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, професора кафедри інженерії програмного забезпечення та кібербезпеки Факультету інформаційних технологій Державного торговельно-економічного університету **Хлапоніна Юрія Івановича** 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 IT характеризується швидким переходом до розподілених комп'ютерних систем, активним впровадженням хмарних та мобільних платформ, технологій програмно-керованих мереж. Використання SD-WAN забезпечує централізоване адміністрування мережевої інфраструктури, гнучке керування маршрутизацією трафіку та зменшення витрат на експлуатацію. Проте застосування SD-WAN обумовлює виникнення нових загроз у сфері кібербезпеки. Програмне централізоване управління, використання віртуалізованих компонентів, інтеграція із зовнішніми хмарними платформами та автоматизоване налаштування політик маршрутизації формують додаткові потенційні точки атаки. Сучасні кіберзагрози відзначаються високим рівнем автоматизації, використанням методів штучного інтелекту, складними багаторівневими сценаріями атак та здатністю адаптуватися до змін середовища. Найбільшу небезпеку становлять атаки класу Advanced Persistent Threat, метою яких є тривале приховане перебування у мережі, поступове отримання розширених привілеїв і компрометація критично важливих ресурсів. Тому забезпечення безпеки комп'ютерних систем з управлінням SD-WAN є особливо актуальним.

Суттєву роль у дослідженні безпеки комп'ютерних систем відіграють графи атак, які дають змогу формалізувати можливі сценарії дій зловмисника, визначати взаємозв'язки між уразливостями, мережевими

вузлами та рівнями доступу. Проте наявні підходи до побудови таких графів мають низку обмежень. Більшість із них орієнтовані на статичні мережеві структури та не враховують динамічні зміни топології SD-WAN-мереж, модифікацію політик маршрутизації й оновлення конфігурацій віртуалізованих компонентів. Із розширенням масштабів мережевої інфраструктури графи атак стають значно складнішими, що спричиняє збільшення обчислювальних витрат на їх аналіз і ускладнює використання таких моделей у режимі реального часу.

Одним із найперспективніших напрямів удосконалення сучасних систем кібербезпеки є впровадження методів штучного інтелекту та машинного навчання. Застосування цих технологій дозволяє автоматизувати аналіз великих обсягів мережевого трафіку, виявлення аномальної активності, класифікацію кіберзагроз і прогнозування можливих сценаріїв атак. Інтелектуальні алгоритми здатні адаптуватися до змін у мережевому середовищі, що забезпечує більш ефективне та проактивне реагування на нові типи кіберзагроз.

Дисертаційна робота Вишнівського О.В. присвячена розв'язанню актуального наукового задання 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 та практичних рекомендацій обумовлена аналізом та теоретичним узагальненням широкого кола наукових праць вітчизняних та зарубіжних авторів. Використання достатньої кількості результатів наукових та практичних публікацій у їх поєднанні з задіяними коректними методами досліджень мають позитивний вплив на достовірність наукових положень, висновків та практичних рекомендацій, що подані в роботі.

Для розв'язання конкретних завдань дослідження автор широко застосовує загальнонаукові і емпіричні методи дослідження. Дослідження базується на сучасних методах системного підходу, теорії графів, імовірнісного аналізу, теорії управління, машинного навчання та архітектурного проєктування програмно-конфігурованих мереж.

Достовірність і новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації підтверджується результатами імітаційного моделювання.

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

Подані в роботі модель та методи дозволяє отримати наступні науково обґрунтовані практичні результати. А саме.

1. Проведено комплексний аналіз 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;

2. 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%;

3. На основі удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN, графу атак та розробленого алгоритму Q-навчання було спроєктовано 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%, запобіганя

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 вдосконалені інформаційної мережі підприємства;

4. 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, зокрема: 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 автор недостатньо висвітлив питання масштабованості запропонованої системи для географічно-розподілених комп'ютерних SD-WAN мереж та корпоративних інфраструктур із значною кількістю вузлів і каналів передачі даних.

2. У дисертаційній роботі автором недостатньо обґрунтовано вибір саме Q-навчання як базового алгоритму навчання з підкріпленням порівняно з такими підходами Deep Q-Network (DQN), Proximal Policy Optimization (PPO) або Actor-Critic.

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:
професор кафедри інженерії програмного забезпечення та кібербезпеки
Державного торговельно-економічного університету

доктор технічних наук, професор Юрій ХЛАПОНІН

Державний торговельно-економічний університет
Ідентифікаційний код 44470624

Підпис Ю. Хлапоніна засвідчую
Начальник відділу кадрів
Н. Шевченко