Рішення
разової спеціалізованої вченої ради PhD 14207
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії **Родіон ХВОРОСТЯНИЙ**,
(власне ім'я, прізвище здобувача (ки))

1997 року народження, громадянин України,
(назва держави, громадянином якої є здобувач (ка))

освіта вища: закінчив (ла) у 2020 році Державний університет телекомунікацій,
(найменування закладу вищої освіти)

за спеціальністю «Кібербезпека»,
(за дипломом)

Здійснював підготовку в аспірантурі Державного університету інформаційно-комунікаційних технологій (2022-2026 рр.), виконав акредитовану освітньо-наукову програму «Кібербезпека» зі спеціальності 125 «Кібербезпека», галузі знань 12 «Інформаційні технології».

Разова спеціалізована вчена рада, утворена наказом Державного університету інформаційно-комунікаційних технологій, Міністерства освіти і науки України, м. Київ
(повне найменування закладу вищої освіти (наукової установи), підпорядкування (у родовому відмінку), місто)
від «22» травня 2026 року № 227, у складі:

Голови разової спеціалізованої вченої ради — **Віталія САВЧЕНКА**, доктора технічних наук, професора, професора кафедри управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

Рецензентів – **Юрія ПЕПИ**, кандидата технічних наук, доцента, професора кафедри технічних систем кіберзахисту Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій;
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

Сергія ЗИБІНА, доктора технічних наук, професора, професора кафедри систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

Офіційних опонентів – **Юрія ХЛАПОНІНА**, доктора технічних наук, професора, професора кафедри інженерії програмного забезпечення та кібербезпеки Факультету інформаційних технологій Державного торговельно-економічного університету;
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

Миколи БРАЇЛОВСЬКОГО, кандидата технічних наук, доцента, доцента кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

На засіданні «29» червня 2026 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології
(галузь знань)
Родіону ХВОРОСТЯНОМУ
(власне ім'я, прізвище здобувача (ки) у давальному відмінку)
на підставі публічного захисту дисертації **«Моделі та методи управління кібербезпекою транспортної телекомунікаційної мережі на основі мультиагентних технологій»**
(назва дисертації)
за спеціальністю (спеціальностями) 125 «Кібербезпека».
(код і найменування спеціальності відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)
Дисертацію виконано у Державному університеті інформаційно-комунікаційних технологій, Міністерства освіти і науки України, м. Київ
(найменування закладу вищої освіти (наукової установи), підпорядкування, місто)

Науковий керівник:

ТУРОВСЬКИЙ Олександр Леонідович – доктор технічних наук, професор, завідувач кафедри технічних систем кіберзахисту Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.
(власне ім'я, прізвище, науковий ступінь, вчене звання, місце роботи, посада)

На сьогоднішній день транспортні телекомунікаційні мережі відіграють ключову роль у забезпеченні функціонування сучасної економіки. Водночас їх висока складність та відкритість до інтеграції з іншими мережами обумовлюють підвищену вразливість до кібератак, результатом яких можуть бути суттєві наслідки для держави. Існуючі підходи до побудови систем управління кібербезпекою транспортних телекомунікаційних мереж базуються переважно на централізованих механізмах контролю або статичних моделях захисту, не враховуючи динаміку змін топології та розподілений характер прийняття рішень. Логічним наслідком у такій ситуації є перехід до використання мультиагентних систем управління, які забезпечують децентралізоване прийняття рішень та адаптивну взаємодію між елементами мережі. Водночас ефективність такого підходу значною мірою залежить від наявності формалізованих моделей і методів, що забезпечують узгоджену взаємодію агентів при вирішенні ключових задач управління кібербезпекою мережі.

Метою дослідження є підвищення захищеності транспортної телекомунікаційної мережі в умовах впливу кібератак. Дисертацію виконано державною мовою, структура та правила оформлення дисертації відповідають вимогам затвердженим наказом МОН України від 12.01.2017 №40. Дисертацію подано у вигляді спеціально підготовленого рукопису, який є завершеним науковим дослідженням, в якому вирішено актуальне наукове завдання щодо розроблення та удосконалення моделей і методів мультиагентного управління кібербезпекою транспортної телекомунікаційної мережі в умовах впливу кібератак, яке має суттєве значення для теорії та практики дослідження технологій, методів, моделей та засобів кібербезпеки та захисту інформації транспортних телекомунікаційних мереж.

Наукові результати, отримані в дисертаційній роботі:

Наукова новизна отриманих результатів полягає в наступному:

1. Вперше розроблено модель ієрархічної мультиагентної системи управління кібербезпекою транспортної телекомунікаційної мережі, яка базується на декомпозиції основних функцій управління захистом мережі (моніторинг, діагностування, оцінювання стану, прийняття рішень, реалізація керуючих впливів, координація, адаптація, формування та контроль виконання політик) та ієрархічному розподілі цих функцій за рівнями мережевої

архітектури (периферійний, агрегаційний, транспортний, магістральний, управлінський та сервісний), що дозволяє реалізувати принцип локальності прийняття рішень агентами для оперативного реагування на загрози на нижніх рівнях та забезпечити глобальну узгодженість і адаптивність системи на вищих рівнях ієрархії.

2. Удосконалено метод мультиагентного діагностування елементів транспортної телекомунікаційної мережі щодо виявлення ознак кібератак, який, за рахунок поєднання в моделі ієрархічної мультиагентної системи управління кібербезпекою алгоритмів діагностування Препарати-Метце-Чєна, моделі Візантійської угоди з розподілом функцій між агентами моніторингу, виявлення загроз і координації, та застосування процедури децентралізованого ієрархічного узгодження діагностичних рішень, забезпечує можливість виявлення та локалізації компрометованих вузлів за умов наявності недостовірних або суперечливих діагностичних повідомлень в мережах складної топології.

3. Удосконалено модель мультиагентного балансування навантаження транспортної телекомунікаційної мережі в умовах впливу кібератак, в якій, на відміну від існуючих моделей, що орієнтуються на статичні або централізовано визначені метрики каналів, враховуються динамічні зміни ступеня уразливості вузлів, визначені методом мультиагентного діагностування елементів, та реалізується адаптивний розподіл трафіку шляхом вирішення задачі оптимізації з обмеженнями на пропускну здатність каналів і допустимий рівень довіри до вузлів, що дозволяє перенаправляти потоки даних на більш захищені маршрути при виявленні атак на окремі елементи мережі, забезпечуючи збереження цільових показників якості обслуговування в умовах деструктивного впливу.

4. Вперше розроблено метод мультиагентної взаємодії, який базується на інтеграції в моделі ієрархічної мультиагентної системи управління кібербезпекою результатів застосування методів мультиагентного діагностування та балансування навантаження та реалізує алгоритм визначення критичних вузлів і мінімально необхідної кількості резервних зв'язків, що забезпечує децентралізоване формування раціональної конфігурації додаткових зв'язків для збереження зв'язності мережі з мінімальними витратами ресурсів з метою забезпечення захищеності транспортної телекомунікаційної мережі в умовах впливу кібератак..

Практичне значення отриманих результатів.

Практичне значення одержаних результатів полягає в тому, що розроблені у дисертаційній роботі моделі, методи та практичні рекомендації дозволяють реалізувати різні варіанти побудови мультиагентних систем управління кібребезпекою транспортної телекомунікаційної мережі, які, у порівнянні з відомими технологічними рішеннями, забезпечують: порівняну з TI-LFA ефективність відновлення (MTTR 8.4 с проти 0.05–0.2 с) з урахуванням того, що запропонована система надає захист від кібератак різних типів; перевагу над Cisco TrustSec у швидкості реагування (11.5 с проти 60–120 с) за рахунок розподіленої архітектури агентів; вищу повноту виявлення загроз (93.3%) порівняно зі стандартними SNMP-системами (40–60%) та рівнем, близьким до TrustSec (85–90%); прийнятний рівень хибних спрацьовувань (3.3%), що є в межах промислових стандартів для систем виявлення загроз (1–5%). Ключовою перевагою запропонованої системи є її здатність одночасно виявляти та реагувати на різні типи кібератак, тоді як TI-LFA забезпечує захист лише від фізичних відмов, а TrustSec зосереджений на автентифікації та сегментації.

Результати досліджень прийняті до впровадження в діяльність ПНВП "Сардер Телеком", а також реалізовані в освітньому процесі кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій.

Здобувач має _8_ наукових публікацій за темою дисертації, з них: _3_ наукових статті, які опубліковані у спеціалізованих фахових виданнях, затверджених наказом МОН України. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у _4_ збірниках тез доповідей.

(наводиться аналіз наукових публікацій щодо дотримання вимог пунктів 8, 9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії) (зазначити наукові публікації)

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Хворостяний, Р., & Корецький, О. (2025). Методика побудови платформи штучного інтелекту моніторингу конфіденційного та аномального трафіку при умові мінімізації часу розгортання та надійності функціонування. Herald of Khmelnytskyi National University. Technical Sciences, 351(3.1), 119–125. https://doi.org/10.31891/2307-5732-2025-351-14
2. Хворостяний, Р. В., & Туровський, О. Л. (2026). Метод взаємодії агентів в мультиагентній системі управління кібербезпекою транспортної телекомунікаційної мережі під час діагностування кібератак. Телекомунікаційні та інформаційні технології, 1(90), 38–49. https://doi.org/10.31673/2412-4338.2026.019005
3. Хворостяний, Р. В. (2026). Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131. https://doi.org/10.31673/2409-7292.2026.011588.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Хворостяний, Р. В., Сад, Р. М., & Верещак, П. В. (2024). Аналіз процесу обробки персональних даних в локальних комп'ютерних мережах та способів несанкціонованого доступу до них. У Всеукраїнська науково-практична конференція "Актуальні проблеми безпеки інформаційно-телекомунікаційних систем" (с. 70–72). Київ, ДУІКТ-КНУБА. https://duikt.edu.ua/uploads/p_2661_93669247.pdf
2. Аверічев, І. М., & Хворостяний, Р. В. (2024). Модель системи управління кібербезпекою транспортної телекомунікаційної мережі: концепція, архітектура та механізми захисту. У Всеукраїнська науково-практична конференція "Актуальні проблеми безпеки інформаційно-телекомунікаційних систем" (с. 110–111). Київ, ДУІКТ-КНУБА. https://duikt.edu.ua/uploads/p_2661_93669247.pdf
3. Koretskyi, O., Khvorostianyi, R., & Bondarenko, Y. (2025). Hardware and software complex for the functioning of a neural network for identification and traffic management in 5G/IMT-2020 networks. In The IV International Conference "Emerging Technology Trends on the Smart Industry and the Internet of Things "TTSIIT" (с. 44–49). Київ, КНУБА. https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view
4. Хворостяний, Р. (2025). Транспортна інформаційно-комунікаційна мережа як об'єкт кіберзагроз. У XIV міжнародна науково-технічна конференція "Безпека інформаційних технологій" (с. 231–234). Тернопіль, ЗУНУ. https://drive.google.com/file/d/1Nt2w9E-N97TAIdAGqWKbaXsqASyP-4tt/view
5. Корецький, О. В., & Хворостяний, Р. В. (2025). Методичний підхід до побудови платформи штучного інтелекту моніторингу конфіденційного та аномального трафіку. У І Міжнародна науково-практична конференція "Прикладні системи управління та робототехніка" (с. 218–221). Київ, ІПСУ НАН України. https://iacs.institute/content/conferencespdf/1/kolektivna-monografiya-za-materialami-konferencii--ipsu-2025.pdf?1770983479.5214.

Наукові праці, які додатково відображають наукові результати дисертації:

1. Хворостяний, Р. В. (2023). Проблеми безпеки та заходи протидії атакам в NFC. Сучасний захист інформації, 1(53), 39–46. https://doi.org/10.31673/2409-7292.2023.010005
2. Захаржевський, А. Г., Таванюк, Д. М., & Хворостяний, Р. В. (2023). Технологія сніфінгу у локальній мережі підприємства з використанням Wireshark. Сучасний захист інформації, 3(55), 22–31. https://doi.org/10.31673/2409-7292.2023.030003.

У дискусії взяли участь голова і члени спеціалізованої вченої ради та присутні на захисті фахівці:

Рецензент – **ПЕПА Юрій Володимирович**, кандидат технічних наук, доцент, професор кафедри технічних систем кіберзахисту Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій надав позитивну рецензію із зауваженнями:

1. До наведеного у роботі обгрунтування доцільності застосування ієрархічної мультиагентної моделі управління кібербезпекою транспортної телекомунікаційної мережі варто було б додати приклади реальних транспортних мереж, у яких управління кібербезпекою здійснювалося б за запропонованим автором ієрархічним мультиагентним підходом. Також, доцільно було б навести статистичні показники якості такого управління.

2. У розділі 3 роботи автор наводить алгоритми: мультиагентного діагностування на рівні агентів моніторингу, регіонального діагностування та регіонального консенсусу на рівні агентів виявлення загроз, глобального аналізу та ієрархічного консенсусу на рівні агентів координації. Разом з тим, для глибшого розуміння внеску автора у цих алгоритмах варто було б виділити реалізацію моделі Препарати-Метце-Чєна та Візантійської угоди в окремі блоки.

3. При оцінці достовірності методу мультиагентного діагностування елементів транспортної мережі автор досліджує приклад з 6–20 вузлів мережі. Разом з тим, у роботі не зазначається, яка максимальна кількість елементів може бути продіагностована за допомогою розробленого методу у прийнятний час із заданою ефективністю.

Рецензент – **ЗИБІН Сергій Вікторович**, доктор технічних наук, професор, професор кафедри систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій надав позитивну рецензію із зауваженнями:

1. У роботі було б доцільно більш глибоко розкрити вплив на елементи транспортних телекомунікаційних мереж різних типів атак та визначити ключові параметри мережевого обладнання (маршрутизаторів, комутаторів, серверів управління), які зазнають такого впливу. Також, необхідно було б навести найбільш уразливі до кібератак протоколи транспортних телекомунікаційних мереж.

2. При формулюванні загальної формалізованої постановки наукового завдання автору варто було б зазначити, яким чином здійснюється вибір вагових коефіцієнтів для складових формули (1.1), зокрема: рівня деградації зв'язності мережі, рівня перевантаження (дисбалансу трафіку), ризику компрометації вузлів.

3. При обгрунтуванні доцільності застосування ієрархічної мультиагентної моделі управління кібербезпекою транспортної телекомунікаційної мережі автором не зазначено яким чином було обрано групу експертів, які визначали узгоджені кількісні оцінки моделей управління кібербезпекою транспортних мереж..

Опонент – **ХЛАПОНІН Юрій Іванович**, доктор технічних наук, професор, професор кафедри інженерії програмного забезпечення та кібербезпеки Факультету інформаційних технологій Державного торговельно-економічного університету надав позитивний відгук із зауваженнями:

1. У розділі 1 наведено графік (рис. 1.2. Глобальний ринок кібератак у телекомунікаційному секторі) з посиланням на джерело: Market Growth Report. (2026). Cyber attack in telecom sector market size, share, growth, and industry analysis, by type (denial-of-service attacks, phishing, malware, hacking, ransomware, botnets), by application (telecommunications, IT security, public & private sector, government), regional insights and forecast to 2035. https://www.marketgrowthreports.com/market-reports/cyber-attack-in-telecom-sector-market-113188 Разом з тим, залишається незрозумілим, що саме мається на увазі під " Глобальним ринком кібератак" – загальні вкладення розробників шкідливого програмного забезпечення на організацію атак, чи загальні витрати компаній світу на протидію кібератакам.

2. В Алгоритмі мультиагентного балансування навантаження варто було б навести пояснення, яким чином обирається Параметр управління навантаженням у мережі, від якого залежить характер перерозподілу трафіку між вузлами.

3. Під час моделювання роботи мультиагентної системи захисту мережі у програмному комплексі Cisco Packet Tracer автор обрав три типи маршрутизаторів (Cisco ISR 4331, Cisco ISR 4321, Cisco ISR 2911). Разом з тим, у роботі не пояснюються причини такого вибору мережевих пристроїв для дослідної мережі.

4. У розділі 4, під час оцінки ефективності мультиагентної системи управління кібербезпекою, автору варто було б пояснити доцільність застосування "метрик управління довірою" для оцінювання якості системи.

Опонент – **БРАЙЛОВСЬКИЙ Микола Миколайович**, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, надав позитивний відгук із зауваженнями:

1. У розділі 3 автором розроблено Алгоритм визначення критичних вузлів та мінімальної кількості резервних зв'язків. Разом з тим, у роботі не зазначається, коли більш доцільно застосовувати такий алгоритм: на етапі нормальної роботи мережі для визначення потенційних резервних зв'язків, чи після початку кібератаки для перебудови маршрутів передачі даних.

2. Потребує додаткового пояснення термін "субсекундне відновлення після відмови каналів".

Голова ради – **САВЧЕНКО Віталій Анатолійович**, доктор технічних наук, професор, професор кафедри управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій надав позитивний відгук без зауважень.

Результати відкритого голосування:

«За» 5 (п'ять) членів ради,

«Проти» немає.

«Утримались» немає.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує

Родіону ХВОРОСТЯНОМУ

(власне ім'я, прізвище, здобувача (ки) у давальному відмінку)

ступінь доктора філософії з галузі знань 12 «Інформаційні технології»

(галузь знань)

за спеціальністю 125 «Кібербезпека»

(код і найменування спеціальності (спеціальностей) відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Відеозапис трансляції захисту дисертації додається.

Окрема думка члена разової ради додається (за наявності).

Голова разової спеціалізованої вченої ради _____ (підпис) Віталій САВЧЕНКО (власне ім'я та прізвище)