

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U002753

Особливі позначки: відкрита

Дата реєстрації: 22-06-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: № НСВС/60/26 від 13.08.2026



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Шибает Геннадій Дмитрович

2. Hennadii D. Shybaiev

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0009-3131-812X

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: 22-07-2026

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Організація відсутня

Код за ЄДРПОУ: 00000000

Місцезнаходження: -----, Київ, 00000, Україна

Форма власності: Змішана

Сфера управління:

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 14655

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.01

Тема дисертації:

1. Методи адаптивної еволюції довіри у федеративному навчанні для кіберзахисту енергетичних мікромереж
2. Methods of adaptive evolution of trust in federal developments for cyber protection of energy micro-disruptions

Реферат/анотація:

1. Шибаєв Г. Д. Методи адаптивної еволюції довіри у федеративному навчанні для кіберзахисту енергетичних мікромереж. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека. – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, 2026. Дисертаційну роботу присвячено розробленню моделей і методів довірчо-орієнтованого федеративного навчання для виявлення аномалій у розподілених енергетичних мікромережах. Актуальність дослідження зумовлена цифровізацією енергетичних систем, поширенням відновлюваних джерел енергії, інтелектуальних лічильників, сенсорних мереж і локальних контролерів, що перетворюють мікромережі на складні кіберфізичні системи. У таких умовах інформаційні атаки, помилки телеметрії, деградація сенсорів або компрометація вузлів можуть впливати не лише на дані, а й на фізичні режими генерації, споживання,

накопичення та балансування енергії. Метою роботи є розроблення моделей і методів довірчо-орієнтованого федеративного навчання для виявлення аномалій у мікромережах, які підвищують стійкість глобальної моделі до атак отруєння, локального концептуального дрейфу та ненадійної поведінки окремих вузлів. Об'єктом дослідження є кібербезпека та кіберстійкість розподілених енергетичних мікромереж як кіберфізичних систем. Предметом дослідження є методи, моделі та алгоритми довірчо-орієнтованого федеративного навчання для кіберзахисту мікромереж. У роботі обґрунтовано доцільність використання федеративного навчання як підходу, що дає змогу будувати спільну модель без централізації сирих локальних даних. Показано, що класичний алгоритм FedAvg є недостатньо стійким в умовах статистичної неоднорідності, часткової участі клієнтів, дрейфу даних, шкідливих оновлень і атак отруєння. Для подолання цих обмежень запропоновано узагальнений метод довірчо-орієнтованого федеративного навчання, який поєднує локальне LSTM-орієнтоване виявлення аномалій, багатофакторне оцінювання поведінкової надійності вузлів, байесівське оновлення довіри, довірчо-зважену агрегацію параметрів моделей та адаптивне керування участю клієнтів у федеративних раундах. Наукова новизна роботи полягає в розробленні методу довірчо-орієнтованого федеративного навчання для мікромереж; удосконаленні механізму федеративної агрегації шляхом урахування рейтингу довіри до клієнтів; удосконаленні моделі адаптивного оцінювання довіри на основі багатофакторних поведінкових доказів; подальшому розвитку застосування LSTM-моделей для виявлення аномалій у часових рядах енергетичних параметрів. Для формування довіри враховано геометричну узгодженість локального оновлення з глобальним напрямом, вплив оновлення на валідаційну якість, стабільність участі вузла, локальну інтенсивність аномалій, фізичну правдоподібність поведінки та нормове відхилення оновлення. Експериментальну перевірку проведено в середовищі з шістьма вузлами мікромережі, які моделюють фотоелектричні підсистеми, розумний лічильник, вузол накопичення енергії, контролер навантаження та потенційно ненадійний вузол. Розглянуто нормальний сценарій, сценарій отруєння, сценарій дрейфу та комбінований сценарій. Показано, що запропонований метод зберігає стабільну збіжність у нормальних умовах і забезпечує вищу стійкість до атак порівняно з FedAvg. У сценарії отруєння середньоквадратична помилка FedAvg зростала до 0,181, тоді як для запропонованого методу залишалася близько 0,102; Recall зростав з 0,73 до 0,88, а FPR зменшувався з 0,19 до 0,07. Практичне значення результатів полягає в можливості використання запропонованих моделей і методів при створенні захищених систем моніторингу та виявлення аномалій у мікромережах, smart grid-платформах, розподілених енергетичних системах та інших кіберфізичних середовищах, де необхідно поєднати локальність даних, колективне навчання, стійкість до ненадійних вузлів і своєчасне виявлення небезпечних відхилень. Ключові слова: мікромережа, кібербезпека, федеративне навчання, критична інфраструктура, довірчо-орієнтована агрегація, LSTM, виявлення аномалій, концептуальний дрейф, отруєння моделі, кіберфізична система.

2. Shybaiev H. D. Adaptive Trust Evolution Methods in Federated Learning for Cybersecurity of Energy Microgrids. – Qualifying scientific work as a manuscript. Dissertation for the degree of Doctor of Philosophy in Field of Knowledge 12 – Information Technology, Specialty 125 – Cybersecurity. – National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, 2026. The dissertation is devoted to the development of models and methods of trust-aware federated learning for anomaly detection in distributed energy microgrids. The relevance of the research is determined by the digital transformation of power systems, the spread of renewable energy sources, smart meters, sensor networks, energy storage units, and local controllers, which transform microgrids into complex cyber-physical systems. Under such conditions, information attacks, telemetry manipulation, sensor degradation, or compromised nodes may affect not only data flows but also physical processes of generation, consumption, storage, and power balancing. The aim of the dissertation is to develop models and methods of trust-aware federated learning for anomaly detection in microgrids that increase the robustness of the global model against poisoning attacks, local concept drift, and unreliable behavior of individual nodes. The object of the research is the cybersecurity and cyber-resilience of distributed energy microgrids as cyber-physical systems. The subject of the research is methods, models, and algorithms of trust-aware federated learning for microgrid cyber defense. The work substantiates the use of federated learning as an approach that

enables collaborative model training without centralizing raw local data. It is shown that the classical FedAvg algorithm is insufficiently robust under statistical heterogeneity, partial client participation, data drift, malicious updates, and poisoning attacks. To overcome these limitations, a generalized method of trust-aware federated learning is proposed. The method integrates local LSTM-based anomaly detection, multi-factor assessment of behavioral reliability of nodes, Bayesian trust updating, trust-weighted aggregation of model parameters, and adaptive control of client participation in federated rounds. The scientific novelty of the dissertation consists in the development of a trust-aware federated learning method for microgrids; the improvement of the federated aggregation mechanism by introducing client trust scores; the improvement of an adaptive trust assessment model based on multi-factor behavioral evidence; and the further development of LSTM-based anomaly detection in time series of energy parameters. Trust formation takes into account the geometric consistency of a local update with the global direction, the influence of the update on validation quality, the stability of node participation, local anomaly intensity, physical plausibility of node behavior, and norm deviation of the update. The experimental evaluation was performed in an environment with six microgrid nodes modeling photovoltaic subsystems, a smart meter, an energy storage node, a load controller, and a potentially unreliable node. Normal operation, poisoning, drift, and combined scenarios were considered. The results show that the proposed method maintains stable convergence under normal conditions and provides higher robustness to attacks compared with FedAvg. In the poisoning scenario, the mean squared error of FedAvg increased to 0.181, whereas for the proposed method it remained approximately 0.102; Recall increased from 0.73 to 0.88, and FPR decreased from 0.19 to 0.07. The practical significance of the results lies in the possibility of using the proposed models and methods for developing protected monitoring and anomaly detection systems in microgrids, smart grid platforms, distributed energy systems, and other cyber-physical environments where data locality, collaborative learning, resilience to unreliable nodes, and timely detection of dangerous deviations must be combined. Keywords: microgrid, cybersecurity, federated learning, critical infrastructure, trust-aware aggregation, LSTM, anomaly detection, concept drift, model poisoning, cyber-physical system.

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:

- Шибаєв Г. Д., Гальчинський Л. Ю. Застосування методів машинного навчання для виявлення роботи кейлогерів в операційній системі. Інформатика та математичні методи в моделюванні. 2024. Т. 14, № 3. С. 249–258. <https://doi.org/10.15276/imms.v14.no3.249>
- Shybaiev H., Halchynskiy L. Detecting the operation of keyloggers using the dendritic cell algorithm with multiple resolutions. Theoretical and Applied Cybersecurity. 2025. Vol. 7, No. 2. P. 53–63. <https://doi.org/10.20535/tacs.2664-29132025.2.337840>
- Шибаєв Г. Федеративне виявлення аномалій на основі LSTM з адаптацією до локального контексту. Інформаційні технології та суспільство. 2025. № 3(18). С. 198–204. <https://doi.org/10.32689/maup.it.2025.3.26>
- Шибаєв Г., Гальчинський Л. Довіро-зважена агрегація у федеративному навчанні для мікромереж. Herald of Khmelnytskyi National University. Technical Sciences. 2025. Vol. 359, No. 6.2. P. 56–63. <https://doi.org/10.31891/2307-5732-2025-359-77>
- Шибаєв Г., Гальчинський Л. Застосування методів машинного навчання для виявлення роботи кейлогерів в операційній системі. Інформаційні технології та безпека : матеріали XXIV Міжнародної науково-практичної конференції ІТБ-2024. Київ : Інжиніринг, 2024. С. 101–103.

- Shybaiev H. Detecting the operation of keyloggers using the dendritic cell algorithm with multiple resolutions. 2024 IEEE 5th International Conference on Advanced Trends in Information Theory. Lviv, Ukraine, 21–23 Nov. 2024.
- Шибаєв Г., Гальчинський Л. Виявлення роботи кейлоггерів допомогою алгоритму дендритної клітинки з багаторазовою роздільною здатністю. Grail of Science. 2023. № 30. С. 173–176.
- Шибаєв Г., Гальчинський Л. Виявлення витоку інформації в ядрі Linux за допомогою методу багатоваріаційного виконання. Collection of scientific papers «Scientia». Sydney, Australia, June 10, 2022. С. 64–68.

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

Соціально-економічна спрямованість: підвищення автоматизації виробничих процесів; підвищення кіберстійкості та безпеки об'єктів критичної енергетичної інфраструктури.

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. Гальчинський Леонід Юрійович
2. Leonid Y. Galchynsky

Кваліфікація: к.т.н., доцент, 05.13.03

Ідентифікатор ORCID ID: 0000-0002-3805-1474

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Циганок Віталій Володимирович
2. Vitaliy V. Tsyganok

Кваліфікація: д.т.н., професор, 01.05.04

Ідентифікатор ORCID ID: 0000-0002-0821-4877

Додаткова інформація:

Повне найменування юридичної особи: Інститут проблем реєстрації інформації Національної академії наук України

Код за ЄДРПОУ: 03771755

Місцезнаходження: вул. М. Шпака, Київ, 03113, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Лаптев Олександр Анатолійович

2. Oleksandr Laptiev

Кваліфікація: д. т. н., старший науковий співробітник, 05.13.21

Ідентифікатор ORCID ID: 0000-0002-4194-402X

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, Київ, 01033, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Пишнограєв Іван Олександрович

2. Ivan O. Pyshnohraiev

Кваліфікація: к. ф.-м. н., доц., 01.05.04

Ідентифікатор ORCID ID: 0000-0002-3346-8318

Додаткова інформація: ;<https://scholar.google.com/citations?user=9qVIOVYAAAAJ&hl=en>

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Хайдуров Владислав Володимирович

2. Vladyslav V. Khaidurov

Кваліфікація: к. т. н., с.д., 01.05.02

Ідентифікатор ORCID ID: 0000-0002-4805-8880

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

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

Ланде Дмитро Володимирович

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

Ланде Дмитро Володимирович

**Відповідальний за підготовку
облікових документів**

Шибает Геннадій Дмитрович

Реєстратор

Юрченко Тетяна Анатоліївна

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



Юрченко Тетяна Анатоліївна