimental study of the organization and evaluation of automated penetration testing", is devoted to the practical verification of the developed method. In this section, the practical implementation and experimental verification of the developed method of automated penetration testing using artificial intelligence was carried out. A reproducible laboratory environment was deployed based on the Amazon Web Services cloud infrastructure, which ensured scalability, isolation and secure execution of experiments. A two-tier structure was created, which included a set of tools (Nmap, Burp Suite, SSLyze) and target web applications (OWASP Juice Shop, DVWA, WebGoat), which allowed to simulate real testing scenarios. A series of experiments were conducted to compare manual and automated approaches to detecting vulnerabilities in network, web and TLS configurations. The results obtained showed an increase in the accuracy and completeness of vulnerability detection. A quantitative analysis of the experimental results was conducted, performance and reliability metrics were formed, and methodological recommendations for implementing the toolkit into practice were developed. The conclusions of the dissertation summarize the solution to the scientific and practical problem of penetration testing automation by integrating reinforcement learning methods, Markov decision processes, and large language models.

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, 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.
- 2. 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.

- 3. Журавчак А. Ю., Гарасимчук О. І., Опірський І. Р. Аналіз безпеки протоколу OAuth // Вісник Львівського державного університету безпеки життєдіяльності. – 2023. – № 27. – С. 67–76.
- 4. Журавчак А. Ю., Піскозуб А. З. Аналіз загроз та ризиків в екосистемі Web3 в контексті безпеки // Інформаційні технології та безпека. – 2023. – Т. 11, № 2. – С. 227–238.
- 5. Журавчак А. Ю., Посувайло М. В. Тестування на проникнення з використанням глибокого навчання з підкріпленням // Кібербезпека: освіта, наука, техніка. – 2024. – № 3 (23). – С. 17–30.
- 6. Журавчак А. Ю., Піскозуб А. З. Методи для тестування безпеки веб-застосунків // Кібербезпека: освіта, наука, техніка. – 2024. – № 2 (26). – С. 115–122.
- 7. Журавчак А. Ю., Піскозуб А. З. Аналіз методів машинного навчання для автоматизації тестування на проникнення // Кібербезпека: освіта, наука, техніка. – 2025. – № 3 (27). – С. 54–62.
- 8. Журавчак А. Ю., Піскозуб А. З., Журавчак Д. Ю., Глущенко П. К., Беляєв І. Аналіз автоматизації тестування на проникнення за допомогою марковських процесів прийняття рішень // Сучасний захист інформації. – 2025. – № 1 (61). – С. 82–88.
- 9. Журавчак А., Піскозуб А., Банах Р., Журавчак Д., Глущенко П. Аналіз інструменту для виявлення вразливостей у хмарних технологіях // Кібербезпека: освіта, наука, техніка. – 2025. – № 4 (28). – С. 288–294.
- 10. Піскозуб, А., Журавчак, А., Журавчак, Д., Журавчак, Ю., & Беляєв, І. (2025). Застосування нейронних мереж для вибору інструментів для тестування на проникнення. *Social Development and Security*, 15(4), 126–132.
- 11. Zhuravchak, D., Tolkachova, A., Piskozub, A., Dudykevych, V., i 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.
- 12. 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
- 13. Zhuravchak A. Y., Piskozub A., Skorynovych B. V., Lakh Y., Zhuravchak D. Y., Hlushchenko P. K., Venherskyi P., Beliaiev I., Vorokhob M., Kolbasynskyi I. V. Design and development of a large language model-based tool for vulnerability detection // Східно-Європейський журнал передових технологій. – 2025. – № 2/2 (134). – С. 75–83.
- 14. Zhuravchak Y., Zhuravchak D., Zhuravchak, A., Oprisky I. Security regression visualization in CI/CD using trivy and GitHub actions // CEUR Workshop Proceedings. – 2025. – Vol. 4042 : Proceedings of the cyber security and data protection, CSDP 2025, Lviv, Ukraine, July 31, 2025. – P. 272–281.
- 15. Журавчак Ю. Ю., Журавчак, А. Ю., Журавчак Д. Ю. Автоматизоване створення baseline-звітів та зниження шуму у CI/CD середовищах засобами універсальних сканерів безпеки // Телекомунікаційні та інформаційні технології. – 2025. – № 3 (88). – С. 64–71.
- 16. Журавчак Ю. Ю., Журавчак Д. Ю., Журавчак А. Ю. Порівняння сканерів на вразливості для виявлення обфускованого шкідливого коду в контейнерах // Комп'ютерні системи та мережі. – 2025. – Вип. 7, № 2. – С. 60–70.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Піскозуб Андріян Збігневич
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. 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: 45307965

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

Форма власності: Комунальна

Сфера управління: Держадміністрація

Ідентифікатор ROR:

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: Центральнотехнічний національний технічний університет

Код за ЄДРПОУ: 02070950

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Рецензенти

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:

Власне Прізвище Ім'я По-батькові:

1. Сабодашко Дмитро Володимирович

2. Dmytro Sabodashko

Кваліфікація: д.філософ, 125

Ідентифікатор ORCID ID: 0000-0003-1675-0976

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

Хома Володимир Васильович

Власне Прізвище Ім'я По-батькові
головуючого на засіданні

Хома Володимир Васильович

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