# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0826U005370

**Особливі позначки:** відкрита

**Дата реєстрації:** 02-10-2026

**Статус:** Запланована

**Реквізити наказу МОН / наказу закладу:**

## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Підлісний Юрій Іванович

2. Yurii I. Pidlisnyi

**Кваліфікація:**

**Ідентифікатор ORCID ID:** 0009-0001-9783-3898

**Вид дисертації:** доктор філософії

**Аспірантура/Докторантура:** так

**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:**

**Спеціальність за освітою:** Комп`ютерні системи і мережі

**Місце роботи здобувача:** Національний університет "Чернігівська політехніка"

**Код за ЄДРПОУ:** 05460798

**Місцезнаходження:** вул. Шевченка, Чернігів, Чернігівський р-н., 14035, 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 17161

**Повне найменування юридичної особи:** Національний університет "Чернігівська політехніка"

**Код за ЄДРПОУ:** 05460798

**Місцезнаходження:** вул. Шевченка, Чернігів, Чернігівський р-н., 14035, 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 "Чернігівська політехніка"

**Код за ЄДРПОУ:** 05460798

**Місцезнаходження:** вул. Шевченка, Чернігів, Чернігівський р-н., 14035, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

## V. Відомості про дисертацію

**Мова дисертації:** Українська

**Коди тематичних рубрик:** 50.41.25, 50.05.13, 50.05.15, 50.05.17, 50.05.09

### Тема дисертації:

1. Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ

2. Methods and Models for Context-Adaptive Information Security Risk Assessment in IoT Environments

### Реферат/анотація:

1. Актуальність роботи. Розвиток Інтернету речей (Internet of Things, IoT), кіберфізичних систем, периферійних обчислень і промислового Інтернету речей (Industrial Internet of Things, IIoT) супроводжується ускладненням сучасних інформаційно-комунікаційних систем. IoT-середовища об’єднують пристрої з різним призначенням, обчислювальними можливостями та протоколами взаємодії. Їхній склад, конфігурація і зв’язки між компонентами можуть змінюватися під час експлуатації. Водночас зростає різноманітність кіберзагроз, здатних впливати як на окремі пристрої, так і на роботу середовища загалом. У дисертації розв’язано актуальне наукове завдання, що полягає в розробленні моделі формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації та удосконаленні методу оцінювання ризиків інформаційної безпеки IoT-середовищ у процесі аудиту. Під час визначення рівня ризику також враховується попередньо сформований показник ризику прихованої компрометації. Метою роботи є розроблення моделі побудови контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації та удосконалення методу оцінювання

ризиків інформаційної безпеки IoT-середовищ з урахуванням цього профілю, поточного стану безпеки й попередньо сформованого показника ризику прихованої компрометації під час аудиту. Для досягнення мети проаналізовано підходи до класифікації IoT-пристроїв, виявлення вразливостей, аналізу аномальної активності та оцінювання ризиків. Розроблено модель формування контекстно-ризикового профілю пристрою за результатами інтелектуально-контекстної класифікації. Удосконалено метод оцінювання ризиків на основі нечіткого логічного виведення типу Мамдані з урахуванням показника ризику прихованої компрометації BackdoorRisk. Визначено підхід до побудови інформаційної технології для узгодженого застосування моделі та методу. Запропоновані рішення перевірено з використанням відкритих наборів даних з безпеки IoT і програмно сформованих контекстно-ризикових сценаріїв. Наукова новизна одержаних результатів полягає в такому: – Вперше розроблено модель побудови контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Модель передбачає класифікацію пристрою за п'ятьма критеріями: рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища. Результати класифікації за кожним критерієм зберігаються в профілі без зведення до одного числового показника. – Удосконалено метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані. Метод передбачає спільне врахування семи вхідних параметрів: критичності активу, рівня загрози, рівня вразливості, можливостей потенційного порушника, імовірності реалізації загрози, тяжкості її наслідків та попередньо сформованого показника ризику прихованої компрометації BackdoorRisk. Параметри, що залежать від контексту, уточнюються з урахуванням профілю пристрою та даних про поточний стан безпеки. Показник BackdoorRisk надходить до системи як окремий вхідний параметр. – Набув подальшого розвитку підхід до побудови інформаційної технології оцінювання ризиків інформаційної безпеки IoT-середовищ. На відміну від відокремленого застосування класифікації пристроїв та оцінювання ризиків, підхід передбачає використання контекстно-ризикового профілю пристрою разом із даними про поточний стан безпеки для формування вхідних параметрів нечіткого оцінювання. Практичне значення одержаних результатів полягає у програмній реалізації модуля оцінювання ризиків інформаційної безпеки IoT-середовищ та окремої експериментальної процедури класифікації мережевих подій. Модуль реалізовано в середовищі MATLAB із використанням Fuzzy Logic Toolbox. Він обробляє сім попередньо сформованих вхідних параметрів, виконує нечітке логічне виведення типу Мамдані та визначає показник RiskLevel і відповідну категорію ризику. Експериментальну класифікацію мережевих подій досліджено окремо як засіб одержання відомостей про активність в IoT-середовищі. Впровадження результатів. Результати дисертаційного дослідження впроваджено у практичну діяльність ТОВ «ЛЮМ'ЄР ЕЛЕКТРО», ТОВ «АРКАДА ФІНАНС» і ТОВ «АТРІЯ КОМПАНІ» для аналізу стану інформаційної безпеки, оцінювання ризиків та аналізу аномальної мережевої активності. Окремі результати використовуються в освітньому процесі Національного університету «Чернігівська політехніка» під час підготовки фахівців з кібербезпеки та комп'ютерних наук. Одержані результати дають змогу формувати оцінку ризику з урахуванням характеристик IoT-пристрою, його контекстно-ризикового профілю та поточного стану безпеки. Визначений у роботі підхід до побудови інформаційної технології встановлює порядок спільного застосування розробленої моделі й удосконаленого методу в процесі аудиту IoT-середовищ.

2. Relevance of the research. The development of the Internet of Things (IoT), cyber-physical systems, edge computing, and the Industrial Internet of Things (IIoT) is accompanied by increasing complexity in modern information and communication systems. IoT environments bring together devices with different purposes, computing capabilities, and communication protocols. Their composition, configuration, and connections between components may change during operation. At the same time, the range of cyber threats capable of affecting both individual devices and the environment as a whole continues to grow. The dissertation addresses the scientific problem of developing and improving methods and models for context-adaptive information security risk assessment in IoT environments during security audits. The proposed solution combines intelligent context-aware device classification, the formation of contextual risk profiles, and fuzzy risk assessment. The risk level is also determined with consideration of a previously calculated hidden compromise risk indicator. The aim of the

research is to develop and improve methods and models for context-adaptive information security risk assessment in IoT environments that account for device characteristics, operating conditions, and the current security state and can be used during security audits. To achieve this aim, approaches to IoT device classification, vulnerability detection, anomalous activity analysis, and risk assessment were analyzed. A model for forming a device's contextual risk profile based on the results of intelligent context-aware classification was developed. A risk assessment method based on Mamdani fuzzy inference was improved by incorporating the hidden compromise risk indicator, BackdoorRisk An approach to building an information technology for the coordinated use of the model and method was defined. The proposed solutions were evaluated using open IoT security datasets and programmatically generated contextual risk scenarios. The scientific novelty of the results is as follows: – A model for forming an IoT device's contextual risk profile based on the results of intelligent context-aware classification was developed for the first time. The model classifies a device according to five criteria: its level of embedded intelligence, security characteristics, interaction architecture, functional context, and the dynamic nature of the environment. The classification results for each criterion are retained in the profile without being reduced to a single numerical value. – A method for context-adaptive information security risk assessment in IoT environments based on Mamdani fuzzy inference was improved. The method jointly considers seven input parameters: asset criticality, threat level, vulnerability level, attacker capability, likelihood of threat occurrence, severity of impact, and the previously calculated hidden compromise risk indicator, BackdoorRisk. Context-dependent parameters are refined using the device profile and data on the current security state. BackdoorRisk is supplied to the system as a separate input parameter. – The approach to building an information technology for information security risk assessment in IoT environments was further developed. The approach uses a device's contextual risk profile together with data on its current security state to form the input parameters for fuzzy risk assessment. The practical significance of the results lies in the software implementation of an information security risk assessment module for IoT environments and a separate experimental procedure for classifying network events. The module was implemented in MATLAB using the Fuzzy Logic Toolbox. It processes seven previously calculated input parameters, performs Mamdani fuzzy inference, and determines the RiskLevel value and corresponding risk category. The experimental classification of network events was studied separately as a means of obtaining information about activity in an IoT environment. Implementation of the results. The results of the dissertation research have been implemented in the operations of LUMIERE ELECTRO LLC, ARKADA FINANCE LLC, and ATRIYA COMPANY LLC for information security analysis, risk assessment, and anomalous network activity analysis. Some of the results are also used in the educational process at Chernihiv Polytechnic National University in the training of cybersecurity and computer science specialists. The results make it possible to assess risk with consideration of an IoT device's characteristics, its contextual risk profile, and the current security state. The proposed approach to building the information technology establishes a procedure for the combined use of the developed model and improved method during IoT security audits.

### Державний реєстраційний номер ДіР:

**Пріоритетний напрям розвитку науки і техніки:** Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

**Стратегічний пріоритетний напрям інноваційної діяльності:** Не застосовується

**Підсумки дослідження:** Теоретичне узагальнення і вирішення важливої наукової проблеми

### Публікації:


- 1. Pidlisnyi Yuriy, Intelligent-Contextual Model for the Classification of Internet of Things Environments // [Central Ukrainian Scientific Bulletin Technical Sciences]. 2025. № 12(43). С. 20–30. https://DOI: 10.32515/2664-262X.2025.12(43).1.20-30.

- 2. Mariia KAPUSTIAN, Yurii PIDLISNYI, Mykhailo SHELEST, Methods of Hiding Data in Computer Networks: From Classics to IoT and AI // [Computer systems and information technologies]. 2025. № 4–3. DOI: https://doi.org/10.31891/csit-2025-4-3.
- 3. Pidlisnyi Yuriy, Fuzzy Logic in IoT Security Risk Assessment: Rule Construction and Implementation // [Computer Science and Engineering]. 2025. № 3(41). С. 237–253. DOI: https://doi.org/10.25140/2411-5363-2025- 3(41)-237-253.
- 4. Pidlisnyi Yuriy , Audit of IoT Networks: Assessing Vulnerabilities and Protecting Against Cyber Attacks // [Computer Science and Engineering]. 2025. № 1(39). С. 170–183. DOI: https://doi.org/10.25140/2411-5363-2025- 1(39)-170-183.
- 5. Pidlisnyi Yuriy , Possible Ways to Improve Privacy in IoT Networks // [ Central Ukrainian Scientific Bulletin Technical Sciences]. 2025. № 11(42). С. 46–55. DOI: https://doi.org/10.32515/2664-262X.2025.11(42).1.46-55.
- 6. Підлісний Юрій, Використання алгоритмічних та технічних аспектів кібербезпеки в мережі IoT / Ю.І. Підлісний // Кібербезпека в сучасному світі: актуальні виклики : матеріали конференції. – Одеса, 2024. – С. 63– 64.
- 7. Підлісний Юрій, Технології захисту приватності в мережі IoT / Ю.І. Підлісний// Міжвідомчий міжрегіональний семінар наукової ради НАН України «Технічні засоби захисту інформації». – [Київ], [2025]. С.58- 60.
- 8. Підлісний Юрій, Мультиагентні системи для виявлення та нейтралізації кіберзагроз в IoT / Ю. І. Підлісний // Юність науки – 2025 : матеріали всеукраїнської наукової конференції молодих учених. – Чернігів, 2025. – С. 1124–1125.
- 9. Підлісний Юрій, Використання NetLogo для моделювання кібератак на IoT-системи / Ю.І. Підлісний // Безпека інформаційних технологій : матеріали XIV Міжнародної науково-технічної конференції (ITSec- 2025), 22–24 травня 2025 р. – Тернопіль, 2025. – С. 150–152.
- 10. Yuriy PIDLISNYI, Mykhailo SHELEST, Detection of Hidden Threats in IoT Systems Based on Kleptoaudit and Fuzzy Risk Assessment / Yuriy PIDLISNYI, Mykhailo SHELEST// Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей : матеріали V Міжнародної науково-практичної конференції (TTSIIT-2026). – [Київ], 2026. – С. 11– 15.
- 11. Підлісний Юрій, Шелест Михайло, Застосування нечітких продукційних правил для контекстно-довірчогооцінювання кіберризиків у середовищі Інтернету речей/ Ю.І. Підлісний, М.Є. Шелест // Безпека інформаційних технологій : матеріали XV Міжнародної науково-технічної конференції (ITSec-2025), 27–29 травня 2026 р. – Тернопіль, 2026. – С. 29–31.


**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. Шелест Михайло Євгенович

2. Mykhailo Y. Shelest

**Кваліфікація:** д. т. н., професор, 05.13.21

**Ідентифікатор ORCID ID:** 0000-0001-7110-4876

**Додаткова інформація:**

**Повне найменування юридичної особи:** Національний університет "Чернігівська політехніка"

**Код за ЄДРПОУ:** 05460798

**Місцезнаходження:** вул. Шевченка, Чернігів, Чернігівський р-н., 14035, 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. Хлапонін Юрій Іванович
2. Yuri I. Hlaponin

**Кваліфікація:** д. т. н., професор, 05.12.02

**Ідентифікатор ORCID ID:** 0000-0002-9287-0817

**Додаткова інформація:**

**Повне найменування юридичної особи:** Державний торговельно-економічний університет

**Код за ЄДРПОУ:** 44470624

**Місцезнаходження:** вул. Кіото, Київ, 02156, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

**Власне Прізвище Ім'я По-батькові:**

1. Хома Володимир Васильович
2. Volodymyr Khoma

**Кваліфікація:** д. т. н., професор, 05.11.05

**Ідентифікатор ORCID ID:** 0000-0001-9391-6525

**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:**

**Рецензенти**

**Власне Прізвище Ім'я По-батькові:**

1. Дорош Марія Сергіївна

2. Mariia S. Dorosh

**Кваліфікація:** д. т. н., професор, 05.13.22

**Ідентифікатор ORCID ID:** 0009-0006-2727-7992

**Додаткова інформація:** https://www.scopus.com/authid/detail.uri?authorId=56912183600; https://publons.com/researcher/3150165/mariia-dorosh/; https://www.researchgate.net/profile/Mariia_Dorosh2; https://scholar.google.com.ua/citations?hl=uk&user=saY6cfkAAAAJ; https://dblp.org/pid/256/0170.html

**Повне найменування юридичної особи:** Національний університет "Чернігівська політехніка"

**Код за ЄДРПОУ:** 05460798

**Місцезнаходження:** вул. Шевченка, Чернігів, Чернігівський р-н., 14035, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

**Власне Прізвище Ім'я По-батькові:**

1. Войцеховська Марія Михайлівна

2. Mariia M. Voitsekhovska

**Кваліфікація:** д.філософ, 122

**Ідентифікатор ORCID ID:** 0000-0002-1711-101X

**Додаткова інформація:**

**Повне найменування юридичної особи:** Національний університет "Чернігівська політехніка"

**Код за ЄДРПОУ:** 05460798

**Місцезнаходження:** вул. Шевченка, Чернігів, Чернігівський р-н., 14035, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

## VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові голови ради** Казимир Володимир Вікторович

| | |
|---|---|
| **Власне Прізвище Ім'я По-батькові головуючого на засіданні** | Казимир Володимир Вікторович |
| **Відповідальний за підготовку облікових документів** | Лисенко Наталія Володимирівна |
| **Реєстратор** | Юрченко Тетяна Анатоліївна |
| **Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності** | Юрченко Тетяна Анатоліївна |