

Голові разової спеціалізованої вченої  
ради Державного університету  
інформаційно-комунікаційних  
технологій

доктору технічних наук, професору

Віталію САВЧЕНКУ

вул. Солом'янська, 7, м. Київ, 03110

## ВІДГУК

офіційного опонента – кандидата технічних наук, доцента, доцента кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка **Браїловського Миколи Миколайовича** на дисертаційну роботу **Хворостяного Родіона Віталійовича** на тему “Моделі та методи управління кібербезпекою транспортної телекомунікаційної мережі на основі мультиагентних технологій”, подану на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека.

### Актуальність теми

Сучасна транспортна телекомунікаційна мережа – це багаторівнева телекомунікаційна інфраструктура, яка об'єднує оптичні (DWDM, OTN) та пакетні (IP/MPLS, Ethernet) технології для забезпечення високошвидкісного (>100 Гбіт/с) транзиту агрегованого трафіку між географічно розподіленими сегментами мережі (містами, країнами, континентами). Типовими кібератаками на такі мережі є DDoS-атаки на магістральні канали, атаки на протоколи маршрутизації (BGP, OSPF) та компрометація вузлів транспортного рівня. Уразливості транспортних мереж обумовлюються статичністю маршрутних політик, затримками в механізмах відновлення та обмеженою спостережністю стану вузлів. Це обумовлює перехід від статичних механізмів захисту до адаптивних систем управління кібербезпекою.

На основі проведеного аналізу сучасного стану та проблематики управління кібербезпекою транспортних телекомунікаційних мереж автором було виявлено загальне протиріччя, яке полягає у невідповідності між необхідністю побудови комплексної, адаптивної, ієрархічно організованої мультиагентної системи управління кібербезпекою транспортної телекомунікаційної мережі та відсутністю узагальнених моделей і методів, що забезпечують узгоджене вирішення задач діагностування, управління навантаженням і забезпечення структурної стійкості мережі в умовах кібератак. Зазначені обставини підтверджують актуальність поставленого наукового завдання.

### Ступінь обґрунтованості наукових результатів, висновків та рекомендацій, сформульованих в дисертації

Обґрунтованість та достовірність наукових результатів, висновків та рекомендацій, одержаних в дисертації, підтверджується коректною постановкою

завдань дослідження, аналізом широкого спектру науково-технічної літератури за темою дисертації, повнотою розгляду на теоретичному та експериментальному рівнях об'єкта дослідження, обґрунтованим дослідженням та використанням перевірених методів для вирішення визначених завдань, зокрема: теорії графів (для формалізації структури та аналізу зв'язності транспортної мережі); теорії надійності та живучості мереж (для оцінки впливу відмов вузлів і каналів на функціонування мережі); розподіленого діагностування на основі моделі Препарати-Метце-Чена та Візантійської угоди, (для визначення стану вузлів в умовах суперечливої інформації); оптимізації потоків (для адаптивного розподілу трафіку з урахуванням обмежень); розподіленого керування (для децентралізованого прийняття рішень та узгодження дій агентів); математичного та імітаційного моделювання (для перевірки працездатності запропонованих моделей і методів).

### **Оцінка новизни наукових результатів дисертації**

Наукова новизна одержаних результатів полягає в тому, що у дисертаційній роботі:

вперше розроблено модель ієрархічної мультиагентної системи управління кібербезпекою транспортної телекомунікаційної мережі, яка базується на декомпозиції основних функцій управління захистом мережі та ієрархічному розподілі цих функцій за рівнями мережевої архітектури, 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;

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-Чена, моделі Візантійської угоди з розподілом функцій між агентами, забезпечує можливість виявлення та локалізації компрометованих вузлів за умов наявності недостовірних або суперечливих діагностичних повідомлень в мережах складної топології;

удосконалено модель мультиагентного балансування навантаження транспортної телекомунікаційної мережі в умовах впливу кібератак, в якій, на відміну від існуючих моделей, враховуються динамічні зміни ступеня уразливості вузлів, визначені методом мультиагентного діагностування елементів, та реалізується адаптивний розподіл трафіку шляхом вирішення задачі оптимізації, 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;

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.

### **Практична цінність наукових результатів**

Розроблені у дисертаційній роботі моделі та методи управління кібербезпекою дають можливість сформулювати рекомендації для широкого кола фахівців з питань захисту мереж. У порівнянні з відомими технологічними рішеннями, розроблені моделі і методи 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.

### **Зв'язок роботи з науковими програмами, планами, темами**

Дисертаційна робота Хворостяного Р.В. виконана відповідно до Законів України “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України”, “Про електронні комунікації”; Постанови Кабінету Міністрів України “Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах”, та в рамках науково-дослідних робіт Державного університету інформаційно-комунікаційних технологій.

### **Повнота викладу основних результатів дисертації в публікаціях**

Наукові результати дисертаційної роботи Хворостяного Р.В. опубліковані у 8 наукових працях, серед яких 3 статті у спеціалізованих фахових виданнях, затверджених наказом МОН України, 2 статті в інших виданнях. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 4 збірниках тез доповідей: Всеукраїнська науково-практична конференція “Актуальні проблеми безпеки інформаційно-телекомунікаційних систем” (3–5.11.2024); IV Міжнародна науково-практична конференція “Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей” “TTSIIT” (30–31.01.2025); XIV міжнародна науково-технічна конференція “Безпека інформаційних технологій” (22–24.05.2025); I Міжнародна науково-практична конференція “Прикладні системи управління та робототехніка” (12–13.11.2025).

**Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення**

Дисертаційна робота Хворостяного Р.В. відповідає діючим вимогам щодо дисертацій на здобуття наукового ступеня доктора філософії, передбаченим “Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії”, затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

### **Недоліки та зауваження до дисертаційної роботи**

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”.

Вказані недоліки не знижують наукової цінності та практичної значимості одержаних результатів і не впливають на загальну позитивну оцінку роботи.

### **Відповідність дисертації встановленим вимогам та її загальна оцінка**

Дисертація Хворостяного Р.В. відповідає вимогам “Порядку підготовки здобувачів вищих ступенів доктора філософії та доктора наук у закладах вищої освіти (наукових установах)”, затвердженого Постановою Кабінету Міністрів України від 23 березня 2016 р. № 261, “Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії”, затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а її автор – Хворостяний Родіон Віталійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

### **Офіційний опонент:**

доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка,  
кандидат технічних наук, доцент



Микола БРАІЛОВСЬКИЙ

