

ВИСНОВОК
Національного університету «Чернігівська політехніка»
про наукову новизну, теоретичне та практичне значення результатів
дисертації Підлісного Юрія Івановича
на тему «Методи та моделі контекстно-адаптивного оцінювання ризиків
інформаційної безпеки IoT-середовищ», поданої на здобуття ступеня
доктора філософії
з галузі знань 12 – Інформаційні технології
за спеціальністю 122 – Комп'ютерні науки

1. Актуальність теми дослідження та її зв'язок з науково-дослідними роботами

IoT-середовища об'єднують пристрої з різним функціональним призначенням, обчислювальними можливостями та протоколами взаємодії. Їхній склад і конфігурація змінюються під час експлуатації, тому оцінювання ризиків інформаційної безпеки потребує врахування характеристик пристроїв, умов їх роботи та поточного стану безпеки. Неповнота даних і можливість прихованої компрометації додатково ускладнюють визначення рівня ризику.

Класифікація пристроїв, аналіз мережевих подій і оцінювання ризиків у відомих підходах часто виконуються окремо. Дисертація спрямована на узгоджене використання цих відомостей під час формування контекстно-ризикового профілю та вхідних параметрів нечіткої системи оцінювання. Це визначає актуальність теми для галузі інформаційних технологій.

Роботу виконано в Національному університеті «Чернігівська політехніка» в межах науково-дослідних робіт: «Методологія побудови захищеного кіберпростору» (державний реєстраційний номер 0124U004485, 2024–2027 рр.); «Моделі та методи забезпечення безпеки й довіри в кіберпросторі з урахуванням клептографічних загроз» (0126U001352, 2026–2028 рр.); «Методи й моделі забезпечення цілісності даних у каналах керування БпЛА в умовах застосування засобів РЕБ» (0125U001728, 2025–2026 рр.).

2. Мета і завдання дослідження

Метою дослідження є підвищення обґрунтованості оцінювання ризиків інформаційної безпеки IoT-середовищ у процесі аудиту шляхом розроблення та удосконалення методів і моделей, що враховують контекст функціонування IoT-пристроїв, поточний стан безпеки та попередньо сформований показник ризику прихованої компрометації за неповноти й невизначеності вхідних даних.

Для досягнення мети в дисертації вирішено такі завдання:

1. Проаналізовано методи класифікації IoT-пристроїв, аналізу стану безпеки та оцінювання ризиків; визначено їхні обмеження в динамічних IoT-середовищах.

2. Розроблено модель формування контекстно-ризикового профілю пристрою за результатами інтелектуально-контекстної класифікації.

3. Удосконалено метод контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення типу Мамдані з урахуванням показника BackdoorRisk.

4. Розвинуто підхід до побудови інформаційної технології; визначено її архітектуру, компоненти, потоки даних і порядок повторного оцінювання.

5. Проведено програмну реалізацію та експериментальну перевірку запропонованих рішень на відкритих наборах даних і програмно сформованих сценаріях.

Об'єкт дослідження – процеси оцінювання ризиків інформаційної безпеки IoT-середовищ під час аудиту. Предмет дослідження – методи та моделі контекстно-адаптивного оцінювання ризиків, що використовують контекстно-ризикові профілі пристроїв, нечітке логічне виведення та показник ризику прихованої компрометації.

3. Наукові положення, розроблені особисто здобувачем, та їх новизна

У дисертаційній роботі розв'язано науково-прикладне завдання розроблення та удосконалення методів і моделей контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ у процесі аудиту. Основні результати, що визначають наукову новизну дослідження, полягають у такому.

Вперше запропоновано:

модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Вона враховує п'ять критеріїв: рівень вбудованого інтелекту, характеристики безпеки, архітектуру взаємодії, функціональний контекст і динамічність середовища. Результати класифікації зберігаються у профілі без зведення до одного числового показника та використовуються для визначення й інтерпретації параметрів оцінювання ризику.

Удосконалено:

метод контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення типу Мамдані. Метод спільно враховує критичність активу, рівні загрози та вразливості, можливості потенційного порушника, імовірність реалізації загрози, тяжкість наслідків і попередньо сформований показник BackdoorRisk. Контекстно залежні параметри уточнюються з урахуванням профілю пристрою та поточного стану безпеки. За результатами виведення визначається показник RiskLevel.

Набув подальшого розвитку: підхід до побудови інформаційної технології контекстно-адаптивного оцінювання ризиків. Контекстно-ризикові профілі та дані про стан безпеки використовуються для формування вхідних параметрів оцінювання. Визначено архітектуру, склад компонентів та інформаційні потоки між ними; зміна характеристик пристроїв або стану середовища передбачає оновлення параметрів і повторне оцінювання ризику.

Основні результати дослідження конкретизовано в моделі формування контекстно-ризикового профілю IoT-пристрою, методі нечіткого оцінювання ризиків та підході до побудови інформаційної технології їх спільного застосування. Модель класифікує пристрої за п'ятьма критеріями й зберігає

одержані характеристики в профілі, який використовується для формування та інтерпретації параметрів ризику. Метод на основі нечіткого логічного виведення типу Мамдані враховує сім вхідних параметрів, зокрема показник ризику прихованої компрометації BackdoorRisk, і визначає інтегральний показник RiskLevel.

Розроблено архітектуру інформаційної технології, яка визначає склад компонентів, інформаційні потоки та порядок оновлення вхідних даних і повторного оцінювання ризику за зміни стану IoT-середовища. Модуль нечіткого оцінювання ризиків програмно реалізовано в MATLAB із використанням Fuzzy Logic Toolbox. Його перевірено на програмно сформованих контекстно-ризикових сценаріях; класифікацію мережевих подій окремо досліджено на відкритих наборах даних з безпеки IoT.

4. Обґрунтованість та достовірність наукових положень, висновків і рекомендацій

Обґрунтованість результатів забезпечується аналізом досліджень і підходів до управління ризиками, формалізацією контекстно-ризикового профілю, визначенням семи вхідних змінних системи Мамдані, функцій належності та бази з 40 продукційних правил. Реалізацію перевірено аналізом спрацьовування правил, поверхонь нечіткого виведення та покомпонентної монотонності.

Для дослідження класифікації мережевих подій використано дані BoT-IoT, TON-IoT та Edge-IoTset. На незалежній тестовій частині з 4105 записів XGBoost досяг Accurasy 0,9481 і F1-міри 0,9374. Окремо FIS-модель перевірено на незалежній тестовій частині з 40 000 програмно сформованих контекстно-ризикових сценаріїв; отримано Accurasy 0,971175, F1-міру 0,982012 та FPR 0,078250.

Вплив контексту перевірено порівнянням із контрольною конфігурацією та почерговим усуненням уточнення окремих параметрів. Досліджено також вплив BackdoorRisk, пропущених значень і час виконання нечіткого виведення, який у дослідженій реалізації в середньому становив 0,0543 мс на запис.

Кількісну валідацію FIS виконано на програмно сформованих сценаріях. Наведені показники характеризують саме ці умови перевірки; подальша апробація на реальних потоках IoT-даних є окремим завданням.

5. Теоретичне та практичне значення результатів дисертаційного дослідження

Теоретичне значення полягає в розвитку модельних і методичних засад контекстно-адаптивного оцінювання ризиків IoT-середовищ. Показано зв'язок між характеристиками пристрою, його контекстно-ризиковим профілем, параметрами нечіткої системи та інтегральним показником RiskLevel.

Практичне значення полягає у програмній реалізації модуля оцінювання ризиків у MATLAB із використанням Fuzzy Logic Toolbox та окремих експериментальній перевірці класифікації мережевих подій. Модуль обробляє сім сформованих вхідних параметрів і визначає показник та категорію ризику.

Архітектура повної інформаційної технології описана у дисертації; обсяг програмної реалізації слід розуміти в межах перевірених компонентів.

Практичне значення одержаних результатів підтверджується їх упровадженням у діяльність ТОВ «ЛЮМ'ЄР ЕЛЕКТРО», ТОВ «АРКАДА ФІНАНС» і ТОВ «АТРІЯ КОМПАНІ». Результати роботи використовуються під час аналізу стану інформаційної безпеки IoT-середовищ, оцінювання ризиків і виявлення аномальної мережевої активності. Це дає змогу враховувати характеристики пристроїв та поточний стан середовища під час визначення пріоритетності заходів захисту. Окремі результати дослідження також використовуються в освітньому процесі Національного університету «Чернігівська політехніка» під час підготовки здобувачів освіти за напрямками кібербезпеки та комп'ютерних наук.

6. Апробація результатів дослідження

Основні положення та результати дисертаційної роботи доповідалися й обговорювалися на наукових конференціях і семінарах, зокрема: конференції «Кібербезпека в сучасному світі: актуальні виклики» (Одеса, 2024 р.); Всеукраїнській науковій конференції молодих учених «Юність науки – 2025» (Чернігів, 2025 р.); XIV Міжнародній науково-технічній конференції «Безпека інформаційних технологій» (ITSec-2025, Тернопіль, 22–24 травня 2025 р.); V Міжнародній науково-практичній конференції «Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей» (TTSIT-2026, Київ, 24–25 березня 2026 р.); XV Міжнародній науково-технічній конференції «Безпека інформаційних технологій» (ITSec-2026, Тернопіль, 27–29 травня 2026 р.). Окремі результати також представлено на міжвідомчому міжрегіональному семінарі Наукової ради НАН України «Технічні засоби захисту інформації» (2025 р.).

7. Повнота викладення основних наукових результатів дисертації в публікаціях та особистий внесок автора

Основні результати дисертаційного дослідження відображено в 11 опублікованих наукових працях: п'яти статтях у наукових фахових виданнях України та шести публікаціях у матеріалах наукових конференцій. Шоста стаття, присвячена аудиту безпеки IoT-середовищ і виявленню прихованих загроз, пройшла рецензування та готується до публікації у виданні серії *Lecture Notes in Networks and Systems* видавництва Springer, що індексується в Scopus

У працях висвітлено класифікацію IoT-пристроїв і формування контекстно-ризикових профілів, оцінювання ризиків із застосуванням нечіткого логічного виведення, аналіз мережевої активності та врахування загроз прихованої компрометації.

Список публікацій здобувача за темою дисертації

Наукові праці з основними науковими результатами дисертації:

1. Pidlisnyi Y. Intelligent-Contextual Model for the Classification of Internet of Things Environments. *Central Ukrainian Scientific Bulletin. Technical Sciences*. 2025. № 12 (43). С. 20–30. DOI: 10.32515/2664-262X.2025.12(43).1.20-30. *Праця виконана одноосібно. У ній представлено модель класифікації IoT-середовищ з урахуванням їхніх контекстних характеристик.*

2. Kapustian M., Pidlisnyi Y., Shelest M. Methods of Hiding Data in Computer Networks: From Classics to IoT and AI. *Computer Systems and Information Technologies*. 2025. № 4–3. DOI: 10.31891/csit-2025-4-3. *Особистий внесок здобувача: дослідження способів прихованого передавання даних та пов'язаних із ними загроз у середовищах IoT.*

3. Pidlisnyi Y. Fuzzy Logic in IoT Security Risk Assessment: Rule Construction and Implementation. *Computer Science and Engineering*. 2025. № 3 (41). С. 237–253. DOI:10.25140/2411-5363-2025-3(41)-237-253. *Праця виконана одноосібно. У ній розглянуто побудову правил і реалізацію нечіткої системи оцінювання ризиків безпеки IoT.*

4. Pidlisnyi Y. Audit of IoT Networks: Assessing Vulnerabilities and Protecting Against Cyber Attacks. *Computer Science and Engineering*. 2025. № 1 (39). С. 170–183. DOI:10.25140/2411-5363-2025-1(39)-170-183. *Праця виконана одноосібно. У ній досліджено оцінювання вразливостей і захист від кібератак у процесі аудиту IoT-мереж.*

5. Pidlisnyi Y. Possible Ways to Improve Privacy in IoT Networks. *Central Ukrainian Scientific Bulletin. Technical Sciences*. 2025. № 11 (42). С. 46–55. DOI:10.32515/2664-262X.2025.11(42).1.46-55.

Праця виконана одноосібно. У ній досліджено підходи до захисту приватності в IoT-мережах

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Підлісний Ю. І. Використання алгоритмічних та технічних аспектів кібербезпеки в мережі IoT. *Кібербезпека в сучасному світі: актуальні виклики* : матеріали конференції. Одеса, 2024. С. 63–64.

7. Підлісний Ю. І. Технології захисту приватності в мережі IoT. *Міжвідомчий міжрегіональний семінар Наукової ради НАН України «Технічні засоби захисту інформації»*. 2025. С. 58–60. *Праця виконана одноосібно.*

8. Підлісний Ю. І. Мультиагентні системи для виявлення та нейтралізації кіберзагроз в IoT. *Юність науки – 2025* : матеріали Всеукраїнської наукової конференції молодих учених. Чернігів, 2025. С. 1124–1125. *Праця виконана одноосібно.*

9. Підлісний Ю. І. Використання NetLogo для моделювання кібератак на IoT-системи. *Безпека інформаційних технологій* : матеріали XIV Міжнародної науково-технічної конференції ITSec-2025 (Тернопіль, 22–24 травня 2025 р.). Тернопіль, 2025. С. 150–152. *Праця виконана одноосібно.*

10. Pidlisnyi Y., Shelest M. Detection of Hidden Threats in IoT Systems Based on Kleptoaudit and Fuzzy Risk Assessment. *Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей* : матеріали V Міжнародної науково-практичної конференції TTSIT-2026. Київ, 2026. С. 11–15.

Особистий внесок здобувача: дослідження врахування прихованих загроз під час нечіткого оцінювання ризиків IoT-середовищ.

11. Підлісний Ю. І., Шелест М. Є. Застосування нечітких продукційних правил для контекстно-довірчого оцінювання кіберризиків у середовищі Інтернету речей. *Безпека інформаційних технологій* : матеріали XV Міжнародної науково-технічної конференції ITSec-2026 (Тернопіль, 27–29 травня 2026 р.). Тернопіль, 2026. С. 29–31. *Особистий внесок здобувача: розроблення та застосування нечітких продукційних правил для оцінювання ризиків у середовищі IoT.*

Стаття, що готується до публікації:

Pidlisnyi Y., Morozov A., Klymenko V. P., Ievlev N. G. *Methodology for Auditing IoT Security: Identification of Backdoors and Kleptographic Backdoors in Dynamic Environments*. Стаття пройшла рецензування та готується до публікації у збірнику матеріалів конференції MODS 2025 серії *Lecture Notes in Networks and Systems* видавництва Springer.

8. Загальний висновок

Дисертаційна робота Підлісного Юрія Івановича на тему «Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ» є самостійним завершеним науковим дослідженням, у якому розв'язано актуальне науково-прикладне завдання підвищення ефективності онлайн-виявлення та ідентифікації відмов напівпровідникових перетворювачів електроенергії.

Основні наукові положення містять наукову новизну, належно обґрунтовані та підтверджені моделюванням і експериментальними дослідженнями. Одержані результати мають теоретичне та практичне значення, пройшли апробацію й відображені в наукових публікаціях здобувача. Зміст роботи відповідає поставленій меті та завданням, роботу виконано державною мовою.

За актуальністю, науковою новизною, обґрунтованістю та практичною цінністю результатів дисертація відповідає спеціальності 122 «Комп'ютерні науки» та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261 (зі змінами). Основні наукові результати опубліковано з дотриманням вимог пункту 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами).

Рекомендувати дисертацію Підлісного Юрія Івановича на тему «Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ» до публічного захисту в разовій спеціалізованій вченій раді для присудження Підлісному Юрію Івановичу ступеня доктора філософії в галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Головуючий
завідувач кафедри інформаційних
та комп'ютерних систем,
к.т.н., доцент



Роговенко А. І.



Підпис: Роговенко А.І.

Засвідчую

відділ кадрів

7 09 2026 р.