

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U001372

Особливі позначки: відкрита

Дата реєстрації: 06-05-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: № 915-уч від 16.07.2026, Національний аерокосмічний університет "ХАІ"



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Неретін Олексій Сергійович

2. Oleksii S. Neretin

Кваліфікація: 125

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: 23-06-2026

Спеціальність за освітою: Магістр з імпульсних теплових машин за освітньою програмою «Імпульсні теплові машини»

Місце роботи здобувача: Товариство з обмеженою відповідальністю "ВЕБСПЕЛЧЕКЕР"

Код за ЄДРПОУ: 40525798

Місцезнаходження: пр.Науки, б.38, Харків, Харківський р-н., 61072, 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 13214

Повне найменування юридичної особи: Національний аерокосмічний університет "Харківський авіаційний інститут"

Код за ЄДРПОУ: 02066769

Місцезнаходження: вул. Манька Вадима, Харків, Харківський р-н., 61070, 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 аерокосмічний університет "Харківський авіаційний інститут"

Код за ЄДРПОУ: 02066769

Місцезнаходження: вул. Манька Вадима, Харків, Харківський р-н., 61070, 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, 20.56.02

Тема дисертації:

1. Методи та засоби аналізу кібербезпеки і захисту великих мовних моделей від генерації забороненого контенту на локальних і хмарних серверах
2. Methods and means of cybersecurity analysis and protection of large language models from generating forbidden content on local and cloud servers

Реферат/анотація:

1. Мета дисертаційної роботи полягає в підвищенні точності оцінювання кібербезпеки та рівня захищеності великих мовних моделей (Large Language Models, LLMs) від генерації забороненого контенту шляхом аналізу критичності вразливостей, прогнозування кібератак на LLMs, які розгортаються локально і на хмарних серверах. У рамках загальної задачі розглядається розроблення методів та засобів аналізу критичності вразливостей, прогнозування кібератак на великі мовні моделі, які розгортаються локально і на хмарних серверах, та обґрунтування вибору і впровадження контрзаходів за визначеними критеріями. Часткові задачі включають аналіз методів та засобів оцінювання та забезпечення кібербезпеки, розроблення моделі кібербезпеки, розроблення методу аналізу критичності вразливостей, удосконалення методу оцінювання та

забезпечення кібербезпеки шляхом аналізу наслідків атак на вразливості та вибору контрзаходів, розроблення структури та елементів інформаційної технології (ІТ) оцінювання та забезпечення кібербезпеки. Вперше запропоновано модель кібербезпеки великих мовних моделей, яка, на відміну від відомих, надає теоретико-множинне представлення загроз, вразливостей та кібератак на модельному та системному рівнях, що надає змогу здійснювати подальший аналіз ризиків порушення, оцінювати рівень захищеності та визначати контрзаходи. Удосконалено метод аналізу критичності вразливостей великих мовних моделей шляхом вибору джерел даних з експлойтами, їх колекціонування та симулювання атак на моделі для статичної оцінки ймовірності та успішності атак, а також її комбінування з рівнем тяжкості наслідків для ризик-орієнтованого визначення критичності, що забезпечує підвищення повноти та достовірності оцінювання кібербезпеки. Дістав подальшого розвитку ІМЕКА (Intrusion Modes and Effects Criticality Analysis) метод оцінювання та забезпечення кібербезпеки великих мовних моделей шляхом аналізу наслідків атак на вразливості та вибору контрзаходів, що дозволяє забезпечити прийнятний ризик порушення кібербезпеки за наявності обмежень.

2. The dissertation aims to improve the accuracy of cybersecurity assessments and the level of protection of large language models (LLMs) against the generation of forbidden content by analyzing the criticality of vulnerabilities and predicting cyberattacks on LLMs deployed locally and on cloud servers. The overall objective involves the development of methods and means for the analysis of vulnerability criticality, the prediction of cyberattacks on large language models deployed locally and on cloud servers, and the substantiation of the selection and implementation of countermeasures according to specified criteria. The specific tasks include the analysis of methods and means of assessing and ensuring cybersecurity, the development of a cybersecurity model, the development of a method for analysis of the vulnerability criticality, the improvement of the method for assessing and ensuring cybersecurity by analyzing the effects of attacks on vulnerabilities and selecting countermeasures, and the development of the structure and elements of information technology for assessing and ensuring cybersecurity. For the first time, a cybersecurity model for large language models is proposed, which, in contrast to the known ones, provides a set-theoretical representation of threats, vulnerabilities, and cyberattacks at the model and system levels, which allows for further analysis of the risks of violations, assess the level of security, and determine countermeasures. The method of analysis of the criticality of vulnerabilities in large language models is improved by selecting data sources with exploits, collecting them, and simulating attacks on models for static assessment of the probability and success of attacks, and combining this with the severity of effects for risk-based criticality determination, which improves the completeness and reliability of cybersecurity assessment. The IMECA (Intrusion Modes and Effects Criticality Analysis) method of assessing and ensuring the cybersecurity of large language models is further developed by analyzing the effects of attacks on vulnerabilities and selecting countermeasures, which allows to ensure an acceptable risk of cybersecurity violation in the presence of constraints.

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. Neretin, O., Kharchenko, V. IMECA method of risk-based assessment and ensuring cybersecurity of Large Language Models. Herald of Advanced Information Technology. 2026, Vol. 9, No. 1, P. 60–70.
- 2. Неретін, О., Харченко, В. Метод аналізу критичності вразливостей великих мовних моделей. Measuring and computing devices in technological processes. 2026, № 1, С. 443–450.

- 3. Neretin, O., Kharchenko, V. Information Technology for Assessing and Ensuring Cybersecurity of Large Language Models. Security of Infocommunication Systems and Internet of Things. 2025, Vol. 3, No. 2, P. 02020.
- 4. Neretin, O., Kharchenko, V. A model of ensuring LLM cybersecurity. Radioelectronic and Computer Systems. 2025, Vol. 2025, No. 2, P. 201-215.

Наукова (науково-технічна) продукція: технології; методи, теорії, гіпотези

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 012211001065, 012413003250

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Харченко Вячеслав Сергійович
2. Vyacheslav Kharchenko

Кваліфікація: д. т. н., член-кор.НАН України, професор, 20.02.14

Ідентифікатор ORCID ID: 0000-0001-5352-077X

Додаткова інформація:

Повне найменування юридичної особи: Національний аерокосмічний університет "Харківський авіаційний інститут"

Код за ЄДРПОУ: 02066769

Місцезнаходження: вул. Манька Вадима, Харків, Харківський р-н., 61070, 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. Яцків Василь Васильович
2. Vasyl V. Yatskiv

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0001-9778-6625

Додаткова інформація: Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/G-4831-2017>; Scopus Author ID: 27468042400;

<https://scholar.google.com.ua/citations?hl=uk&user=o56LposAAAAJ>

Повне найменування юридичної особи: Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, Тернопіль, Тернопільський р-н., 46009, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Каштальян Антоніна Сергіївна

2. Kashtalian S. Antonina

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0002-4925-9713

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Тецький Артем Григорович

2. Artem H. Tetskyi

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

Ідентифікатор ORCID ID: 0000-0003-1745-2452

Додаткова інформація:

<https://www.scopus.com/authid/detail.uri?authorId=57202894656>; <https://scholar.google.com.ua/citations?user=tqripcQAAAAJ&hl=en>

Повне найменування юридичної особи: Національний аерокосмічний університет "Харківський авіаційний інститут"

Код за ЄДРПОУ: 02066769

Місцезнаходження: вул. Манька Вадима, Харків, Харківський р-н., 61070, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Брежнев Євген Віталійович

2. Yevhen V. Brezhniev

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний аерокосмічний університет "Харківський авіаційний інститут"

Код за ЄДРПОУ: 02066769

Місцезнаходження: вул. Манька Вадима, Харків, Харківський р-н., 61070, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

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

Лукін Володимир Васильович

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

Лукін Володимир Васильович

**Відповідальний за підготовку
облікових документів**

Дмитренко Євгенія Валеріївна

Реєстратор

Юрченко Тетяна Анатоліївна

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



Юрченко Тетяна Анатоліївна