Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії Чепель Леонід Валерійович 1995 року народження, громадянин України, освіта вища: закінчив у 2019 році Київський національний університет імені Тараса Шевченка за спеціальністю 123 «Комп'ютерна інженерія», виконав акредитовану освітньо-наукову програму 123 «Комп'ютерна інженерія».

Разова спеціалізована вчена рада, утворена наказом Київського національного університету імені Тараса Шевченка, Міністерства освіти і науки України, м. Київ від 09.07.2026 року № 380-34, у складі:

Голови разової спеціалізованої вченої ради -	**Володимира ЗАСЛАВСЬКОГО**, доктора технічних наук, професора, професора кафедри математичної інформатики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка;
Рецензентів -	**Сергія ДАКОВА**, кандидата технічних наук, доцента, доцента кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;
	Сергія ПАЛІЯ, кандидата технічних наук, доцента, доцента кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;
Офіційних опонентів -	**Ярослава ДОРОГОГО**, доктора технічних наук, професора, завідувача кафедри штучного інтелекту та кібербезпеки ДВНЗ «Донецький національний технічний університет»;
	Олексія НАЛАПКА, доктора філософії, докторанта (штатного) науково-організаційного відділу Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

на засіданні 10 вересня 2026 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології Чепелю Леоніду Валерійовичу на підставі публічного захисту дисертації «**Методи і засоби побудови мереж Інтернету речей на основі гібридної блокчейн-архітектури з адаптивним консенсусом та мультифакторним управлінням вузлами**» за спеціальністю 123 «Комп'ютерна інженерія».

Дисертацію виконано на кафедрі комп'ютерної інженерії факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, Міністерства освіти і науки України, м. Київ.

Науковий керівник – **Бойко Юрій Володимирович,** кандидат фізико-математичних наук, доцент, завідувач кафедри комп'ютерної інженерії факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка.

Дисертацію подано у вигляді спеціально підготовленого рукопису українською мовою, що повністю відповідає вимогам пункту 6 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 року № 44 (зі змінами), та містить науково обґрунтовані результати, а саме:

- Проведено порівняльний аналіз блокчейн-платформ Ethereum PoS, Ethereum PoA (Clique), Hyperledger Fabric та DAG-рішень за єдиною системою критеріїв (затримка, пропускна здатність, використання ресурсів, безпека, придатність для апаратно обмежених пристроїв) та критеріальних методів вибору вузлів у блокчейн-мережах Інтернету речей. Встановлено, що жодна з наявних платформ не поєднує одночасно низьку затримку, підтримку апаратно обмежених пристроїв, масштабованість, безпеку та координацію вузлів для розподілу обчислювальних задач, на підставі чого обґрунтовано доцільність гібридного підходу та сформульовано задачі дослідження. Результати аналізу мають самостійну методичну цінність як основа для вибору платформи проєктувальниками розподілених систем.
- Удосконалено модель гібридної багаторівневої блокчейн-архітектури для мереж Інтернету речей, яка, на відміну від відомих рішень, використовує тришарову кластерну організацію: рівень сенсорів із симетричним шифруванням для апаратно обмежених пристроїв, рівень локальної блокчейн-мережі з підтримкою смарт-контрактів та адаптивним консенсусом, рівень зовнішньої блокчейн-мережі з агрегацією транзакцій. Вибір типу блокчейну на кожному рівні обґрунтовано на основі порівняльного аналізу за критеріями пропускної здатності, безпеки та придатності для IoT, що забезпечує побудову масштабованої, децентралізованої та безпечної мережі з підтримкою гетерогенних пристроїв та можливістю автономної роботи кластерів.
- Вперше запропоновано метод адаптивного консенсусу Proof of Indicators (PoI) для блокчейн-мереж Інтернету речей, який, на відміну від інших реалізацій, впроваджує динамічний механізм вибору валідаторів на основі комплексної метрики ефективності, техніку поширення компактних блоків з передачею хешів транзакцій замість повних даних та конфігуровану затримку генерації блоків позачерговими вузлами для зменшення ймовірності розгалужень ланцюга. Метод реалізовано мовою Go на базі Go-Ethereum; експериментальне дослідження у Docker-середовищі з 15 вузлами продемонструвало зменшення мережевого трафіку на 20,5 %, скорочення кількості розгалужень ланцюга на 80 %, підвищення пропускної здатності до 10 % та зменшення часу поширення блоків на 8,5 % порівняно з базовим протоколом Clique.
- Удосконалено модель вибору вузлів для блокчейн-координованих периферійних обчислень у мережах Інтернету речей, яка, на відміну від відомих підходів, використовує мультифакторну скорингову функцію мультиплікативної композиції,

що поєднує репутацію вузла та метрики реального часу (доступність процесора і пам'яті, ємність черги задач, актуальність метрик, часові гарантії) із розділенням обчислень поза блокчейном та координації через смарт-контракти. Це дає змогу запобігти концентрації задач на перевантажених вузлах та забезпечити автоматичне балансування навантаження з лінійною обчислювальною складністю. Модель реалізовано на базі смарт-контрактів Solidity та Python-агентів і перевірено експериментально.

Результати дисертаційної роботи впроваджено у практичну діяльність ТОВ «ГРЕВАХ УКРАЇНА» (м. Київ) у вигляді системи на базі консенсусу Proof of Indicators для моніторингу роботи верстатів та координації роботи виробничих майданчиків без залучення хмарної інфраструктури (акт впровадження № 25-3 від 30.04.2026) та в операційну діяльність компанії WIREX LIMITED (Лондон, Велика Британія) у вигляді мультифакторного гібридного підходу до блокчейн-координованих периферійних обчислень, застосованого для балансування навантаження обчислювальних вузлів у децентралізованій інфраструктурі (сертифікат впровадження від 05.05.2026).

Здобувач має 10 наукових публікацій за темою дисертації, з них 4 статті опубліковані у наукових виданнях, включених до переліку фахових видань України (1 стаття категорії А та 3 статті категорії Б), опубліковано 6 тез доповідей на наукових конференціях. Перелік статей здобувача за темою дисертації:

1. Чепель, Л. В., & Бойко, Ю. В. (2024). Підхід до безпеки та організації мереж IoT з використанням блокчейн технології. Вісник Вінницького політехнічного інституту, (4), 129–138. https://doi.org/10.31649/1997-9266-2024-175-4-129-138

2. Чепель, Л. В., & Бойко, Ю. В. (2025). Побудова мереж IOT військового призначення з використанням блокчейн технології. Information Technology: Computer Science, Software Engineering and Cyber Security, (2), 186–194. https://doi.org/10.32782/IT/2025-2-19

3. Chepel, L., & Boyko, Y. (2026). Proof-of-Indicators: development and validation of an adaptive consensus mechanism for Internet of Things blockchain networks. Technology Audit and Production Reserves, 2(2(88)), 15–24. https://doi.org/10.15587/2706-5448.2026.356851

4. Chepel, L., & Boyko, Y. (2026). Multi-factor hybrid approach for blockchain-enabled IoT edge computing. Computer Systems and Information Technologies, (1), 78–87. https://doi.org/10.31891/csit-2026-1-8

У дискусії взяли участь (голова, рецензенти, офіційні опоненти, інші присутні) та висловили зауваження:

Володимир ЗАСЛАВСЬКИЙ, доктор технічних наук, професор, професор кафедри математичної інформатики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка.

Оцінка позитивна, без зауважень.

Юрій БОЙКО, кандидат фізико-математичних наук, доцент, завідувач кафедри комп'ютерної інженерії факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка.

Оцінка позитивна, без зауважень.

Сергій ДАКОВ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Оцінка позитивна із зауваженнями:

1. Окремі відомості про протокол Clique та його обмеження подано і в першому розділі (при порівняльному аналізі платформ), і на початку третього. Можливо, було б доречно описати ці елементи один раз із подальшими посиланнями, що ущільнило б виклад.
2. Система вимірювань у роботі побудована ретельно, а всі керуючі параметри методу зведені в єдину таблицю, що відкриває можливість його налаштування під конкретне середовище. Однак саме при доборі коефіцієнтів базової оцінки та штрафних функцій у подальших роботах стануть у пригоді відомості про кількість повторних прогонів і розсіювання значень між ними, що дозволять відрізнити вплив зміни коефіцієнта від коливань мережевих метрик.
3. Запропоноване в підрозділі 4.5 відкладене призначення задач як розв'язання виявленої проблеми оновлення оцінки вузла не частіше одного разу за блок необхідно формалізувати (умови відкладення, гранична затримка призначення, поведінка за пакетного надходження задач) та експериментально перевірити.
4. Рекомендації щодо вибору блокчейн-платформ мають самостійну методичну цінність і придатні для використання поза межами дисертації. Саме тому варто було б звести їх у підсумкову таблицю «сценарій застосування – вимоги – рекомендована конфігурація», що зробило б цей результат ще зручнішим для проєктувальників.
5. У роботі відсутні додатки; доцільно було б навести у них принаймні ключові фрагменти коду розроблених модулів (модифікацій Go-Ethereum, смарт-контрактів) або посилання на репозиторій із програмною реалізацією для підтвердження відтворюваності результатів.

Наведені зауваження мають рекомендаційний характер, не зачіпають сутності отриманих результатів і не знижують загальної позитивної оцінки роботи.

Сергій ПАЛІЙ, кандидат технічних наук, доцент, доцент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Оцінка позитивна із зауваженнями:

1. Техніка компактних блоків дає найбільший ефект за умови, коли тіла транзакцій істотно перевищують розмір їхніх хешів; у проведених експериментах сумарне зменшення мережевого трафіку становить 20,5 %. Було б доцільно детальніше показати, як цей ефект змінюється залежно від сценарію навантаження та розміру транзакцій, зокрема для дрібних телеметричних повідомлень у кілька десятків байтів, характерних для сенсорних мереж. Визначення таких залежностей полегшило б оцінювання доцільності застосування запропонованого механізму в конкретних IoT-сценаріях.

2. Мультиплікативна композиція скорингової функції має корисну властивість «вето-ефекту», однак водночас робить результат вибору чутливим до значень порогових констант. Практичні рекомендації щодо налаштування параметрів для різних класів задач периферійних обчислень – обчислювально інтенсивних, чутливих до затримки та довготривалих фонових – могли б спростити перенесення запропонованої моделі до реальних умов експлуатації.
3. Експериментальна перевірка виконувалася у контейнерному середовищі, що має суттєву перевагу з точки зору відтворюваності, однак контейнери використовують ядро та процесорну архітектуру хоста. Додаткові випробування хоча б на невеликому стенді з фізичних одноплатних комп'ютерів дозволили б оцінити поведінку запропонованої моделі за реальних апаратних умов, зокрема з урахуванням зниження тактової частоти під тривалим навантаженням, повільнішого доступу до пам'яті та накладних витрат на збирання показників стану вузла.
4. Масштаб експериментальної перевірки основних характеристик запропонованого консенсусу є обмеженим кількістю вузлів у тестовому середовищі. Було б корисно додатково дослідити поведінку PoI при істотному збільшенні кількості вузлів та за різних топологій мережі. Це дало б змогу повніше оцінити масштабованість запропонованого підходу та межі його ефективного застосування.
5. Окреслені в перспективах напрями – застосування доказів без розкриття інформації та федеративного навчання – подано загально. Їх конкретизація хоча б на рівні постановок задач (які саме твердження доводяться без розкриття даних, які моделі та на яких даних навчаються) зробила б розділ перспектив логічним продовженням роботи, а не переліком можливостей.

Зазначені зауваження не мають принципового характеру та не ставлять під сумнів наукову новизну, достовірність отриманих результатів або загальну позитивну оцінку дисертації.

Ярослав ДОРОГИЙ, доктор технічних наук, професор, завідувач кафедри штучного інтелекту та кібербезпеки ДВНЗ «Донецький національний технічний університет».

Оцінка позитивна із зауваженнями:

1. У запропонованій системі мультифакторного управління значення доступності ресурсів формуються на стороні периферійного вузла через бібліотеку psutil і передаються в смарт-контракт без криптографічної верифікації. Запровадження надійних механізмів підтвердження реального обчислювального стану унеможливило б ситуації, коли зловмисний вузол штучно завищує свої вільні ресурси для перехоплення задач.
2. Для перевірки результатів обчислень, виконаних периферійними вузлами поза блокчейном, застосовується лише хеш-функція Keccak-256, що здатна виявити модифікацію даних, проте не замінює повноцінну верифікацію правильності самих обчислень. Інтеграція алгоритмів на зразок доказів з нульовим розголошенням (ZKP) зробила б систему більш стійкою, що цілком обґрунтовано винесено автором у перспективи досліджень.
3. Формалізація динамічного ранжування валідаторів успішно виявляє специфічні класи загроз, однак повноцінна модель безпеки з формальним математичним доведенням

стійкості консенсусу Proof of Indicators до шахрайства у роботі відсутня. Її наявність зробила б теоретичне обґрунтування надійності консенсусу більш переконливим.

4. Поза розглядом залишилася поведінка PoI при одночасній відмові або компрометації значної частки валідаторів, а також стійкість зовнішнього рівня архітектури до Sybil-атак, що для відкритих p2p-мереж, де вартість створення псевдонімних вузлів низька, є одним із визначальних векторів загроз. Якісний аналіз цих сценаріїв посилив би безпекову аргументацію роботи.
5. Використання мультиплікативної композиції факторів створює жорсткий «вето-ефект», який вимагає ручного калібрування констант залежно від потреб конкретного середовища. Розроблення адаптивних ваг факторів, які б автоматично підлаштовувалися під профілі різних задач, суттєво розширило б можливості автоматичного розгортання системи.
6. Мультифакторний вибір обчислювальних вузлів спирається на реактивний моніторинг ресурсів із фіксованою періодичністю, що створює ризик прийняття рішень на основі застарілих даних. Впровадження предиктивних моделей для прогнозування майбутнього навантаження вузла на наступний період блоку дозволило б значно скоротити кількість конфліктних призначень при пакетній подачі задач.

Зазначені зауваження не впливають на загальне позитивне враження від дисертаційної роботи.

Олексій НАЛАПКО, доктор філософії, докторант (штатний) науково-організаційного відділу Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

Оцінка позитивна із зауваженнями:

1. Придатність архітектури для військового застосування у другому розділі показано через перелік властивостей. Однак у цій сфері діють кількісні вимоги: скільки часу кластер має зберігати автономність, яку частку вузлів можна втратити без порушення координації, за який час мережа відновлює координацію після роз'єднання сегментів. Без таких критеріїв і перевірки за ними розділ лишається радше ескізом застосування, ніж його обґрунтуванням. Формулювання відповідних критеріїв становить необхідний наступний крок цього прикладного напряму.
2. Експерименти проведено за таких мережевих умов: випадкова затримка до 200 мс, варіація затримки пакетів до 20 мс, без втрат пакетів. Бездротові канали можуть характеризуватися значно гіршими показниками – втратами пакетів, розривами з'єднань, різкими коливаннями затримок, тому варто провести додаткове тестування в складніших умовах.
3. Серед виміряних ресурсів відсутнє енергоспоживання. Для вузлів на автономному живленні воно нерідко є визначальним обмеженням, тож вимірювання споживаної потужності на фізичних пристроях становило б логічне продовження експериментальної програми.

4. Спільна робота PoI та мультифакторного управління у підрозділі 4.6 описана концептуально, і автор коректно відносить наскрізний експеримент до подальших досліджень. Погоджуючись із такою послідовністю, слід зауважити, що методику цього майбутнього експерименту доцільно було окреслити вже на цьому етапі: сценарії навантаження, метрики та очікувані ефекти від взаємодії двох контурів управління.
5. Накладні витрати блокчейн-координації у четвертому розділі – обчислювальну вартість виконання смарт-контрактів і затримки підтвердження транзакцій за трисекундного інтервалу генерації блоків охарактеризовано побіжно. Їх кількісна оцінка була б доречною, адже саме вони визначають граничну інтенсивність потоку задач, яку платформа мультифакторного управління здатна обслужити без накопичення черги підтверджень.

Зауваження 2–5 окреслюють напрями розвитку дослідження, зауваження 1 стосується глибини опрацювання одного з прикладних сценаріїв; жодне з них не ставить під сумнів отримані результати.

Результати відкритого голосування:

«За» 5 членів ради,

«Проти» 0 членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує Чепелю Леоніду Валерійовичу ступінь доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 123 «Комп'ютерна інженерія».

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої вченої ради
доктор технічних наук, професор **Володимир ЗАСЛАВСЬКИЙ**

ПІДПИС ЗАСВІДЧУЮ
Вчений секретар НЛУ
КАРАУЛЬНА
10.0