

Голові разової спеціалізованої вченої
ради Державного університету
інформаційно-комунікаційних
технологій
доктору технічних наук, професору
Замрій Ірині Вікторівні
03110, м. Київ, вул. Солом'янська, 7

ВІДГУК

Офіційного опонента – доктора технічних наук, професора, декана факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» **Корнаги Ярослава Ігоровича** на дисертаційну роботу Вишнівського Олександра Вікторовича на тему «Метод побудови захищеної комп'ютерної системи на основі графу атак та штучного інтелекту» подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки

Актуальність теми дисертації

Сучасний розвиток інформаційних технологій супроводжується стрімким переходом до розподілених цифрових середовищ, активним впровадженням хмарних платформ, віртуалізації, мобільних рішень і програмно-керованих мереж. Однією з найбільш поширених технологій у цьому напрямі є SD-WAN, що забезпечує централізоване адміністрування мережевої інфраструктури, ефективне використання каналів зв'язку та зменшення витрат на їх експлуатацію. SD-WAN активно застосовується у корпоративних мережах, державних інформаційних системах, хмарних сервісах, банківському секторі, промисловості та об'єктах критичної інфраструктури, ставши важливим елементом цифрової трансформації.

Водночас поширення SD-WAN створює нові ризики у сфері кібербезпеки. Компрометація центрального контролера, помилки конфігурації, недостатня сегментація мережі або перехоплення службового трафіку можуть спричинити серйозні порушення роботи інформаційної інфраструктури. Традиційні засоби забезпечення інформаційної безпеки мають низку обмежень, що особливо проявляються у середовищах SD-WAN. Насамперед вони недостатньо ефективно реагують на динамічні зміни конфігурації мережі та не враховують особливості програмно-керованої архітектури. У зв'язку з цим питання забезпечення безпеки SD-WAN-мереж набуває особливої актуальності в сучасних умовах.

Одним із перспективних підходів до вирішення зазначених проблем є застосування моделей комп'ютерних систем у просторі станів. Такий метод

дозволяє описати функціонування мережевої інфраструктури через множину станів та переходів між ними, що створює можливість дослідження динаміки змін параметрів безпеки, оцінювання ризиків і прогнозування розвитку кіберзагроз. Для SD-WAN-мереж цей підхід є особливо важливим, оскільки маршрути, політики доступу та мережеві сервіси можуть змінюватися у реальному часі залежно від поточного стану системи.

Дисертаційна робота Вишнівського О.В. присвячена розв'язанню актуального наукового завдання сутність якого полягає в розробці моделей і методів побудови захищеної інтелектуальної комп'ютерної системи з управлінням SD-WAN на основі графу атак.

Оцінка обґрунтованості та достовірності наукових положень

Обґрунтованість наукових положень, висновків і практичних рекомендацій забезпечується ґрунтовним аналізом та узагальненням значної кількості наукових праць вітчизняних і зарубіжних дослідників. Використання широкої бази наукових і прикладних публікацій у поєднанні з коректно обраними методами дослідження сприяє підвищенню достовірності отриманих результатів, а також підтверджує наукову цінність сформульованих висновків і практичних рекомендацій.

Для вирішення поставлених у дослідженні завдань автором застосовано комплекс загальнонаукових та емпіричних методів. Теоретичною основою роботи є сучасні підходи системного аналізу, теорія графів, методи імовірнісного аналізу, теорія управління, алгоритми машинного навчання, а також принципи архітектурного проектування програмно-керованих мереж.

Достовірність, наукова новизна та практична значущість сформульованих у дисертації положень, висновків і рекомендацій підтверджуються результатами проведеного імітаційного моделювання та отриманими експериментальними даними.

Оцінка новизни наукових результатів дисертаційного дослідження

У дисертаційній роботі одержані наступні нові наукові результати.

1. Вперше розроблено модель комп'ютерної системи SD-WAN на основі апарату простору станів та теорії автоматичного управління, в якій відповідно за рахунок формалізації її представлення у вигляді сукупності вектору стану і вектору управління, функції якості обслуговування та врахування зміни часових характеристик передачі даних, пропускної здатності каналів зв'язку, ступеня заповнення буферних черг мережевих вузлів та ймовірності втрат пакетів, дозволило забезпечити стійкість і керованість системи.

2. Вперше розроблено метод інтелектуального управління комп'ютерною системою SD-WAN, в якому відповідно на основі побудованої моделі комп'ютерної системи SD-WAN, розроблених алгоритмів для управління на основі методу глибокого навчання з підкріпленням для дискретного та неперервного просторів стану, дозволило забезпечити зниження затримки, рівня втрати пакетів і підвищити значення функціоналу якості.

3. Удосконалено метод побудови захищеної комп'ютерної системи SD-WAN, в якому відповідно на основі комплексної інтеграції побудованої моделі комп'ютерної системи SD-WAN, математичної моделі спрямованого графу атак, комплексного показника ризику, розробленого алгоритму Q-навчання для агента SD-WAN з підкріпленням та механізму розривів ланцюжків кібератак на ранніх стадіях їх розвитку, дозволило превентивно перебудовувати мережеві маршрути та мінімізувати час реакції на інциденти.

Практична цінність отриманих результатів

Практична значення дослідження полягає у можливості створення інтелектуальних систем кіберзахисту нового покоління, здатних забезпечувати проактивне виявлення загроз, мінімізації ризиків компрометації мережевої інфраструктури, зниженні кількості хибнопозитивних спрацювань та скороченні часу реагування на кіберінциденти, а саме:

- здійснено комплексний аналіз вітчизняних та міжнародних підходів до моделювання комп'ютерних систем з управлінням SD-WAN, управлінням кіберзахистом таких систем з використанням графу атак на основі машинного навчання. Обґрунтовано, що існує необхідність розробки комплексної математичної моделі комп'ютерної системи з управлінням SD-WAN у просторі станів на основі теорії управління. Управління кібербезпекою необхідно проводити на основі графу атак, який дозволить описувати можливі сценарії дій порушника, взаємозв'язки між вразливостями, мережевими вузлами та рівнями привілеїв застосовуючи методи штучного інтелекту та машинного навчання;

- на основі методу інтелектуального управління комп'ютерною системою SD-WAN розроблена архітектура нейронної мережі для реалізації алгоритмів інтелектуального управління. Запропонована модель комп'ютерної системи SD-WAN та метод управління комп'ютерною системою SD-WAN були впроваджені в інформаційну мережу ТОВ «АЙТІ КУРСОР» (акт впровадження від 27.11.2025 р.). Це забезпечило підвищення продуктивності інформаційної мережі: середнє завантаження каналів знизилося на 44%, середня затримка – на 65%, рівень втрати пакетів – на 85%, а значення функціоналу якості покращилося на 61%;

- на основі удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN, графу атак та розробленого алгоритму Q-навчання було спроектовано та розгорнуто комплексний імітаційний тестовий стенд. Для верифікації прогнозованих можливостей захищеної комп'ютерної системи SD-WAN розроблено комплексну імітацію цілеспрямованої кібератаки класу APT. Запропонований метод забезпечив найвищий відсоток виявлення APT-атак 97%, виявлення lateral movement 94%, запобігання ексфільтрації 92%, виявлення Lateral movement 94% та найменший середній час реакції 0,8с. Отримані результати впроваджені ТОВ «Науково-виробниче підприємство хімічних продуктів» (акт впровадження від 18.03.2026 р.) при вдосконаленні інформаційної мережі підприємства;

- розроблені модель та методи використано в навчальному процесі Державного університету інформаційно-комунікаційних технологій при оновленні робочих програм навчальних дисциплін та підготовці методичного забезпечення кафедр комп'ютерних наук та штучного інтелекту (акт використання від 17.03.2026р.).

Результати дослідження можуть бути використані при побудові захищених корпоративних SD-WAN-мереж, державних інформаційних систем, хмарних платформ, центрів обробки даних та об'єктів критичної інформаційної інфраструктури.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконана відповідно до положень Законів України “Про інформацію”, “Про концепцію національної програми інформатизації”, Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25.02.2017 р. № 47/2017; Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.2020 № 392/2020, та плану наукової та науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій, а саме в рамках науково-дослідних робіт «Методика підвищення ефективності систем управління безпроводовими мережами на основі векторного синтезу» (Державний реєстраційний номер ОК 0226U000385) та «Методи побудови функціонально стійких захищених інформаційних систем з централізованим управлінням» (Державний реєстраційний номер РК 0125U002823).

Повнота викладу основних результатів дисертації в публікаціях

Одержані автором результати дисертаційної роботи опубліковано в 11 наукових працях. У їх склад входять: 2 наукові статті у періодичних наукових виданнях, які індексуються наукометричною базою *Scopus*; 9 наукових статей у періодичних виданнях України включених до “Переліку наукових фахових видань України”. За матеріалами виступів на науково-технічних конференціях опубліковано 11 тез доповідей.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення

Дисертаційна робота Вишнівського О.В. та анотація до неї мають закінчений змістовний обсяг наукової праці. Характеризуються логічним поданням наукового матеріалів і відповідають діючим вимогам щодо дисертацій на здобуття наукового ступеня доктора філософії передбаченим чинним Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженим постановою Кабінету Міністрів України від 12 січня 2022 р. №44.

Зауваження до проведеного дисертаційного дослідження

Аналіз змісту дисертаційної роботи, поданих в ній наукових та практичних результатів дисертаційного дослідження дозволи позитивно оцінити її зміст та визначити певні зауваження, що подані нижче:

1. В дисертаційній роботі обґрунтовано вибір математичного апарату простору станів для побудови моделі інтелектуальної комп'ютерної системи

з управлінням SD-WAN. Проте недостатньо розглянуто питання стійкості моделі до значних змін параметрів мережевого середовища та неповноти вхідних даних.

2. В дисертаційній роботі недостатньо розглянуто питання обчислювальної складності побудови та реалізації графу атак у великих розподілених SD-WAN інфраструктурах з динамічною топологією.

3. Під час моделювання сценаріїв атак основна увага приділена відомим загрозам, тоді як стійкість запропонованого методу до атак нульового дня (Zero-Day Attacks) досліджена недостатньо повно.

4. У дисертаційній роботі не достатньо повно описана процедура адаптації графу атак до змін конфігурації SD-WAN, зокрема під час автоматичного додавання нових вузлів, сервісів та політик маршрутизації.

5. Дисертаційна робота містить результати комп'ютерного моделювання для оцінки методу інтелектуального управління комп'ютерною системою SD-WAN. При виборі архітектури нейронної мережі обрано два приховані шари з 256 та 128 нейронами, проте відсутнє обґрунтування причин вибору саме такої конфігурації.

Приведені зауваження не впливають на наукову цінність та новизну поданих в дисертаційній роботі Вишнівського Олександра Вікторовича результатів. Робота має важливе теоретичне і практичне значення.

Висновок

Дисертаційна робота Вишнівського О.В. є завершеною науковою роботою, що містить нові наукові результати, які в сукупності вирішують актуальне наукове завдання щодо розроблення моделей і методів побудови захищеної інтелектуальної комп'ютерної системи з управлінням SD-WAN на основі графу атак.

За рівнем наукової новизни, якістю досліджень, достовірністю та обґрунтованістю висновків дисертація Вишнівського О.В. на тему «Метод побудови захищеної комп'ютерної системи на основі графу атак та штучного інтелекту» відповідає спеціальності 122 Комп'ютерні науки і чинним вимогам п. 6-9 «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 – Вишнівський Олександр Вікторович, заслуговує на присудження ступеня доктора філософії за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент

декан факультету інформатики та обчислювальної техніки

Національного технічного університету України

«Київський політехнічний інститут імені Ігоря Сікорського», МОН України

доктор технічних наук, професор

