

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

*Кваліфікаційна наукова праця
на правах рукопису*

ВИШНІВСЬКИЙ ОЛЕКСАНДР ВІКТОРОВИЧ

УДК 004.724.4:004.896

ДИСЕРТАЦІЯ

МЕТОД ПОБУДОВИ ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ НА
ОСНОВІ ГРАФУ АТАК ТА ШТУЧНОГО ІНТЕЛЕКТУ

122 «Комп'ютерні науки»

12 «Інформаційні технології»

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

_____ В.О. Вишнівський

(підпис, ініціали та прізвище здобувача)

Науковий керівник

Катков Юрій Ігорович

доктор технічних наук, доцент

Київ – 2026

АНОТАЦІЯ

Вишнівський В.О. Метод побудови захищеної комп'ютерної системи на основі графу атак та штучного інтелекту. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки» – Державний університет інформаційно-комунікаційних технологій Міністерства освіти і науки України, Київ, 2026.

В дисертаційній роботі вирішено актуальне науково-практичне завдання розробки моделей і методів побудови захищеної інтелектуальної комп'ютерної системи з управлінням SD-WAN на основі графу атак.

Сучасний розвиток інформаційних технологій (ІТ) характеризується широким використанням комп'ютерних систем та хмарних ресурсів в умовах суттєвого збільшення обсягів обробки та передачі інформації. Робота висвітлює дослідження, спрямовані на усунення фундаментальних прогалин існуючих комп'ютерних систем, пов'язаних з їх недостатньою ефективністю, продуктивністю, захищеністю, гнучкістю та адаптивністю, що обмежує потенціал обробки інформації та надання якісних послуг користувачам.

В частині моделювання комп'ютерних систем з управлінням SD-WAN, проаналізовано існування кількох підходів, а саме на базі теорії масового обслуговування та лінійно-квадратичного регулювання. Встановлено, що ключовим недоліком існуючих систем є необхідність точної лінійної моделі та недостатня адаптивність до нелінійностей реальної мережі, зокрема при зміні рівня завантаження більш ніж на 20–30% від робочої точки, що обґрунтувало потребу в розробці гібридної моделі комп'ютерної системи SD-WAN у просторі станів з використанням машинного навчання.

В частині застосування методів машинного навчання у задачах управління комп'ютерними системами активно досліджується з кінця 2010-х років. Встановлено, що традиційні підходи, що засновані на статичних таблицях маршрутизації та протоколах BGP/OSPF, не здатні в режимі реального часу

враховувати стан каналів, рівень завантаженості та визначати прогностичні характеристики якості обслуговування. За своєю суттю, SD-WAN є архітектурним підходом до управління розподіленими мережами, що відокремлює площину управління від площини передачі даних, дозволяючи централізовано конфігурувати та оптимізувати мережеву інфраструктуру незалежно від фізичних транспортних технологій. Це обґрунтувало потребу в розробці методу інтелектуального управління комп'ютерною системою SD-WAN на основі алгоритмів машинного навчання, що дозволяє SD-WAN контролерам самостійно виробляти оптимальні стратегії вибору шляху на основі багатфакторної оцінки: затримки, джиттера, втрати пакетів, пропускну здатності та пріоритету типу трафіку.

В частині кібербезпеки комп'ютерних систем, SD-WAN передбачає децентралізовану топологію з множиною точок підключення до різномірних транспортних середовищ – MPLS, LTE/5G, широкосмугового Інтернету та супутникових каналів, що принципово розширює поверхню атаки та ускладнює реалізацію єдиної політики безпеки. Встановлено, що традиційні методи кіберзахисту, у яких периметр захисту був чітко визначений, являються неефективними. Це обґрунтувало потребу в удосконаленні методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та глибокого навчання з підкріпленням.

Таким чином, проведений аналіз підтвердив актуальність теми роботи та дозволив сформулювати чітке завдання дослідження, спрямоване на розробку цілісного комплексу моделей та методів, що усувають виявлені прогалини та складається з трьох ключових наукових результатів.

По-перше, розроблено модель комп'ютерної системи SD-WAN у просторі станів. Модель представляє собою сукупність векторів стану, управління та функцію якості обслуговування, що дозволяє враховувати динаміку завантаження каналів, затримки, втрати пакетів та стан буферів вузлів комп'ютерної системи SD-WAN. Наукова новизна полягає в тому, що вона ґрунтується на теорії автоматичного управління. Дана модель може бути

застосована у вигляді лінеаризованого варіанту для проведення аналітичних розрахунків, так і у вигляді повної нелінійної форми для проведення симуляції. Визначені умови стійкості та керованості комп'ютерної системи. Для лінійної моделі отримано аналітичний розв'язок задачі оптимального управління SD-WAN.

По-друге, розроблено метод інтелектуального управління комп'ютерною системою SD-WAN на основі комплексного підходу до управління інформаційною мережею SD-WAN. Метод дозволяє знизити затримки, рівень втрати пакетів і підвищити значення функціоналу якості. Наукова новизна полягає в тому, що він ґрунтується на основі машинного навчання. Результати симуляції комп'ютерної системи SD-WAN свідчать, що запропонований підхід машинного навчання з підкріпленням на основі узагальненої моделі у просторі станів забезпечує найкращі показники: середнє завантаження каналів знижується на 44% порівняно з базовим методом ECMP, середня затримка – на 65%, рівень втрати пакетів – на 85%, а значення функціоналу якості покращується на 61%.

По-третє, удосконалено метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак. Метод дозволяє превентивно перебудовувати мережеві маршрути та розривати ланцюжки кібератак на ранніх стадіях їх розвитку. Метод відрізняється від існуючих тим, що він ґрунтується на основі глибокого навчання з підкріпленням. Сформовано математичну модель оцінки ризиків, яка трансформує топологію мережі та відомі вразливості у спрямований граф атак. Розрахунок імовірності проходження вектора атаки та критичності цільового вузла дає змогу системі ухвалювати рішення на основі чітких кількісних метрик. Експериментально доведено, що метод забезпечив найвищу ефективну пропускну здатність 942Mbps, показав мінімальну середню затримку 8,4ms та мінімальний рівень втрат пакетів 0,12. 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.

Для проведення емпіричної валідації удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та оцінки ефективності алгоритму Q-навчання було спроектовано та розгорнуто комплексний імітаційний тестовий стенд та розроблено комплексну імітацію цілеспрямованої кібератаки класу APT.

Отримані моделі та методи усувають виявлені недоліки існуючих комп'ютерних систем SD-WAN та формують такі переваги, як висока продуктивність, пропускна здатність, мінімальна середня затримка, мінімальний рівень втрат пакетів, високий відсоток виявлення APT-атак, виявлення lateral movement, запобігання експільтрації, виявлення Lateral movement та найменший середній час реакції.

Ключові слова: комп'ютерні системи, високонавантажені системи, розподілені системи, інформаційні технології, блокчейн, смарт-контракти, масштабованість, надійність, продуктивність, інформаційна безпека, децентралізація, управління ресурсами, обробка даних, розподілені обчислення, архітектура систем.

ABSTRACT

Vyshnivskyi V.O. Method for Building a Secure Computer System Based on an Attack Graph and Artificial Intelligence. – Qualifying scientific work as a manuscript.

Dissertation for obtaining the degree of Doctor of Philosophy in the field of knowledge 12 “Information Technologies” in specialty 122 “Computer Science” – State University of Information and Communication Technologies of the Ministry of Education and Science of Ukraine, Kyiv, 2026.

The dissertation solves an important scientific and practical task of developing models and methods for building a secure intelligent computer system with SD-WAN management based on an attack graph.

The modern development of information technologies is characterized by the widespread using of computer systems and cloud resources under conditions of a significant increase of the amount of information processing and transmission. The work highlights research aimed at eliminating the fundamental shortcomings of existing computer systems related to their lack of the efficiency, performance, security, flexibility, and adaptability, which limits the potential of information processing and the provision of high-quality services to users.

In terms of computer systems modeling with SD-WAN management, several approaches have been analyzed, namely those based on queuing theory and linear-quadratic regulation. It has been established that the key drawback of existing systems is the requirement for an accurate linear model and insufficient adaptability to the nonlinearities of real networks, particularly when the load level changes by more than 20–30% from the operating point. This substantiated the need to develop a hybrid model of an SD-WAN computer system in the state space using machine learning methods.

The application of machine learning methods to computer system management tasks, active research has been conducted since the late 2010s. It has been determined that traditional approaches based on static routing tables and BGP/OSPF protocols are unable to take into account in real time for channel conditions, load levels, and

predictive quality-of-service characteristics. In essence, SD-WAN is an architectural approach to managing distributed networks that separates the control layer from the data layer, enabling centralized configuration and optimization of network infrastructure independently of physical transport technologies. This substantiated the need to develop a method for intelligent management of an SD-WAN computer system based on machine learning algorithms, enabling SD-WAN controllers to independently generate optimal path selection strategies based on multifactor evaluation, including latency, jitter, packet loss, bandwidth, and traffic type priority.

In the field of cybersecurity of computer systems, SD-WAN involves a decentralized topology with multiple connection points to heterogeneous transport environments such as MPLS, LTE/5G, broadband Internet, and satellite channels, which fundamentally expands the attack surface and complicates the implementation of a unified security policy. It has been established that traditional cybersecurity methods, where the security perimeter was clearly defined, are ineffective. This substantiated the need to improve the method for building a secure SD-WAN computer system based on attack graphs and deep reinforcement learning.

Thus, the conducted analysis confirmed the relevance of the dissertation topic and made it possible to formulate a clear research objective aimed at developing a comprehensive set of models and methods that eliminate the identified shortcomings and consist of three key scientific results.

First, a model of an SD-WAN computer system in the state space has been developed. The model represents a set of state vectors, control vectors, and a quality-of-service function, which makes it possible to take into account for channel load dynamics, delays, packet losses, and the state of node buffers in the SD-WAN computer system. The scientific novelty lies in the fact that the model is based on automatic control theory. This model can be applied both as a linearized version for analytical calculations and as a full nonlinear form for simulation purposes. The stability and controllability conditions of the computer system have been determined. For the linear model, an analytical solution to the optimal SD-WAN control problem has been obtained.

Second, the method of intelligent management of an SD-WAN computer system based on an integrated approach to SD-WAN information network management has been developed. The method makes it possible to reduce latency and packet loss levels and improve the value of the quality functional. The scientific novelty lies in the fact that the method is based on machine learning. The results of the SD-WAN computer system simulation indicate that the proposed reinforcement learning approach based on a generalized state-space model provides the best performance indicators: average channel utilization is reduced by 44% compared to the baseline ECMP method, average latency by 65%, packet loss by 85%, and the quality functional value is improved by 61%.

Third, the method for building a secure SD-WAN computer system based on an attack graph has been improved. The method enables proactive reconfiguration of network routes and disruption of cyberattack chains at early stages of their development. The proposed method differs from existing approaches in that it is based on deep reinforcement learning. A mathematical risk assessment model has been developed, transforming the network topology and known vulnerabilities into a directed attack graph. Calculating the probability of attack vector traversal and the criticality of the target node enables the system to make decisions based on clear quantitative metrics. Experimental results demonstrated that the method achieved the highest effective throughput of 942 Mbps, the minimum average latency of 8.4 ms, and the minimum packet loss rate of 0.12. The method also ensured the highest detection rate of APT attacks at 97%, lateral movement detection at 94%, exfiltration prevention at 92%, and the shortest average response time of 0.8 s.

To perform empirical validation of the improved method for building a secure SD-WAN computer system based on attack graphs and to evaluate the effectiveness of the Q-learning algorithm, a comprehensive simulation testbed was designed and deployed, and a comprehensive simulation of a targeted APT-class cyberattack was developed.

The obtained models and methods eliminate the identified shortcomings of existing SD-WAN computer systems and provide such advantages as high

performance, high throughput, minimal average latency, minimal packet loss, high APT attack detection rate, effective lateral movement detection, exfiltration prevention, and minimal average response time.

Keywords: computer system, software-defined networks, machine learning, cybersecurity, information security, intelligent systems, artificial neural networks, cyberattack, information system, information protection, artificial intelligence, deep learning, network security, information network, software systems quality.

Матеріали й тези наукових конференцій

1. Катков Ю.І., Вишнівський О.В., Заднепрянець О.Ю. Дослідження способів застосування штучного інтелекту для моніторингу ІТ-інфраструктури / Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /16 грудня / Київ: ДУІКТ, - 2023р. – С. 72.

https://duikt.edu.ua/uploads/p_2626_86233288.pdf

2. Кравчук П.О., Іщераков С.В., Василенко В.В., Вишнівський О.В. Рекомендаційні системи для вибору мережевого обладнання на основі JAVA технологій / Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /16 грудня / Київ: ДУІКТ, - 2023р. – С. 77.

https://duikt.edu.ua/uploads/p_2626_86233288.pdf

3. Кравчук П.О., Іщераков С.В., Єрмоленко В.О., Вишнівський О.В. Аналіз JAVA фреймворків для авторизації та аутентифікації / Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /16 грудня / Київ: ДУІКТ, - 2023р. – С. 72. https://duikt.edu.ua/uploads/p_2626_86233288.pdf

4. Каргаполов Ю.В., Бледнов В.О., Єрмоленко В.О., Вишнівський О.В. Управління ідентифікацією цифрових об'єктів для мультисервісних систем / Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /16 грудня / Київ: ДУІКТ, - 2023р. – С. 74. https://duikt.edu.ua/uploads/p_2626_86233288.pdf

5. Катков Ю.І., Вишнівський О.В., Бондар В.О., Кравець А.А. Проблеми розробки інструментів для моніторингу потокового відео контенту з використанням штучного інтелекту // Всеукраїнська науково-технічна конференція «Застосування програмного забезпечення в інформаційно-

комунікаційних технологіях» /24 квітня / Київ: ДУІКТ, - 2024р. – С. 460.
https://duikt.edu.ua/uploads/p_2661_45497999.pdf

6. Крентовський Р.С., Вишнівський О.В., Ільїн О.О. Дослідження та аналіз архітектурних підходів при побудові клієнтсерверної взаємодії // IV Всеукраїнська науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті» /15 травня / Київ: ДУІКТ, - 2024р. – С. 128. https://duikt.edu.ua/uploads/p_2661_45318838.pdf

7. Вишнівський О.В., Мороз М.В. Перспективи застосування згорткових нейронних мереж для розпізнавання об'єктів у задачах SLAM для безпілотних систем // Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /12 грудня / Київ: ДУІКТ, - 2024р. – С. 21.
https://duikt.edu.ua/uploads/p_2661_51403301.pdf

8. Шикула О.М., Вишнівський О.В., Мацюк О.М. Дослідження додатку для роботи з математичними функціями на основі JAVASCRIPT // Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /12 грудня / Київ: ДУІКТ, - 2024р. – С95. https://duikt.edu.ua/uploads/p_2661_51403301.pdf

9. Прокопов С.В., Вишнівський О.В. Штучний інтелект і математичне моделювання // V Всеукраїнська науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті»/15 травня / Київ: ДУІКТ, - 2025р. – С. 39-41. https://duikt.edu.ua/uploads/p_2779_68674368.pdf

10. Катков Ю.І., Вишнівський О.В. Модель комп'ютерної мережі з управлінням SD-WAN математичним апаратом простору станів / VII Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /11 грудня / Київ: ДУІКТ, - 2025р. – С. 152.
https://duikt.edu.ua/uploads/p_2779_63555250.pdf

11. Катков Ю.І., Вишнівський О.В. Комплексний метод побудови захищеної комп'ютерної мережі на основі адаптивної самозахисної

інфраструктури / VII Всеукраїнська науково-технічна конференція «Застосування програмного забезпечення в інформаційно-комунікаційних технологіях» / 23 квітня / Київ: ДУІКТ, - 2026р. – С. 448-450.
https://duikt.edu.ua/uploads/p_3086_61927919.pdf.

Статті в наукових фахових виданнях

1. О.В. Вишнівський Критичні аспекти під час впровадження штучного інтелекту в галузі безпілотних транспортних засобів / Вишнівський О.В., Зінченко О. В., Катков Ю. І., Березовська Ю. В., Матвеев А. В. Наукові записки Державного університету телекомунікацій, – 2023, – №1 (2023). – с. 25-34.
<https://journals.dut.edu.ua/index.php/sciencenotes/article/view/2840/2743> DOI:
10.31673/2786-8362.2023.010303

2. О.В. Вишнівський Про деякі аспекти використання штучних нейронних мереж у аналітичній підтримці маркетингових стратегій / Вишнівський О.В., Березовська Ю. В., Ільїн О. О., Матвеев А. В., Мушко М. В. Наукові записки Державного університету телекомунікацій, – 2023, – №2 (2023). – с. 85-90.
<https://journals.dut.edu.ua/index.php/sciencenotes/article/view/2878/2778> DOI:
10.31673/2518-7678.2023.021010

3. Катков Ю.І., Ільїн О.Ю., Вишнівський О.В., Резніченко І.О. Розроблення комп'ютерних ігор із використанням технологій ігрового штучного інтелекту Зв'язок. – 2022. – № 1 (155)- С 16-24. DOI: 10.31673/2412-9070.2022.011725
<http://con.dut.edu.ua/index.php/communication/article/view/2580> DOI:
10.31673/2412-9070.2022.011725

4. О.В. Вишнівський Особливості архітектури моделей цифрових об'єктів у мультисервісних екосистемах / Каргаполов Ю. В., Вишнівський О. В., Гринкевич Г. О., Василенко В. В. Наукові записки Державного університету телекомунікацій, – 2024, – №1 (2024). – с. 33-39.
<https://journals.dut.edu.ua/index.php/sciencenotes/article/view/2944/2839> DOI:
10.31673/2786-8362.2024.010505

5. О.В. Вишнівський Забезпечення енергоефективності програмно визначених мереж (SDNs) при впровадженні різних схем безпеки / Вишнівський О.В., Гніденко М.П., Гніденко М.М., Зінченко В.В. Наукові записки Державного університету телекомунікацій, – 2024, – №2 (2024). – с. 73-83.

<https://journals.dut.edu.ua/index.php/sciencenotes/article/view/3092/2982> DOI: 10.31673/2786-8362.2024.028036

6. О.В. Вишнівський Проблеми, вирішення яких впливають на функціональну стійкість програмно-визначених мереж / Вишнівський О. В., Прокопов С. В., Серих С. О., Гніденко М. М. Зв'язок, 2024, 6(172), pp. 44-52 DOI: 10.31673/2412-9070.2024.060456

<https://con.dut.edu.ua/index.php/communication/article/view/2823/2713> DOI: 10.31673/2412-9070.2024.060456

7. Вишнівський О.В. Метод управління комп'ютерною мережею SD-WAN методами машинного навчання на основі математичної моделі у просторі станів / О.В. Вишнівський, Ю.І. Катков // Науковий журнал “Телекомунікаційні та інформаційні технології”. – К.: ДУІКТ, 2026. Вип.№ 1. – С. 208-217.

<https://tit.duikt.edu.ua/index.php/telecommunication/article/view/2712> DOI: 10.31673/2412-4338.2026.019020.

8. Олександр Вишнівський Невизначеність оцінювання кількісних характеристик якості програмного забезпечення / Антон Шантир, Ольга Зінченко, Євген Чичкарьов, Олександр Вишнівський // Безпека інформації, 2024, 2(30), pp. 202-211 DOI: 10.18372/2225-5036.30.19208

[file:///C:/Users/Victor/Downloads/Uncertainty+in+evaluating+quantitative+quality+characteristics+of+software%20\(1\).pdf](file:///C:/Users/Victor/Downloads/Uncertainty+in+evaluating+quantitative+quality+characteristics+of+software%20(1).pdf)

9. Вишнівський О.В. Метод побудови захищеної комп'ютерної системи на основі графу атак, що управляється SD-WAN / О.В. Вишнівський, Ю.І. Катков // Науковий журнал “ Наука і техніка сьогодні”. – К.: Видавнича група «Наукові перспективи», 2026. Вип. № 4(58) 2026. – С. 3377-3395.

https://files.ukr.net/package/item/download?item=1115170337&token=lWrGfqdAbj-Rvb25gaKGs5vwe0OSFuQuBWuMZWsdTXD1iPiDGgPrnT9ZdPxL4SsU_UPiMr0

[W5oBIWSH-YA4ULv4QD83NOS3LDXaSNGYmjFIpMreSiyd-KTqG--0UkLSHgCN2AcDqCw:Z7NI5_IazEwaVH7f](#) DOI: 10.52058/2786-6025-2026-4(58)-3377-3395.

*Статті в наукових фахових виданнях, що індексуються в міжнародних
базах Scopus*

1. Oleksandr Vyshnivskiy, Vadym Mukhin, Vitalii Kotelianets, Yuri Kargapolov, Valerii Zavgorodnii, Viktor Vyshnyvskiy "Issues of Organizing the Architecture of Processes for Identifying Digital Entities and Services", International Journal of Wireless and Microwave Technologies (IJWMT), Vol.15, No. 4, 8 Aug. 2025, pp. 19-30. <https://doi.org/10.5815/ijwmt.2025.04.02> <https://www.mecspress.org/ijwmt/ijwmt-v15-n4/IJWMT-V15-N4-2.pdf>

2. Oleksandr Vyshnivskiy, Vadym Mukhin, Olha Zinchenko, Vitalii Kotelianets, Oleksandr Zvenihorodskiy, Pavlo Kudrynskiy, Viktor Vyshnyvskiy "Cloud-native AI Pipelines for Continuous Infrastructure Optimization and Anomaly Detection", International Journal of Computer Network and Information Security (IJCNIS), Vol. 18, No. 2, Apr. 2026, pp. 1-18. <https://doi.org/10.5815/ijcnis.2026.02.01> <https://www.mecspress.org/ijcnis/ijcnis-v18-n2/v18n2-1.html>

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	18
ВСТУП.....	20
РОЗДІЛ 1. СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ КОМП'ЮТЕРНИХ СИСТЕМ З УПРАВЛІННЯМ SD-WAN.....	26
1.1. Стан і перспективи розвитку комп'ютерних систем з управлінням SD-WAN.....	27
1.1.1. Аналіз етапів розвитку глобальних корпоративних мереж...	27
1.1.2. Аналіз архітектурних принципів та основних концепцій SD-WAN.....	29
1.1.3. Аналіз існуючих підходів до моделювання SD-WAN.....	31
1.2. Стан і перспективи розвитку застосування технологій штучного інтелекту в комп'ютерних системах з управлінням SD-WAN.....	32
1.2.1. Застосування машинного навчання для динамічної маршрутизації та оптимізації трафіку.....	33
1.2.2. Автоматизація управління мережею на основі намірів.....	34
1.3. Стан і перспективи розвитку технологій кіберзахисту комп'ютерних систем з управлінням SD-WAN.....	36
1.3.1. Архітектурні особливості SD-WAN з точки зору кіберзахисту.....	36
1.3.2. Актуальні загрози та вектори атак на SD-WAN інфраструктури.....	37
1.3.3. Застосування штучного інтелекту для виявлення загроз у SD-WAN середовищах.....	39
1.4. Постановка наукового завдання.....	41
1.5. Висновки до розділу 1.....	44
РОЗДІЛ 2. РОЗРОБКА МОДЕЛІ КОМП'ЮТЕРНОЇ СИСТЕМИ SD-WAN МЕТОДОМ ПРОСТОРУ СТАНІВ	46
2.1. Аналіз сучасних досліджень системи управління комп'ютерної розподіленої мережі SD-WAN.....	46

2.2. Побудова математичної моделі комп'ютерної системи SD-WAN апаратом простору станів.....	48
2.2.1. Архітектура та основні компоненти SD-WAN.....	48
2.2.2. Визначення вектору стану моделі у просторі станів.....	51
2.2.3. Визначення вектору простору управляючих впливів.....	53
2.3. Розробка узагальненої моделі комп'ютерної системи SD-WAN апаратом простору станів.....	55
2.3.1. Модель динаміки переходів між станами системи.....	55
2.3.2. Визначення матриць стану та управління.....	59
2.4. Висновки до розділу 2.....	64
РОЗДІЛ 3. МЕТОД УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ МЕРЕЖЕЮ SD-WAN НА ОСНОВІ МАШИННОГО НАВЧАННЯ.....	66
3.1. Метод оптимального управління SD-WAN на основі машинного навчання.....	67
3.1.1. Постановка завдання розробки методу управління SD-WAN на основі навчання з підкріпленням.....	67
3.1.2. Розробка алгоритму для дискретного управління на основі методу глибокого навчання з підкріпленням для дискретного простору стану.....	69
3.1.3. Розробка алгоритму для неперервного управління на основі методу глибокого навчання з підкріпленням для неперервного простору стану.....	72
3.2. Метод забезпечення захисту комп'ютерної SD-WAN мережі на основі графу атак.....	74
3.2.1. Аналіз систем забезпечення захисту комп'ютерної SD-WAN мережі на основі графу атак.....	74
3.2.2. Розробка архітектури адаптивної системи кіберзахисту.....	79
3.2.3. Удосконалення методу динамічного управління мережевою безпекою на основі навчання з підкріпленням.....	89

3.3. Розробка алгоритму управління мережевою безпекою на основі навчання з підкріпленням.....	96
3.4. Висновки до розділу 3.....	98
РОЗДІЛ 4. ДОСЛІДЖЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ ТА ЇХНЯ ПРАКТИЧНА РЕАЛІЗАЦІЯ.....	101
4.1. Дослідження ефективності методу інтелектуального управління комп'ютерною системою SD-WAN.....	102
4.1.1. Побудова архітектури нейронної мережі.....	102
4.1.2. Алгоритм навчання агента SD-WAN та програмна реалізація середовища симуляції мережі SD-WAN.....	106
4.1.3. Результати симуляції комп'ютерної мережі SD-WAN.....	108
4.2. Дослідження ефективності методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак.....	111
4.2.1. Побудова архітектури тестового стенду.....	112
4.2.2. Опис експерименту по імітації цілеспрямованої кібератаки..	114
4.2.3. Реакція системи захисту на кібератаку та аналіз отриманих результатів.....	116
4.3. Висновки до розділу 4.....	123
ВИСНОВКИ.....	126
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	130
ДОДАТОК А Лістинг програмного коду «Алгоритм навчання агента SD-WAN».....	142
ДОДАТОК Б Лістинг програмного коду «Середовище симуляції мережі SD-WAN».....	143
ДОДАТОК В Лістинг програмного коду «Actor-Critic нейронна мережа (PPO)».....	146
ДОДАТОК Г Лістинг програмного коду «Навчання агента PPO».....	148
ДОДАТОК Д Акти впровадження.....	150

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Actions – агент

APT – складні, багатоетапні і цілеспрямовані загрози

Attacker – зловмисник

Bandwidth – пропускна здатність

Business Continuity – бізнес–процеси

Cloud–Native – хмарні середовища

Control Plane – площина управління

CVE/NVD– бази вразливостей

CVSS– метрики вразливостей

Data Plane – площина передачі даних

Denial of Service – відмови в обслуговуванні

Digital Twin – цифровий двійник

Edge – периферійні пристрої

Environment – комп'ютерна інфраструктура разом із діями зловмисника

False Positives – хибні спрацьовування

Firewall – міжмережевий екран

GAE – метод оцінки функції переваги A_t

GCN – графові згорткові нейронні мережі

IDS/IPS – системи виявлення вторгнень

IoC – індикатор компрометації

latency – затримка

Living off the Land, LotL – техніки прихованого проникнення

Loss Function – мінімізація функції втрат

MDP – марківський процес прийняття рішень

ML – методи машинного навчання

MLP – багатошарові перцептрони

MTTR – час реакції на інцидент

NetFlow/IPFIX – потік телеметрії

NetOps – мережеві інженери

Packet Loss – втрата пакетів

PPO – алгоритм методів навчання з підкріпленням для неперервних просторів дій

QoS якість – обслуговування

Q-функція – функція цінності стану

Rate Limiting – обмеження пропускної здатності

RNN – рекурентні нейронні мережі

RL – навчання з підкріпленням

SASE – Secure Access Service Edge

SD-WAN, Software-Defined Wide Area Network – програмно-конфігуровані глобальні мережі

SecOps – відділи кібербезпеки

Security Plane – площина моніторингу безпеки

SIEM – Security Information and Event Management

Target Network – цільова мережа

Time Gap – критичний часовий розрив

VLAN – підмережа

VNF – віртуальні мережеві функції

Zero-day – атака нульового дня

ZTP – Zero Touch Provisioning

граф атак – Attack Graphs

IS – інформаційна система

IT – інформаційні технології

ЦОД – центр обробки даних

ШІ – штучний інтелект

WAN – глобальні корпоративні мережі

Обґрунтування вибору теми дослідження. Сучасний етап розвитку ІТ характеризується активним переходом до розподілених цифрових інфраструктур, широким використанням хмарних сервісів, віртуалізації, мобільних платформ та концепцій програмно-керованих мереж. Особливого поширення набувають технології SD-WAN, які забезпечують централізоване управління мережевою інфраструктурою, підвищення гнучкості маршрутизації трафіку, оптимізацію використання каналів зв'язку та зниження експлуатаційних витрат. Використання SD-WAN стало важливою складовою цифрової трансформації корпоративних мереж, державних інформаційних систем (ІС), хмарних середовищ, фінансових установ, промислових об'єктів та критичної інфраструктури.

На сучасному етапі розвитку кіберпростору спостерігається постійне зростання кількості та складності кібератак. Особливо небезпечними є цілеспрямовані атаки типу АРТ, які здатні тривалий час залишатися непоміченими, поступово розширюючи рівень компрометації системи. У таких умовах традиційні засоби захисту інформації виявляються недостатньо ефективними.

Перспективним напрямом розв'язання зазначених проблем є використання моделей комп'ютерних систем у просторі станів. Для SD-WAN-систем моделювання у просторі станів є особливо важливим, оскільки конфігурація маршрутів, політик доступу та мережевих сервісів може змінюватися в режимі реального часу.

Важливе значення для аналізу безпеки комп'ютерних систем мають графи атак, які дозволяють описувати можливі сценарії дій порушника, взаємозв'язки між вразливостями, мережевими вузлами та рівнями привілеїв. Однак існуючі методи побудови графів атак мають низку суттєвих недоліків. Вони не враховують динамічну зміну топології SD-WAN-мережі, оновлення політик маршрутизації та зміну конфігурації віртуалізованих компонентів.

Одним із найбільш перспективних напрямів розвитку сучасних систем кібербезпеки є використання методів штучного інтелекту, зокрема технологій машинного навчання. Застосування технології штучного інтелекту дають можливість проводити автоматизацію процесів аналізу великих обсягів мережевих даних, виявлення аномалій, класифікації кіберзагроз та прогнозування сценаріїв атак. Разом із тим існуючі рішення на основі штучного інтелекту також характеризуються певними обмеженнями. Ефективність інтелектуальних систем значною мірою залежить від якості навчальних даних, які не завжди відображають реальні сценарії атак у SD-WAN-середовищах.

Особливо актуальною є задача інтеграції моделей простору станів, графів атак та методів штучного інтелекту в єдину систему аналізу та управління безпекою SD-WAN-інфраструктури. Наявні наукові підходи здебільшого розглядають зазначені компоненти окремо, що обмежує можливості комплексного оцінювання безпеки мережі та прогнозування розвитку атак.

Вагомий внесок у дослідження процесів обробки та передачі інформації, кіберзахисту та штучного інтелекту зробили вчені Беркман Л.Н., Корченко О.Г., Климаш М.М., Савченко В.А., Субач І.Ю., G. Hinton, J. Pearl та ін. Попри значні результати, у працях цих науковців залишаються недостатньо вирішеними питання управління мережевою безпекою інтелектуальних комп'ютерних систем з управлінням SD-WAN на основі графа атак. Відсутність інтегрованих моделей не дозволяє забезпечити ефективне адаптивне управління політиками безпеки, маршрутизацією трафіку та механізмами реагування на кіберінциденти в режимі реального часу визначає актуальність подальших розробок у цьому напрямі.

Таким чином, актуальність теми дисертаційної роботи визначається зростанням складності сучасних кіберзагроз у програмно-керованих мережах, недосконалістю існуючих методів забезпечення безпеки SD-WAN-інфраструктур, обмеженими можливостями традиційних графових моделей та необхідністю розроблення нових інтелектуальних методів побудови захищених

комп'ютерних систем у просторі станів на основі графів атак і технологій штучного інтелекту.

Тому, дисертаційна робота, що присвячена вирішенню науково-прикладного завдання розробки моделей і методів побудови захищеної інтелектуальної комп'ютерної системи з управлінням SD-WAN на основі графу атак, є актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота була виконана в рамках науково-дослідних робіт «Методика підвищення ефективності систем управління безпроводовими мережами на основі векторного синтезу» (Державний реєстраційний номер ОК 0226U000385), Державного університету інформаційно-комунікаційних технологій та «Методи побудови функціонально стійких захищених інформаційних систем з централізованим управлінням» (Державний реєстраційний номер РК 0125U002823), Державного університету інформаційно-комунікаційних технологій.

Мета і задачі дослідження. Метою дисертаційної роботи є підвищення ефективності функціонування захищених комп'ютерних системи SD-WAN на основі математичної моделі у просторі станів методами машинного навчання та управління мережевою безпекою з застосуванням графу атак і багатоагентного навчання з підкріпленням для розподіленого управління щоб мінімізувати час реакції на інциденти.

Для досягнення поставленої мети було визначено наступні **задачі**:

1. Провести аналіз сучасних підходів до моделювання комп'ютерних систем з управлінням SD-WAN, управлінням кіберзахистом таких систем з використанням графу атак на основі машинного навчання.

2. Розробити модель комп'ютерної системи з управлінням трафіком SD-WAN на основі апарату простору станів, яка забезпечує кількісне відображення часових характеристик передачі даних, зміни пропускної здатності каналів зв'язку, ступеня заповнення буферних черг мережеских вузлів та ймовірності втрат пакетів.

3. Розробити метод інтелектуального управління комп'ютерною системою SD-WAN, наукова новизна якого полягає в тому, що він ґрунтується на основі машинного навчання та дозволяє знизити затримки, рівень втрати пакетів і підвищити значення функціоналу якості.

4. Удосконалити метод побудови захищеної комп'ютерної системи SD-WAN на основі графу та глибокого навчання з підкріпленням.

5. Провести комплексне експериментальне дослідження розроблених моделей та методів за допомогою імітаційного моделювання для підтвердження їх ефективності.

Об'єкт дослідження – процеси функціонування високонавантажених комп'ютерних систем з управлінням SD-WAN.

Предмет дослідження – моделі та методи управління захищеними інтелектуальними комп'ютерними системами SD-WAN.

Методи дослідження. Для досягнення мети було використано такі методи дослідження: системний підхід, теорію графів, імовірнісний аналіз, теорії управління, методи машинного навчання та архітектурного проєктування програмно-конфігурованих мереж.

Наукова новизна одержаних результатів полягає в наступному:

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, пропускну здатності каналів зв'язку, ступеня заповнення буферних черг мережеских 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.

Практичне значення одержаних результатів. Метод інтелектуального управління комп'ютерною системою SD-WAN на основі узагальненої моделі у просторі станів забезпечує підвищення продуктивності інформаційної мережі: середнє завантаження каналів знижується на 44% порівняно з базовим методом ЕСМР, середня затримка – на 65%, рівень втрати пакетів – на 85%, а значення функціоналу якості покращується на 61%.

Створення інтелектуальних систем кіберзахисту нового покоління забезпечує проактивне виявлення загроз, мінімізує ризики компрометації мережевої інфраструктури, зниження кількості хибнопозитивних спрацювань та скорочення часу реагування на кіберінциденти. 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.

Окремі положення, обґрунтовані в дисертаційній роботі щодо ефективного побудови інтегрованих інтелектуальних захищених комп'ютерних систем з управлінням SD-WAN апаратом простору станів на основі графу атак впроваджені (підтверджено відповідними актами) в ТОВ «АЙТІ КУРСОР» (від 27.11.2025 р.), ТОВ «Науково-виробниче підприємство хімічних продуктів» (від 18.03.2026 р.).

Особистий внесок здобувача. Дисертація є самостійним науковим дослідженням. Всі результати, що виносяться на захист, отримані автором

особисто. Здобувачем розроблено модель комп'ютерної системи SD-WAN у просторі станів, метод інтелектуального управління комп'ютерною системою SD-WAN, алгоритмічне та програмне забезпечення для управління безпекою комп'ютерної системи SD-WAN на основі графу атак методом навчання з підкріпленням, удосконалено метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак.

Апробація матеріалів дисертації. Основні положення та результати дисертаційної роботи доповідалися та обговорювалися на міжнародних та всеукраїнських науково-практичних конференціях, а також обговорювалися на засіданнях кафедри комп'ютерних наук ДУІКТ, опубліковані в 9 наукових працях у періодичних виданнях України включених до Переліку наукових фахових видань України та у 2 виданнях, що індексуються в міжнародних наукометричних базах Scopus.

Структура та обсяг дисертації. Дисертаційна робота складається з анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, списку використаних джерел та додатків. Робота містить 21 рисунок, 5 таблиць та 10 сторінок додатків. Список використаних джерел налічує 110 найменувань.

Загальний обсяг дисертації становить 153 сторінки машинописного тексту, з них 109 сторінок основного тексту.

РОЗДІЛ 1

СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ КОМП'ЮТЕРНИХ СИСТЕМ З УПРАВЛІННЯМ SD-WAN

Цифрова трансформація сучасних технологій передачі інформації вимагає від комп'ютерних систем високої гнучкості, масштабованості та безпеки. Традиційні WAN-мережі, засновані на статичній маршрутизації та ручному налаштуванні кожного вузла, більше не здатні ефективно обслуговувати динамічний трафік хмарних застосунків (SaaS, IaaS). Тому сучасним рішенням цієї проблеми стала технологія програмно-визначених мереж у територіально розподілених середовищах – Software-Defined Wide Area Network (SD-WAN). Проте зі зростанням масштабів мереж складність управління ними виходить за межі можливостей людини, що зумовлює гостру потребу в автоматизації на основі штучного інтелекту (ШІ) [1], [52], [91], [104].

Сучасний стан автоматизації побудови SD-WAN характеризується переходом до концепції Zero Touch Provisioning (ZTP). Це дозволяє підключати нові філії компанії до загальної мережі без виїзду технічного спеціаліста на місце. Автоматизований контролер самостійно завантажує необхідні конфігурації та політики безпеки на Edge-пристрій відразу після його підключення до мережі Інтернет.

Проте автоматизація сьогодні – це не лише швидке розгортання. Це перехід до Intent-Based Networking – мереж, що керуються намірами. Замість програмування конкретних команд, адміністратор формує високорівневу мету, а система автоматизації самостійно розраховує та впроваджує відповідні параметри на всіх рівнях інфраструктури.

Найбільш значущим досягненням сучасності є впровадження методів Artificial Intelligence for IT Operations у середовище SD-WAN. Використовуючи рекурентні нейронні мережі (RNN) та алгоритми LSTM, системи аналізують телеметрію каналів зв'язку в реальному часі. Це дозволяє передбачити деградацію каналу (зростання затримки чи джиттера) ще до того, як користувач

відчує проблему. На відміну від стандартних алгоритмів, ШІ здатний аналізувати тисячі можливих шляхів у мультихмарних топологіях, обираючи оптимальний канал (MPLS, Internet, 5G) на основі вартості, продуктивності та поточної черги. Системи ШІ здатні ідентифікувати кореневу причину збою (Root Cause Analysis) та автоматично застосовувати заходи з відновлення стійкості, наприклад, переспрямовувати трафік або змінювати конфігурацію віртуальних шлюзів.

Захист SD-WAN сьогодні невіддільний від концепції Secure Access Service Edge (SASE). Сучасний стан кібербезпеки також вимагає інтелектуального аналізу кожної сесії.

Незважаючи на значний прогрес, аналіз ринку показує наявність низки бар'єрів. По-перше, це проблема того, що мережевим інженерам іноді важко зрозуміти, чому алгоритм прийняв саме таке рішення щодо перемаршрутизації трафіку. По-друге, це питання якості даних для навчання. Якщо вхідна телеметрія зашумлена або неповна, модель ШІ може генерувати помилкові рішення, що знижує загальну стійкість мережі.

Також актуальним залишається питання інтеграції SD-WAN із застарілою інфраструктурою, де автоматизація обмежена технічними характеристиками обладнання.

1.1. Стан і перспективи розвитку комп'ютерних систем з управлінням SD-WAN

1.1.1. Аналіз етапів розвитку глобальних корпоративних мереж

Глобальні корпоративні мережі Wide Area Network (WAN) пройшли тривалий шлях технологічної еволюції, що охоплює понад чотири десятиліття розвитку телекомунікаційної галузі. Початковий етап (1980–1995pp.) характеризувався домінуванням аналогових виділених ліній та ранніх пакетних мереж стандарту X.25, які забезпечували пропускну здатність у межах 64 Кбіт/с при значній вартості оренди каналів [2].

Перехід до цифрових технологій у 1995–2005 рр. ознаменувався масовим впровадженням протоколу Frame Relay та технології Asynchronous Transfer Mode, що дозволили підвищити пропускну здатність до рівня T1/E1 (1.544/2.048 Мбіт/с). Проте визначальним технологічним зрушенням стало впровадження протоколу Multiprotocol Label Switching, що забезпечив детерміновану якість обслуговування (QoS), передбачувану затримку та підтримку класів сервісу для трафіку різних категорій [3].

Технологія MPLS стала домінуючим рішенням для побудови корпоративних WAN впродовж 2005–2015 рр. Її ключовими перевагами є гарантований рівень Service Level Agreement, ізоляція трафіку, підтримка MPLS VPN, а також висока надійність опорної мережі оператора зв'язку. Разом із тим MPLS має суттєві обмеження: висока вартість оренди каналів (у 10–50 разів вища за широкосмугове підключення еквівалентної пропускну здатності), тривалий цикл провізйонування нових каналів (4–12 тижнів), жорстка прив'язаність до одного оператора та відсутність гнучкості у перерозподілі смуги пропускання [4].

Паралельно з розвитком MPLS активно розвивалися широкосмугові технології доступу: ADSL/VDSL, кабельні мережі DOCSIS, а згодом – оптоволоконні з'єднання GPON/FTTB. Ці технології забезпечили доступну за вартістю альтернативу MPLS, однак без гарантій QoS та з асиметричним профілем пропускну здатності. Криза традиційного WAN остаточно позначилась у контексті масового переходу корпорацій до хмарних обчислень та мобільної роботи персоналу: трафік все менше рухався між філіями East-West і все більше – між філіями та хмарними ресурсами North-South, що кардинально змінило профіль навантаження на WAN-інфраструктуру [5].

Саме в цьому контексті на початку 2010-х років виникла концепція Software-Defined WAN. Першою комерційною SD-WAN-системою прийнято вважати продукт компанії VeloCloud (заснована 2012 р.), що пізніше увійшла до складу VMware. Паралельно розвивались рішення Viptela (поглинута Cisco у 2017 р.), Silver Peak (поглинута HPE/Aruba у 2020 р.), Versa Networks та Fortinet.

Аналітична компанія Gartner вперше виділила SD-WAN як окрему успішну в розвитку категорію у 2017 р., а вже у 2025 р. ринок SD-WAN перевищив 3.2 млрд дол. США [6].

1.1.2. Аналіз архітектурних принципів та основних концепцій SD-WAN

Стандартизацію архітектури SD-WAN здійснює організація MEF Forum, що у 2019 р. опублікувала специфікацію MEF 70, оновлену до версії MEF 70.1 у 2021 р. [7]. Відповідно до цього стандарту, архітектура SD-WAN базується на п'ятих фундаментальних принципах.

Для розділення площин управління та даних централізований контролер приймає всі рішення щодо маршрутизації та QoS, а edge-пристрої (vCPE/uCPE) лише виконують ці рішення на рівні пересилання пакетів. Це принципово відрізняється від традиційних маршрутизаторів, де логіка управління й пересилання пакетів нерозривно пов'язані.

Для забезпечення транспортної незалежності SD-WAN-рішення використовує будь-які доступні WAN-з'єднання (MPLS, Internet broadband, LTE/5G, супутниковий зв'язок) як рівноцінні транспортні підкладки, формуючи поверх них уніфікований overlay-рівень із захищеними IPSec-тунелями. Це забезпечує незалежність від конкретного оператора зв'язку та можливість dynamic multi-homing.

Для забезпечення інтелектуальної маршрутизації, яка орієнтована на застосунки система ідентифікує типи застосунків на рівні L7 (за сигнатурами, DPI або хмарними інтелектуальними базами даних) та застосовує відповідні QoS-політики. Наприклад, VoIP-трафік автоматично спрямовується через MPLS-канал з найменшою затримкою, тоді як резервне копіювання – через дешевше broadband-з'єднання.

Для забезпечення централізованої оркестрації та відповідної аналітики єдина панель управління забезпечує видимість всієї розподіленої мережі у реальному часі, автоматизує розгортання нових вузлів та надає детальну

аналітику продуктивності для кожного застосунку, що є принципово недосяжним у традиційних WAN-архітектурах.

Ключовою метрикою, що відрізняє SD-WAN від традиційного WAN, є здатність до вимірювання якості каналів у реальному часі за параметрами: затримка (latency, мс), джиттер (jitter, мс), рівень втрати пакетів (packet loss, %) та доступна пропускна здатність (Мбіт/с). На основі цих вимірювань контролер здійснює динамічний вибір оптимального каналу для кожного класу трафіку, що принципово відрізняється від статичної маршрутизації OSPF/BGP у традиційних WAN [8].

На сьогодні глобальне використання технологій SD-WAN показує стійке зростання з Compound Annual Growth Rate до 30%. Основними чинниками зростання є масштабна хмарна міграція підприємств, поширення гібридної моделі роботи, стрімкий розвиток IoT-інфраструктури та початок масового впровадження мереж 5G як WAN-транспорту [76], [77].

Лідерами розвитку технологій SD-WAN являються Cisco (на базі платформи Viptela/Meraki), VMware (VeloCloud, Broadcom SD-WAN), Fortinet (FortiGate SD-WAN), Palo Alto Networks (Prisma SD-WAN) та HPE Aruba (EdgeConnect). Порівняльна характеристика провідних SD-WAN платформ приведена у табл. 1.1.

Таблиця 1.1

Порівняльна характеристика провідних SD-WAN платформ

Платформа	Вендор	ML/AI функції	Тип розгортання	Особливості
Viptela/Catalyst SD-WAN	Cisco	Cisco AI Network Analytics	On-prem/Cloud	Глибока інтеграція з IOS-XE, YANG-моделі
VeloCloud / Broadcom SD-WAN	Broadcom	Edge Intelligence	Cloud-first	Dynamic multi-path optimization
FortiGate SD-WAN	Fortinet	FortiAI, NGFW-інтеграція	On-prem / Hybrid	Безпека як основна концепція
Prisma SD-WAN	Palo Alto	AIOps, ML-аналітика	Cloud-native	SASE-архітектура, нульова довіра
EdgeConnect Ultra	HPE Aruba	Central NetConductor	Hybrid	Інтелектуальний WAN Boost

Аналіз табл. 1.1 свідчить, що всі провідні вендори інтегрують елементи штучного інтелекту та машинного навчання у свої платформи, однак більшість реалізацій є закритими та використовують переважно статистичні пороги та евристичні правила, а не повноцінні RL-алгоритми з оптимізацією за функціоналом якості [74], [86], [88]. Це підтверджує актуальність розробки математичної моделі SD-WAN з управлінням на основі навчання з підкріпленням.

1.1.3. Аналіз існуючих підходів до моделювання SD-WAN

Математичне моделювання комп'ютерних мереж у просторі станів є усталеним напрямом досліджень, що бере початок з класичних праць Kleinrock з теорії масового обслуговування та Bertsekas і Gallager [9], [94] з теорії мережевих потоків. Однак застосування цього апарату конкретно до SD-WAN є відносно новим напрямом.

Аналіз публікацій засвідчує існування кількох підходів до моделювання SD-WAN. Перший підхід – моделювання на базі теорії масового обслуговування – представлений роботами [10], де кожен канал e_k моделюється чергою типу $M/M/1$ або $M/G/1$. Модель затримки каналу за формулою Поллачека-Хінчина:

$$d_k(t) = d_k^{\{prop\}} + \frac{\rho_k(t)}{\mu_k(1 - \rho_k(t))} \left(1 + \frac{C_{s,k}^2}{2} \right), \quad (1.1)$$

де $d_k^{\{prop\}}$ – час передачі сигналу в лінії; $\rho_k(t) = \lambda_k(t)/\mu_k$ – коефіцієнт завантаження; $C_{s,k}^2$ – коефіцієнт варіації часу обслуговування. Ця модель точна для стаціонарного режиму, проте не описує перехідні процеси при зміні управляючого впливу.

Другий підхід – лінійно-квадратичне регулювання (LQR) – застосовано у роботі Mestres et al. [8] для оптимального управління SDN-мережами. Модель у просторі станів (5)–(6) лінеаризується біля робочої точки, після чого оптимальна матриця зворотного зв'язку K * знаходиться з рівняння Річчати:

$$P = Q + A^T P A - A^T P B (R + B^T P B)^{-1} B^T P A. \quad (1.2)$$

Перевагою LQR є аналітична розв'язаність та гарантована стійкість замкненої системи. Суттєвим обмеженням є необхідність точної лінійної моделі та недостатня адаптивність до нелінійностей реальної мережі, зокрема при зміні рівня завантаження більш ніж на 20–30% від робочої точки.

Третій підхід – гібридне моделювання (модель у просторі станів та RL) – є найперспективнішим та недостатньо дослідженим. Суть підходу полягає у використанні математичної моделі як симуляційного середовища для навчання RL-агента. Порівняльний аналіз підходів наведено у табл. 1.2.

Таблиця 1.2

Порівняльний аналіз підходів до моделювання SD-WAN

Підхід	Неліній-ність	Адаптив-ність	Збіжність	Обчислювальна складність
Теорія черг (M/M/1)	Часткова	Низька	Аналітична	O(M) – мінімальна
LQR (лінійна модель)	Ні	Низька	Рівняння Річчати	O(n ³) – полін.
DQN (дискр. д-ї)	Так	Висока	Емпірична	O(Nθ·B) – нейромережа
Гібридне моделювання	Так	Дуже висока	Стабільна (clip)	O(Nθ·B·K) – найвища
Model Predictive Control	Часткова	Середня	Оптимізаційна	O(n ² ·H) – горизонт H

1.2. Стан і перспективи розвитку застосування технологій штучного інтелекту в комп'ютерних системах з управлінням SD-WAN

Застосування методів машинного навчання (ML) у задачах управління комп'ютерними мережами активно досліджується з кінця 2010-х років. За своєю суттю, SD-WAN є архітектурним підходом до управління розподіленими мережами, що відокремлює площину управління від площини передачі даних,

дозволяючи централізовано конфігурувати та оптимізувати мережеву інфраструктуру незалежно від фізичних транспортних технологій [4].

При цьому кожен із виробників обладнання для інформаційних мереж інтегрує власні алгоритми на базі штучного інтелекту (ШІ) та машинного навчання (МН) у свої SD-WAN рішення, формуючи новий клас інтелектуальних мережевих платформ [11], [73].

Технологічне поєднання SD-WAN та ШІ зумовлено кількома чинниками. По-перше, динамічна природа SD-WAN генерує надзвичайно великі масиви телеметричних даних (трафік, затримки, якість каналів, метрики додатків), аналіз яких вручну є практично неможливим. По-друге, вимоги сучасного бізнесу до якості обслуговування (QoS) та безперебійності роботи критичних додатків стають дедалі суворішими. По-третє, поширення хмарних сервісів та моделей роботи Secure Access Service Edge (SASE) потребує адаптивних механізмів маршрутизації, що виходять за межі можливостей традиційних детермінованих алгоритмів [12], [81], [96].

1.2.1. Застосування машинного навчання для динамічної маршрутизації та оптимізації трафіку

Однією з центральних задач, де технології ШІ знаходять практичне застосування в SD-WAN середовищах, є динамічна маршрутизація трафіку. Традиційні підходи, засновані на статичних таблицях маршрутизації та протоколах BGP/OSPF, не здатні в режимі реального часу враховувати стан каналів, рівень завантаженості та прогностичні характеристики якості обслуговування [13], [82].

Алгоритми машинного навчання, зокрема методи навчання з підкріпленням, дозволяють SD-WAN контролерам самостійно виробляти оптимальні стратегії вибору шляху на основі багатфакторної оцінки: затримки, джиттера, втрати пакетів, пропускної здатності та пріоритету типу трафіку. Такі

системи здатні не лише реагувати на поточні умови мережі, але й прогнозувати деградацію якості каналів на підставі аналізу часових рядів [14], [89].

У рамках досліджень, проведених низкою науковців, зокрема в роботах Mestres et al. [8] та Rusek et al. [15], було продемонстровано, що рекурентні нейронні мережі (RNN) та їх різновид – довга короткочасна пам'ять (LSTM) – ефективно застосовуються для прогнозування навантаження на мережеві канали. Це дозволяє проактивно перерозподіляти трафік до настання деградації, підвищуючи загальну якість обслуговування та зменшуючи кількість порушень Service Level Agreement (SLA).

Окрема перспективна область – інтелектуальне управління якістю сервісу для критичних додатків, таких як VoIP, відеоконференції та транзакційні системи. Системи класифікації трафіку на базі глибокого навчання Deep Packet Inspection з елементами DNN здатні ідентифікувати тип трафіку навіть при шифруванні, ґрунтуючись на статистичних характеристиках потоків, що дозволяє застосовувати відповідні QoS-політики автоматично [16].

1.2.2. Автоматизація управління мережею на основі намірів

Концепція мереж на основі намірів Intent-Based Networking (IBN) є логічним розвитком SD-WAN парадигми, що передбачає можливість управляти мережею через декларативний опис бажаного стану, а не через конкретні команди конфігурації. Штучний інтелект виступає ключовим компонентом, що здійснює трансляцію намірів у конкретні мережеві конфігурації, а також безперервно верифікує відповідність поточного стану мережі заявленим намірам [17].

Провідні виробники, зокрема Cisco та Juniper Networks, інтегрували елементи IBN у свої SD-WAN платформи. Cisco DNA Center та Juniper Apstra використовують алгоритми ШІ для автоматизації процесів налаштування, верифікації та виправлення конфігурацій [18]. Такі системи здатні скорочувати

час реакції на мережеві інциденти з годин до хвилин, а в деяких сценаріях – автоматично усувати несправності без втручання оператора.

Важливою складовою IBN є механізми замкненого контуру управління, що реалізуються через ітераційний цикл: збір телеметрії – аналіз за допомогою ШІ – прийняття рішення – виконання дії – верифікація результату. Такий підхід дозволяє досягти самооптимізації та самовідновлення мережевої інфраструктури, що відповідає концепції автономних мереж, що активно розробляється стандартизаційними організаціями ETSI та TM Forum [19].

Незважаючи на значний прогрес у застосуванні ШІ в SD-WAN мережах, ряд фундаментальних дослідницьких проблем залишається відкритим. Так, питання пояснюваності (explainability) рішень, що приймаються алгоритмами машинного навчання в контексті мережевого управління, є критично важливим з точки зору відповідальності операторів. Концепція XAI (Explainable AI) активно досліджується в цьому контексті [20], проте практичне впровадження пояснюваних моделей у реальному часі потребує подальших розробок.

Також існує проблема забезпечення стійкості систем на базі ШІ до навмисних атак – так зване adversarial machine learning – набуває особливої актуальності в контексті мережевої безпеки [21]. Зловмисники можуть цілеспрямовано маніпулювати вхідними даними для систем ШІ, щоб обійти механізми виявлення аномалій або змусити систему прийняти хибні рішення щодо маршрутизації.

Стандартизація інтерфейсів та протоколів для обміну даними між ШІ-компонентами різних виробників у гетерогенних SD-WAN середовищах є нагальною потребою. Ініціативи IETF Network Management Operations (NMOP) та OpenConfig спрямовані на вирішення цієї проблеми [22], проте повноцінна міжвендорна сумісність ШІ-рішень залишається предметом майбутніх досліджень та стандартизаційних зусиль.

Таким чином ШІ стане невід'ємним компонентом будь-якого SD-WAN рішення, а автономні мережі, здатні до самоналаштування та самовідновлення без участі людини-оператора, стануть реальністю для великих корпоративних та

операторських інфраструктур. Інтеграція SD-WAN з технологіями 5G та Edge Computing відкриє нові виміри для застосування ШІ в управлінні розподіленими гетерогенними мережами наступного покоління [23].

Аналіз сучасного стану та перспектив застосування технологій штучного інтелекту в мережах SD-WAN показує, що дана галузь наукових досліджень перебуває на етапі активного розвитку. Ключові напрями застосування ШІ охоплюють динамічну маршрутизацію трафіку, виявлення аномалій та кіберзагроз, автоматизацію управління на основі намірів та реалізацію замкнених контурів самооптимізації. Практичне впровадження зазначених технологій пов'язане з рядом відкритих проблем, серед яких пояснюваність рішень ШІ, стійкість до adversarial-атак та стандартизація міжвендорної взаємодії. Подальші дослідження у цих напрямках становлять науковий інтерес та практичну значущість для розвитку наступного покоління інтелектуальних мережевих інфраструктур.

1.3. Стан і перспективи розвитку технологій кіберзахисту комп'ютерних систем з управлінням SD-WAN

1.3.1. Архітектурні особливості SD-WAN з точки зору кіберзахисту

Програмно-визначені глобальні мережі (SD-WAN) суттєво змінили підходи до побудови корпоративних інфраструктур, водночас породивши нові виклики в галузі кібербезпеки. На відміну від традиційних MPLS-мереж, у яких периметр захисту був чітко визначений, SD-WAN передбачає децентралізовану топологію з множиною точок підключення до різномірних транспортних середовищ – MPLS, LTE/5G, широкосмугового Інтернету та супутникових каналів [24], [105]. Це принципово розширює поверхню атаки та ускладнює реалізацію єдиної політики безпеки.

Централізований SD-WAN контролер, який є ключовим елементом архітектури, одночасно постає критичною точкою відмови та пріоритетною

ціллю для кіберзловмисників. Компрометація площини управління може призвести до повного порушення функціонування мережі, несанкціонованого перенаправлення трафіку або витоку конфіденційних даних [25]. Тому забезпечення безпеки площини управління (control plane security) є фундаментальною вимогою до будь-якого SD-WAN рішення [72].

Дослідження в цьому науковому напрямку виділяють три основні площини, захист яких необхідно забезпечити в SD-WAN середовищах: площина управління (control plane), площина даних (data plane) та площина оркестрації (orchestration plane) [26]. Кожна з них має специфічні вразливості та потребує відповідних механізмів захисту, що зумовлює необхідність комплексного підходу до побудови системи кіберзахисту SD-WAN мереж.

1.3.2. Актуальні загрози та вектори атак на SD-WAN інфраструктури

Аналіз сучасного ландшафту кіберзагроз для SD-WAN середовищ дозволяє виокремити кілька ключових векторів атак. Атаки типу Man-in-the-Middle (MitM) спрямовані на перехоплення або модифікацію трафіку між SD-WAN вузлами. Незважаючи на широке застосування IPsec та TLS для шифрування каналів передачі даних, неналежна конфігурація криптографічних параметрів або використання застарілих шифронаборів залишається поширеною вразливістю [27], [109].

Атаки на площину управління, зокрема ін'єкція хибних маршрутів та підробка ідентичності вузлів, є особливо небезпечними в контексті SD-WAN, оскільки дозволяють зловмисникам впливати на глобальну топологію мережі. Дослідження Scott-Hayward et al. [28] систематизували атаки на SDN/SD-WAN контролери та довели, що недостатня автентифікація між елементами площини управління є одним із найпоширеніших джерел вразливостей.

Окремої уваги заслуговують Distributed Denial of Service (DDoS-атаки), спрямовані на перевантаження SD-WAN контролера або граничних пристроїв. Оскільки SD-WAN вузли часто розгортаються на базі стандартного серверного

обладнання під управлінням загальноцільових операційних систем, вони є більш вразливими до експлуатації системних вразливостей порівняно з традиційними апаратними маршрутизаторами [29], [103].

Значну загрозу становлять атаки на ланцюг поставок, пов'язані з вбудовуванням шкідливого коду в програмне забезпечення SD-WAN рішень на етапі розробки або оновлення. Інцидент SolarWinds 2020 року наочно продемонстрував критичність цього вектора атак для мережевої інфраструктури загалом [30], [108].

Провідні виробники SD-WAN рішень інтегрують засоби кіберзахисту безпосередньо у платформу, формуючи концепцію Security-Driven Networking. Комплексні рішення класу Secure SD-WAN поєднують традиційні функції SD-WAN (динамічна маршрутизація, оптимізація WAN) із вбудованим міжмережним екраном нового покоління (NGFW), системою запобігання вторгненням (IPS), захистом DNS та URL-фільтрацією в рамках єдиної платформи [31].

Концепція Secure Access Service Edge (SASE), запропонована аналітиками Gartner у 2019 році, визначила стратегічний напрям конвергенції мережевих та безпекових функцій у єдиному хмарному сервісі. SASE об'єднує SD-WAN з такими технологіями, як Firewall-as-a-Service, Zero, Cloud Access Security Broker, Secure Web Gateway та Trust Network Access [32], [67]. Така архітектура забезпечує послідовне застосування політик безпеки незалежно від місцезнаходження користувача або пристрою.

Модель нульової довіри Zero Trust Architecture (ZTA), стандартизована NIST у документі SP 800-207 [33], стає де-факто стандартом для побудови системи кіберзахисту SD-WAN інфраструктур. Принцип не довіряти та завжди перевіряти реалізується через мікросегментацію мережі, багатофакторну автентифікацію, безперервну верифікацію ідентичності та мінімізацію привілеїв доступу для всіх суб'єктів мережевої взаємодії.

Криптографічний захист є фундаментальним механізмом безпеки SD-WAN. Сучасні реалізації використовують протокол IPsec з алгоритмами AES-

256-GCM для шифрування каналів передачі даних та RSA/ECDSA для автентифікації вузлів. Дедалі більшого поширення набуває застосування протоколу WireGuard як більш ефективної альтернативи IPsec завдяки спрощеній криптографічній базі та меншій поверхні атаки коду [34].

1.3.3. Застосування штучного інтелекту для виявлення загроз у SD-WAN середовищах

Інтеграція методів штучного інтелекту та машинного навчання у системи кіберзахисту SD-WAN мереж відкриває принципово нові можливості для виявлення та нейтралізації загроз. Поведінковий аналіз мережевого трафіку на базі алгоритмів машинного навчання дозволяє виявляти аномалії, що свідчать про несанкціоновану діяльність, значно ефективніше порівняно з традиційними сигнатурними методами [35], [99].

Алгоритми навчання без учителя, зокрема метод ізольованого лісу та автоенкодерів на базі глибоких нейронних мереж, застосовуються для побудови базових моделей нормальної поведінки мережі та автоматичного виявлення відхилень у режимі реального часу. Дослідження Mirsky et al. [36] продемонстрували ефективність ансамблевих автоенкодерів для онлайн-виявлення мережових вторгнень з низьким відсотком хибнопозитивних спрацювань.

Системи виявлення загроз на базі графових нейронних мереж Graph Neural Networks (GNN) є перспективним напрямом досліджень, що дозволяє моделювати мережеву топологію SD-WAN як граф та виявляти аномалії в структурі взаємодій між вузлами. Такий підхід ефективний для виявлення атак бокового переміщення у мережі – тактики, характерної для складних цільових атак (APT) [37].

Федеративне навчання відкриває можливість для побудови спільних моделей виявлення загроз між організаціями без необхідності централізованого обміну конфіденційними даними про трафік. Такий підхід є особливо

актуальним для галузевих та відомчих SD-WAN мереж, де обмін телеметричними даними між організаціями обмежений вимогами конфіденційності та нормативним регулюванням [38].

Нормативно-правова база у сфері кіберзахисту SD-WAN мереж перебуває у стадії активного формування. На міжнародному рівні ключовими орієнтирами є стандарти ISO/IEC 27001:2022 (системи управління інформаційною безпекою) та ISO/IEC 27033 (безпека мереж), які встановлюють загальні вимоги до захисту мережевої інфраструктури, застосовні й до SD-WAN середовищ [39].

Спеціалізовані рекомендації для SD-WAN безпеки розроблено рядом організацій. Cybersecurity and Infrastructure Security Agency (CISA) опублікувала технічні настанови щодо безпечного розгортання SD-WAN [40]. Організація European Union Agency for Cybersecurity (ENISA) підготувала тематичні звіти щодо загроз для SDN/NFV середовищ, що безпосередньо стосуються SD-WAN інфраструктур [41]. В Україні питання захисту інформаційно-телекомунікаційних систем регулюється Законом України «Про основні засади забезпечення кібербезпеки України» та відповідними нормативними документами ДССЗІ.

Перспективним напрямом стандартизації є розробка специфічних профілів безпеки для SD-WAN рішень у рамках ініціативи Metro Ethernet Forum (MEF), яка визначає сервісні атрибути та вимоги до безпеки SD-WAN сервісів операторського класу. Стандарт MEF 70.1 встановлює базові вимоги до SD-WAN сервісів, включаючи вимоги до шифрування та автентифікації [7].

Серед перспективних напрямів розвитку технологій кіберзахисту SD-WAN слід виокремити: впровадження постквантової криптографії для захисту від загроз з боку квантових комп'ютерів (NIST вже стандартизував перші постквантові алгоритми – CRYSTALS-Kyber та CRYSTALS-Dilithium); розвиток технологій автоматизованого реагування на інциденти (SOAR) з інтеграцією у SD-WAN платформи; застосування цифрових двійників мережевої інфраструктури для моделювання атак та тестування засобів захисту [42].

Аналіз сучасного стану та перспектив розвитку технологій кіберзахисту інформаційних мереж з управлінням SD-WAN засвідчує, що забезпечення безпеки таких мереж є багатовимірною проблемою, що охоплює захист площин управління, даних та оркестрації [106]. Розширена поверхня атаки, притаманна SD-WAN архітектурі, зумовлює необхідність застосування комплексних підходів на базі концепцій SASE та Zero Trust. Інтеграція методів штучного інтелекту у системи виявлення загроз суттєво підвищує ефективність кіберзахисту, проте потребує вирішення проблем пояснюваності та стійкості до adversarial-атак. Формування нормативно-правової бази та стандартизація у сфері SD-WAN безпеки залишаються актуальними напрямками, що потребують подальшого розвитку як на національному, так і на міжнародному рівнях.

1.4. Постановка наукового завдання

На основі проведеного аналізу стану і перспективи розвитку комп'ютерних систем з управлінням SD-WAN, технологій кіберзахисту комп'ютерних систем та застосування технологій штучного інтелекту можна виокремити наступні ключові наукові проблеми у галузі дослідження управління SD-WAN.

Більшість існуючих робіт розглядають окремі аспекти управління SD-WAN (маршрутизацію, QoS або безпеку), не пропонуючи єдиної системи рівнянь у просторі станів, що охоплює всі ключові параметри мережі. Це ускладнює формальний аналіз стійкості та оптимальності системи управління [4], [8] на основі комплексної математичної моделі.

Зі збільшенням розміру мережі ($N > 100$ вузлів, $M > 500$ каналів) розмірність простору станів стає надмірно великою для стандартних алгоритмів Deep RL. Необхідно розробити нові методи декомпозиції задачі на основі застосування ієрархічного RL, багатоагентного RL або факторизації простору станів [43], [44] для забезпечення масштабованості RL-агента.

Більшість RL-алгоритмів навчаються офлайн на симуляційних даних, а потім розгортаються у реальній мережі. Це створює семантичний розрив між

симуляцією та реальністю. Методи онлайн-навчання та адаптації домену для SD-WAN залишаються недостатньо дослідженими [45]. Тому необхідно розробити нові методи навчання у режимі реального часу

Рішення нейромережевих агентів складно інтерпретувати операторам мережі. Розробка методів ХАІ для мережевого управління є актуальним напрямом досліджень, оскільки мережеві оператори потребують розуміння причин прийнятих рішень [44], [46], [75]. Тому необхідні нові методи розробки нейромережевих агентів з прозорими рішеннями агента.

При забезпеченні кіберзахисту комп'ютерних систем з управлінням SD-WAN існують наступні проблеми.

Архітектурні вразливості полягають в тому, що централізований контролер SD-WAN є одночасно серцем мережі та найбільш привабливою цілью для атак. Його компрометація дає зловмиснику повний контроль над маршрутизацією трафіку всієї організації. Крім того, SD-WAN суттєво розширює поверхню атаки – замість одного MPLS-периметра з'являються десятки точок підключення через публічний Інтернет, LTE/5G та хмарні сервіси.

Протоколи взаємодії між контролером та граничними пристроями (edge devices) можуть бути вразливі до ін'єкції хибних маршрутів, подробиць ідентичності вузлів та перехоплення сесій управління. Це обумовлює загрози площини управління комп'ютерних систем з управлінням SD-WAN. Якщо автентифікація між елементами площини управління реалізована неналежно – зловмисник може перенаправити трафік організації непомітно для операторів.

Попри широке використання IPsec і TLS, на практиці часто трапляються: застарілі шифронабори, некоректна конфігурація, відсутність ротації ключів. Окремою перспективною загрозою є квантові комп'ютери, які в майбутньому здатні зламати поточні асиметричні алгоритми – тому перехід на постквантову криптографію вже є актуальним завданням. Тому системи шифрування обумовлюють криптографічні ризики.

SD-WAN за замовчуванням шифрує міжсайтовий трафік, що є перевагою з точки зору конфіденційності, але водночас сліпить традиційні системи

виявлення вторгнень. Виявляти шкідливу активність всередині зашифрованих тунелів без їх розшифрування – складне технічне завдання, яке вирішується методами статистичного аналізу трафіку та машинного навчання, але не повністю.

SD-WAN рішення – це складне програмне забезпечення від конкретних вендорів. Інцидент SolarWinds показав, що шкідливий код може бути впроваджений ще на етапі розробки або розповсюдження оновлень. Організація не має прямого контролю над цим вектором атак і змушена покладатися на заходи безпеки вендора.

Масовий перехід на хмарні сервіси (AWS, Azure, Microsoft 365) змінює модель трафіку: замість централізованої передачі через корпоративний центр обробки даних трафік іде напряму в хмару з кожного філіального офісу. Це ускладнює застосування єдиної політики безпеки та збільшує кількість неконтрольованих шляхів.

У великих розподілених SD-WAN мережах обсяг телеметричних даних є колосальним. Традиційні SIEM-системи часто не справляються з кореляцією подій у режимі реального часу через весь периметр мережі. Виявлення складних цільових атак (APT), які розгортаються повільно і маскуються під легітимний трафік, залишається відкритою проблемою.

Гнучкість SD-WAN є водночас і ризиком – автоматизоване розгортання політик через API дозволяє одній помилці конфігурації миттєво поширитись на всю мережу. Дослідження показують, що більшість інцидентів безпеки пов'язані не з вразливостями ПЗ, а з помилками адміністрування, а саме людського фактору.

Тому в роботі необхідно вирішити актуальне науково-практичне завдання з розроблення моделей і методів побудови захищеної інтелектуальної комп'ютерної системи з управлінням SD-WAN на основі графу атак.

Метою роботи являється підвищення ефективності функціонування захищених комп'ютерних системи SD-WAN на основі математичної моделі у просторі станів методами машинного навчання та управління мережевою

безпекою з застосуванням графу атак і багатоагентного навчання з підкріпленням для розподіленого управління щоб гарантувати мінімальний час реакції на інциденти.

Для досягнення мети дисертаційної роботи необхідно:

розробити комплексну математичну модель комп'ютерної системи з управлінням трафіком SD-WAN на основі апарату простору станів;

розробити метод управління комп'ютерною системою SD-WAN використовуючи методи машинного навчання на основі комплексної математичної моделі у просторі станів;

удосконалити метод побудови захищеної комп'ютерної системи на основі графу атак, що управляється SD-WAN;

Верифікація отриманих наукових результатів потребує створення спеціалізованого експериментального стенду у форматі віртуалізованого хмарного середовища, побудованого на засадах програмно-визначених мереж. Практична реалізація запропонованих теоретичних положень передбачає розроблення програмного комплексу, функціональність якого відповідає отриманим результатам дослідження.

1.5. Висновки до розділу 1

На основі проведеного аналізу стану та перспектив розвитку комп'ютерних систем з управлінням SD-WAN можна сформулювати такі основні висновки.

1. В першому розділі проведено обґрунтування важливості та актуальності вирішення актуального науково-практичного завдання з розроблення моделей і методів побудови захищеної інтелектуальної комп'ютерної системи з управлінням SD-WAN на основі графу атак. Проведено критичний аналіз літератури і сучасного стану досліджень в даній галузі.

2. Технологія SD-WAN є визначальним напрямом розвитку корпоративних WAN. Аналіз сучасного стану процесів автоматизації в SD-WAN свідчить про

те, що галузь перебуває на етапі переходу від реактивного управління до проактивного та автономного. Інтеграція штучного інтелекту дозволяє перетворити SD-WAN на інтелектуальну екосистему, здатну до самонавчання та самозахисту. Основними векторами розвитку на найближчі роки стануть подальше вдосконалення моделей глибокого навчання для прогнозування станів мережі та повна конвергенція мережевих функцій з хмарними сервісами безпеки в рамках архітектури SASE.

3. Методи навчання з підкріпленням (зокрема PPO) є найперспективнішим інструментом для вирішення задачі оптимального управління SD-WAN у просторі неперервних дій за умов нелінійної динаміки мережевого середовища.

4. В існуючих дослідженнях відсутня єдина комплексна математична модель SD-WAN у просторі станів, що охоплює динаміку завантаження каналів, затримки, втрати пакетів та стан буферів вузлів одночасно.

5. Перспективними напрями досліджень являється вдосконалення та розвиток методів побудови графів атак шляхом використання багаторівневих, ієрархічних та ймовірнісних графових моделей. Це дозволить враховувати не лише структуру мережі та наявні вразливості, а й поведінкові характеристики порушника, часові параметри атак, ризики каскадного поширення загроз і взаємозв'язки між фізичними та віртуальними компонентами SD-WAN-інфраструктури. Особливу увагу необхідно приділити дослідженням динамічних графів атак, здатних автоматично оновлюватися відповідно до зміни стану мережі та появи нових кіберзагроз..

Таким чином, в дисертаційній роботі вирішується актуальне науково-практичне завдання з розроблення моделей і методів побудови захищеної інтелектуальної комп'ютерної системи з управлінням SD-WAN на основі графу атак.

РОЗДІЛ 2.

РОЗРОБКА МОДЕЛІ КОМП'ЮТЕРНОЇ СИСТЕМИ SD-WAN МЕТОДОМ ПРОСТОРУ СТАНІВ

Технологія SD-WAN є одним із перспективних напрямів розвитку сучасної мережевої інфраструктури. Вона забезпечує централізоване програмне управління розподіленою мережею через уніфікований контролер [85], [87] відокремлюючи площину управління від площини даних [4]. Це дозволяє динамічно маршрутизувати трафік через кілька типів каналів зв'язку: виділені лінії MPLS, широкосмугові Internet-канали, LTE/5G – залежно від поточного стану мережі та встановлених політик якості обслуговування (QoS).

Разом із тим, зростання складності мережевих топологій, неоднорідність трафіку та динамічна зміна стану каналів зв'язку роблять задачу управління SD-WAN вкрай складною для класичних детермінованих методів [97], [98], [102]. Ефективне управління потребує врахування великої кількості взаємозалежних параметрів у реальному часі: пропускної здатності, затримки, джиттеру, рівня втрати пакетів тощо.

Тому в розділі необхідно розробити узагальнену математичну модель інформаційної мережі з управлінням SD-WAN у просторі станів [90], [92].

Для цього необхідно вирішити наступні завдання: формалізувати математичну модель мережі SD-WAN методом простору станів; визначити вектор стану, вектор управлінь та цільовий функціонал якості; дослідити стійкість системи та умови оптимальності.

2.1. Аналіз сучасних досліджень системи управління комп'ютерної розподіленої мережі SD-WAN

Дослідженню застосування теорії автоматичного до задач мережевого управління присвячено значну кількість наукових праць. В них [48] розглянуто застосування рівнянь простору стану для моделювання черг у мережах зі

своєчасною доставкою пакетів. Архітектурний базис розподіленої комп'ютерної мережі з SD-WAN концептуально корелює з ключовими положеннями парадигми SDN, серед яких є логічна централізація площини управління та абстрагування її функцій засобами спеціалізованого програмного забезпечення [53]. Технологія SD-WAN розширює зазначені положення: її функціонування ґрунтується на застосуванні уніфікованих централізованих політик маршрутизації та адаптивному перерозподілі трафіку на підставі неперервного моніторингу показників якості обслуговування [54], [80], [107].

Відповідно до результатів досліджень, викладених у працях [55], [56] та [57], архітектура SD-WAN реалізує комплекс взаємопов'язаних принципів: глобальну оптимізацію використання ресурсів глобальних мереж передачі даних (WAN), централізоване координування потоків інформації та інтелектуальне управління мережею на основі аналізу інтегрованих метрик якості з'єднань.

Застосування стохастичних процесів у межах теорії мережевого трафіку уможливорює формалізований опис динаміки зміни інтенсивності потоків даних у каналах зв'язку [58], [101].

З позицій теорії автоматичного управління трафіком методологія робастного синтезу регуляторів на основі лінійних матричних нерівностей у поєднанні з леммами обмеженого підсилення та Калмана–Якубовича–Попова забезпечує отримання гарантованих оцінок якості функціонування в умовах найгірших реалізацій збурювальних впливів [59]. Методи оптимального управління – лінійно-квадратичний регулятор та його стохастичне узагальнення – формують теоретичну основу «м'якої» оптимізації цільових показників, тоді як предиктивне управління за моделлю реалізує практично орієнтований механізм оптимізації з урахуванням явних обмежень на змінні стану та керувальні впливи [60], [100].

У [8] запропоновано підхід до оптимального маршрутизації в SDN-мережах із використанням лінійно-квадратичного регулятора. Але в них не враховують специфіки SD-WAN.

Використання машинного навчання в управлінні мережами [45], [49] Deep Q-Network застосовуються для управління QoS. Алгоритм Proximal Policy Optimization [50], [95] показав перевагу у задачах із неперервним простором дій. Однак більшість існуючих підходів розглядають лише окремі аспекти управління, не пропонуючи єдиної математичної апаратур простору станів для SD-WAN.

2.2. Побудова математичної моделі комп'ютерної системи SD-WAN апаратур простору станів

2.2.1. Архітектура та основні компоненти SD-WAN

Мережа SD-WAN являє собою трирівневу ієрархічну систему, яка охоплює: рівень управління (*Control Plane*), рівень оркестрування (*Orchestration Plane*) та рівень даних (*Data Plane*) [1], [4] (рис. 2.1.).

Принципова відмінність від традиційних WAN-рішень полягає у повному відокремленні площини управління від площини пересилання даних, являє собою систему що дозволяє реалізувати централізоване програмне управління гетерогенною мережевою інфраструктурою. Така архітектура забезпечує глобальну видимість стану мережі та можливість динамічного перерозподілу трафіку без втручання адміністратора.

Ключовим елементом архітектури є програмний вузол управління – контролер SD-WAN. Він безперервно збирає телеметрію з усіх граничних пристроїв мережі, обчислює оптимальні маршрути відповідно до встановлених політик та розподіляє керівні директиви. Для забезпечення відмовостійкості контролер, як правило, розгортається у вигляді кластера, однак з точки зору управління система розглядається як єдиний логічний вузол прийняття рішень. Саме контролер реалізує замкнений цикл управління мережею, постійно адаптуючи конфігурацію до поточного стану інфраструктури.

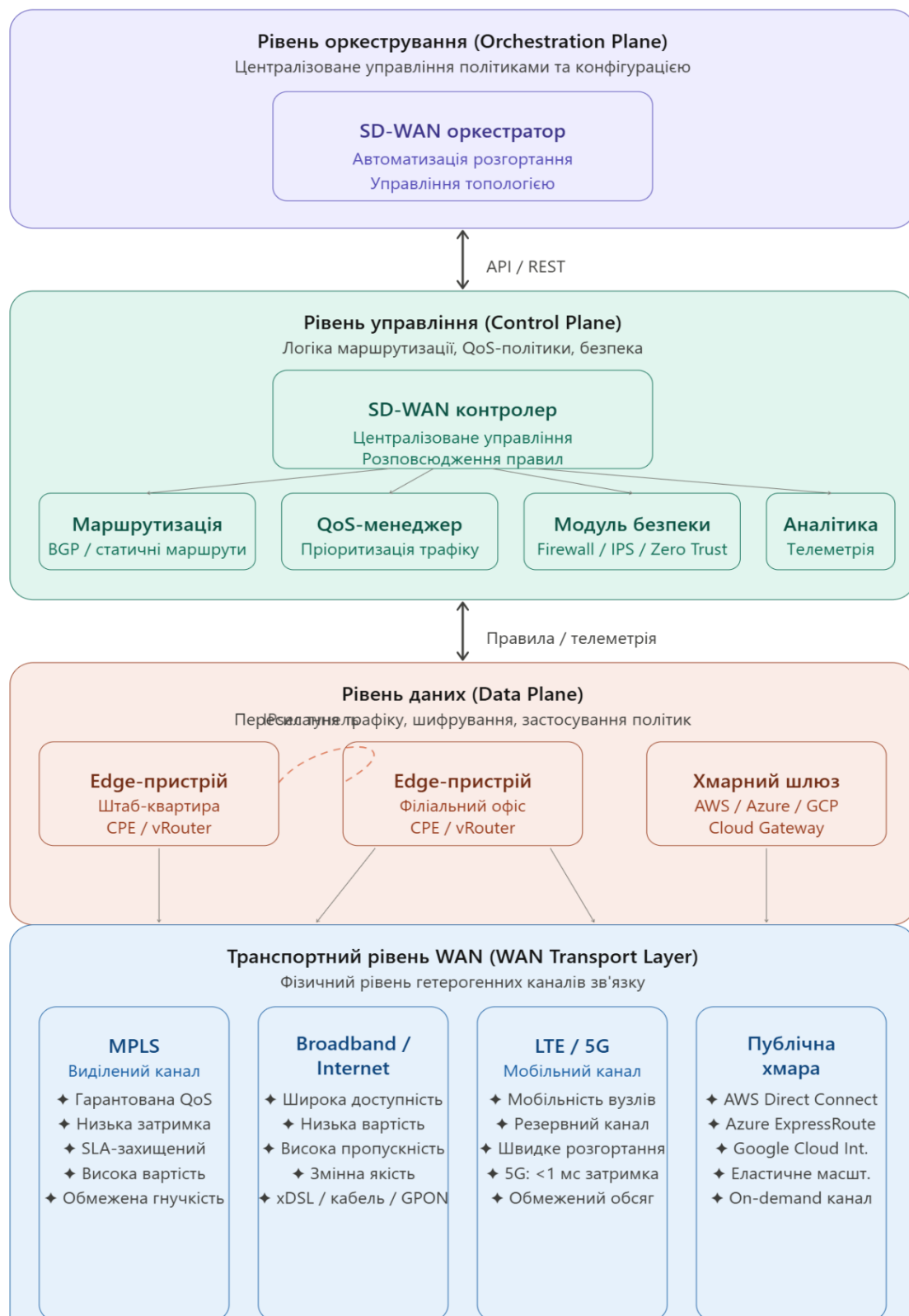


Рисунок 2.1. Структурна схема тривірневої ієрархічної мережі SD-WAN

Апаратно-програмні або повністю віртуалізовані граничні пристрої (*SD-WAN Edge*) розгортаються безпосередньо у вузлах мережі – у філіях підприємств,

центрах обробки даних та хмарних точках присутності. Кожен такий пристрій виконує функції класифікації трафіку, застосування QoS-політик, встановлення та підтримки захищених тунелів, а також збору локальної телеметрії.

Граничні пристрої взаємодіють із контролером через стандартизований південний інтерфейс (*Southbound API*), отримуючи директиви та звітуючи про поточний стан локальних ресурсів, зокрема завантаженість процесора, пам'яті та буферів черг.

Одним із ключових елементів SD-WAN є підтримка одночасного використання гетерогенних транспортних каналів між вузлами мережі. Для кожної пари вузлів може бути доступна довільна комбінація каналів різних типів: виділені лінії MPLS, широкосмугові Internet-канали, мобільні канали LTE та 5G тощо. Кожен транспортний канал характеризується власним набором параметрів якості обслуговування, що динамічно змінюються в часі: доступною пропускною здатністю, затримкою поширення сигналу, джитером та рівнем втрати пакетів. Саме наявність множини гетерогенних каналів між вузлами є принциповою відмінністю SD-WAN від класичних мережевих рішень і основним джерелом додаткових ступенів свободи для системи управління.

У загальному вигляді, математична модель мережі SD-WAN у просторі станів, представляє собою систему рівнянь у вигляді сукупності векторів стану та управління [1].

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) + \Gamma w(t), \\ y(t) = Cx(t) + Du(t) + v(t), \end{cases} \quad (2.1)$$

де $x(t)$ - вектор стану, $y(t)$ - вектор виходу, A - матриця динаміки системи, B - матриця управління, $u(t)$ - вектор управляючих впливів, Γ - матриця розподілу шуму процесу, $w(t)$ - вектор шуму процесу, C - матриця спостереження (виходу), D - матриця прямого зв'язку, $v(t)$ - шум вимірювань.

Розглянемо інформаційну мережу SD-WAN як систему, яка буде складатися з N вузлів, які зв'язані один з одним використовуючи M гетерогенних

каналів зв'язку таких видів, як LTE/5G, MPLS, Broadband. При цьому правління буде здійснюватися централізованим SD-WAN контролером, який збирає телеметрію та генерує управляючі рішення.

Позначимо:

$$G = (V, E), \quad (2.2)$$

де $E = \{e_1, e_2, \dots, e_m\}$ – множина ребер (зв'язків) комп'ютерної системи, $V = \{v_1, v_2, \dots, v_n\}$ – певна множина вузлів комп'ютерної системи.

Кожний канал e_k характеризується набором його характеристик. Такими характеристиками являються максимальна пропускна здатність поточне завантаження $l_k(t)$, C_k , затримка $d_k(t)$, а також рівень втрати пакетів $p_k(t)$.

2.2.2. Визначення вектору стану моделі у просторі станів

Центральним елементом будь-якої моделі у просторі станів є вектор стану, який у стислій формі описує повну інформацію про поточне становище системи, достатню для прийняття оптимального управляючого рішення. Для мережі SD-WAN вектор стану має охоплювати всі параметри, що визначають якість обслуговування трафіку та здатність системи дотримуватися встановлених SLA-вимог у кожний момент часу [1].

При виборі компонентів вектора стану керуються двома основними принципами: повноти та спостережуваності. Принцип повноти вимагає, щоб обраний набір змінних стану був достатнім для однозначного опису динаміки системи та прийняття оптимальних управляючих рішень без залучення додаткової зовнішньої інформації. Принцип спостережуваності передбачає, що всі компоненти вектора стану можуть бути виміряні або оцінені в реальному часі за допомогою наявних засобів телеметрії граничних пристроїв. Відповідно до цих принципів, вектор стану мережі SD-WAN формується з чотирьох

функціонально відособлених підвекторів, кожен з яких відображає окремий функціонал мережевої інфраструктури.

Вектор стану комп'ютерної системи $x(t) \in \mathbb{R}^n$ знаходиться в просторі n змінних та у кожен дискретний момент t буде формуватися з таких елементів [1]

$$x(t) = [xL(t)^T, xD(t)^T, xP(t)^T, xB(t)^T]^T \in \mathbb{R}^n, \quad (2.3)$$

де $xD(t) = [d_1(t), d_2(t), \dots, d_m(t)]^T$ – вектор затримок в каналах комп'ютерної системи, $xL(t) = [l_1(t), l_2(t), \dots, l_m(t)]^T$ – вектор навантаження каналів комп'ютерної системи, $l_k(t) = L_k(t)/C_k \in [0,1]$; $xB(t) = [b_1(t), b_2(t), \dots, b_n(t)]^T$ – вектор стану у буферів вузлів комп'ютерної системи, $xP(t) = [p_1(t), p_2(t), \dots, p_m(t)]^T$ – вектор ймовірностей втрати пакетів в каналі.

Ступінь наповненості буферів черг на кожному граничному пристрої системи описує четвертий підвектор. Стан буферів є інтегральним показником, що відображає баланс між інтенсивністю вхідного трафіку та продуктивністю вихідних каналів вузла. Накопичення черг у буферах безпосередньо призводить до зростання затримки та збільшення джитеру, що, у свою чергу, порушує вимоги SLA для чутливого до затримок трафіку. Включення цього підвектора до простору станів забезпечує можливість превентивного управління: система може здійснювати перерозподіл трафіку ще на етапі формування черг, не очікуючи на їх переповнення та відповідне зростання втрат пакетів.

Сукупність чотирьох описаних підвекторів формує повний вектор стану системи, розмірність якого визначається кількістю транспортних каналів та кількістю вузлів мережі. Три підвектори – завантаження, затримок та ймовірностей втрати – мають розмірність, рівну кількості транспортних каналів, тоді як підвектор стану буферів має розмірність, рівну кількості вузлів мережі. Таким чином, повна розмірність простору станів лінійно зростає зі збільшенням масштабу мережі, що є важливою властивістю для оцінки обчислювальної складності алгоритмів управління.

Вектор стану є функцією дискретного часу, тобто оновлюється із заданою періодичністю відповідно до циклу збору телеметрії. Це відповідає реальній практиці функціонування SD-WAN-контролерів, які використовують метрики від граничних пристроїв з визначеними інтервалами опитування. Дискретний характер вектору стану обумовлює вибір дискретно-часових методів управління та відповідних алгоритмів машинного навчання, що розглядаються у наступних підрозділах.

2.2.3. Визначення вектору простору управляючих впливів

Кожна компонента вектору управляючих впливів відповідає частці трафіку певного класу сервісу, що спрямовується через конкретний транспортний канал у поточний дискретний момент часу. Частка трафіку є нормованою дійсною величиною в діапазоні від нуля до одиниці, де нульове значення означає повне виключення відповідного каналу з обслуговування даного класу трафіку, а одиничне – концентрацію всього трафіку цього класу на одному каналі. Проміжні значення відповідають режиму розщеплення трафіку між кількома каналами одночасно, що є однією з ключових можливостей технології SD-WAN та дозволяє ефективно балансувати навантаження й підвищувати відмовостійкість [1].

Принципово важливою властивістю простору управляючих впливів є нормувальне обмеження: сума часток трафіку кожного класу сервісу по всіх доступних каналах у будь-який момент часу має дорівнювати одиниці. Це обмеження є фізично обґрунтованим – весь трафік кожного класу повинен бути розподілений між наявними каналами без накопичення та втрат. Зазначене обмеження формує симплексну структуру простору допустимих управлінь, що є нетривіальним з точки зору оптимізації та потребує спеціального врахування при проектуванні алгоритмів навчання. Зокрема, не всі стандартні методи навчання з підкріпленням безпосередньо підтримують симплексні обмеження на дії агента, що є однією з методологічних проблем, які розв'язуються у даній роботі.

Суттєвою особливістю запропонованої моделі є те, що вектор управляючих впливів визначається окремо для кожного класу сервісу. Це відображає реальну практику функціонування SD-WAN, де різні класи трафіку мають принципово різні вимоги до параметрів якості обслуговування і, відповідно, потребують різних стратегій вибору каналу. Так, голосовий трафік вимагає передусім мінімізації затримки та джитеру і повинен спрямовуватися на канали з найкращими часовими характеристиками навіть за рахунок вищої вартості. Трафік резервного копіювання, навпаки, невибагливий до затримки, однак потребує максимальної пропускної здатності за мінімальної вартості передачі. Роздільне управління класами трафіку дозволяє системі реалізувати диференційовані стратегії для кожного класу, не жертвуючи якістю обслуговування одних застосунків на користь інших.

Вектор $u(t) \in \mathbb{R}^m$ являється вектором управляючих впливів в просторі m та показує розподіл трафіку між всіма каналами комп'ютерної системи [1]:

$$u(t) = [u_1(t), u_2(t), \dots, u_m(t)]^T, \quad (2.4)$$

де $u_k(t) \in [0, 1]$ – представляє собою частину трафіку сервісу s , який надається через канал e_k у час t . Для цього випадку повинні виконуватися такі обмеження

$$\sum_k u_k^s(t) = 1, \quad \forall s \in S, \quad \forall t, \quad (2.5)$$

де S – уся множина класів певного сервісу. Також, коли необхідно, вектор управління може мати у своєму складі і інші параметри комп'ютерної системи. Це можуть бути пріоритезація черг або формування трафіку.

2.3. Розробка узагальненої моделі комп'ютерної системи SD-WAN апаратом простору станів

Після визначення вектору стану та вектору управляючих впливів наступним кроком є знаходження рівняння, що описує динаміку переходів між станами системи. Саме це рівняння є серцевиною моделі у просторі станів і визначає, яким чином поточний стан мережі та прийняте управляюче рішення формують стан системи у наступний момент часу.

2.3.1. Модель динаміки переходів між станами системи

Динаміка реальної мережі SD-WAN є принципово нелінійною. Ця нелінійність має кілька джерел. По-перше, залежність затримки від завантаження каналу є нелінійною і описується кривими, характерними для систем масового обслуговування: за низького завантаження затримка майже не змінюється, однак поблизу точки насичення різко зростає (рис. 2.2). По-друге, ймовірність втрати пакетів також нелінійно залежить від рівня заповненості буферів і стрибкоподібно збільшується при їх переповненні. По-третє, взаємодія між класами трафіку за спільних ресурсів каналу та буферів вузлів породжує складні перехресні залежності, що не піддаються лінійному опису. Крім того, система піддається зовнішнім збуренням у вигляді непередбачуваних змін інтенсивності вхідного трафіку та раптових відмов каналів зв'язку, що додатково ускладнює аналіз динаміки [1].

Збурення є невід'ємною складовою моделі динаміки мережі і відображають ту частину змін стану системи, яка не залежить від управляючих впливів контролера. З практичної точки зору збурення охоплюють два принципово різні явища. Перше – це флуктуації вхідного трафіку, зумовлені природною нерівномірністю активності користувачів та застосунків: денні піки навантаження, пакетний характер трафіку окремих застосунків, непередбачувані сплески активності. Друге – раптові деградації або повні відмови транспортних

каналів, спричинені фізичними пошкодженнями ліній зв'язку, перевантаженням у проміжних вузлах провайдера або несправностями обладнання. Явне включення вектора збурень до рівняння стану дозволяє коректно розмежувати керовану та некеровану складові динаміки системи, що є необхідною умовою для синтезу робастних алгоритмів управління [1].

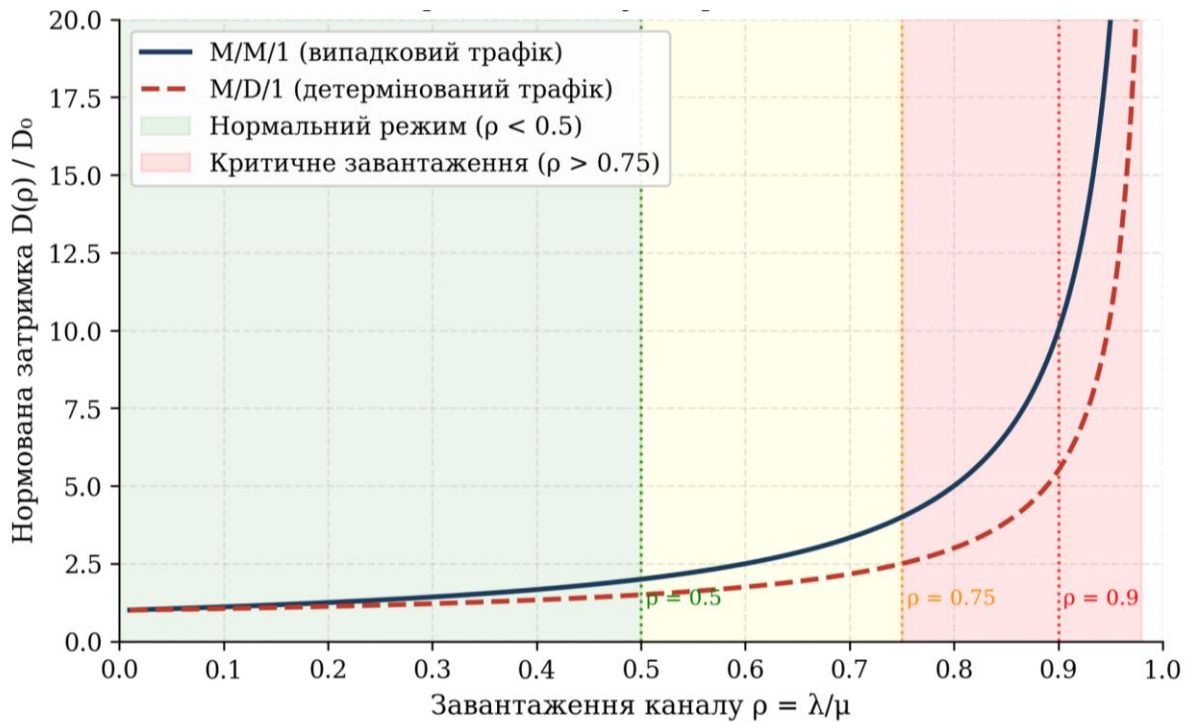


Рисунок 2.2. Залежність затримки пакетів від завантаження каналу

Динаміку мережі SD-WAN у дискретному часі опишемо нелінійним рівнянням стану:

$$x(t + 1) = f(x(t), u(t), w(t)), \quad (2.6)$$

де $w(t)$ – являється вектором впливів. Це фактори комп'ютерної системи, на які сам контролер не може впливати. Проте вони можуть впливати на поточний стан системи. Наприклад це можуть бути DDoS-атака, раптовий сплеск трафіку, обрив каналу. Розглянемо робочу точку (x^*, u^*) [1]

$$\Delta x(t+1) = \mathbf{A}\Delta x(t) + \mathbf{B}\Delta u(t) + \mathbf{\Gamma}w(t), \quad (2.7)$$

$$y(t) = \mathbf{C}\Delta x(t) + \mathbf{D}\Delta u(t) + v(t), \quad (2.8)$$

де $v(t)$ – шум вимірювань, $\mathbf{A} \in \mathbb{R}^{n \times n}$ – матриця, яка характеризує внутрішню динаміку комп'ютерної системи, $\Delta x(t) = x(t) - x^*$, $\Delta u(t) = u(t) - u^*$ – відхилення від місця лінеаризації, $\mathbf{B} \in \mathbb{R}^{n \times m}$ – матриця, яка характеризує управління, $\mathbf{C} \in \mathbb{R}^{l \times n}$ – матриця, яка показує, які стани ми можемо зараз спостерігати, $\mathbf{\Gamma} \in \mathbb{R}^{n \times p}$ – матриця впливів, $\mathbf{D} \in \mathbb{R}^{l \times m}$ – матриця прямого зв'язку.

Нелінійну модель комп'ютерної системи SD-WAN (2.6) можна представити компонентними рівняннями, що залежать від її архітектури.

Побудована узагальнена модель у просторі станів є не самоціллю, а інструментом для вирішення основного завдання – синтезу оптимального алгоритму управління. З одного боку, лінеаризована модель дозволяє провести теоретичний аналіз властивостей системи та отримати аналітичні гарантії стійкості.

З іншого боку, нелінійне рівняння стану слугує середовищем для навчання агента на основі глибокого навчання з підкріпленням, де агент безпосередньо взаємодіє з симульованою динамікою мережі, не потребуючи явного знання її математичної структури. Таке поєднання аналітичного та навчального підходів є методологічною основою даного дослідження і відображає сучасну тенденцію до гібридизації класичної теорії управління та методів машинного навчання. На рис. 2.3 представлено залежність оцінки винагороди та ентропії при навчанні агента на основі глибокого навчання з підкріпленням.

Динаміка завантаження каналу e_k може бути описана рівнянням черги M/G/1 [1]:

$$l_k(t+1) = l_k(t) + \Delta t / C_k [\sum_i \lambda_{ik}(t) u_{ik}(t) - \mu_k(t) l_k(t)] + w_k^l(t), \quad (2.9)$$

де $\lambda_{ik}(t)$ – це інтенсивність трафіку на вході з вузла i , який проходить через канал k ; Δt – крок дискретизації, $\mu_k(t)$ – швидкість обслуговування каналу.

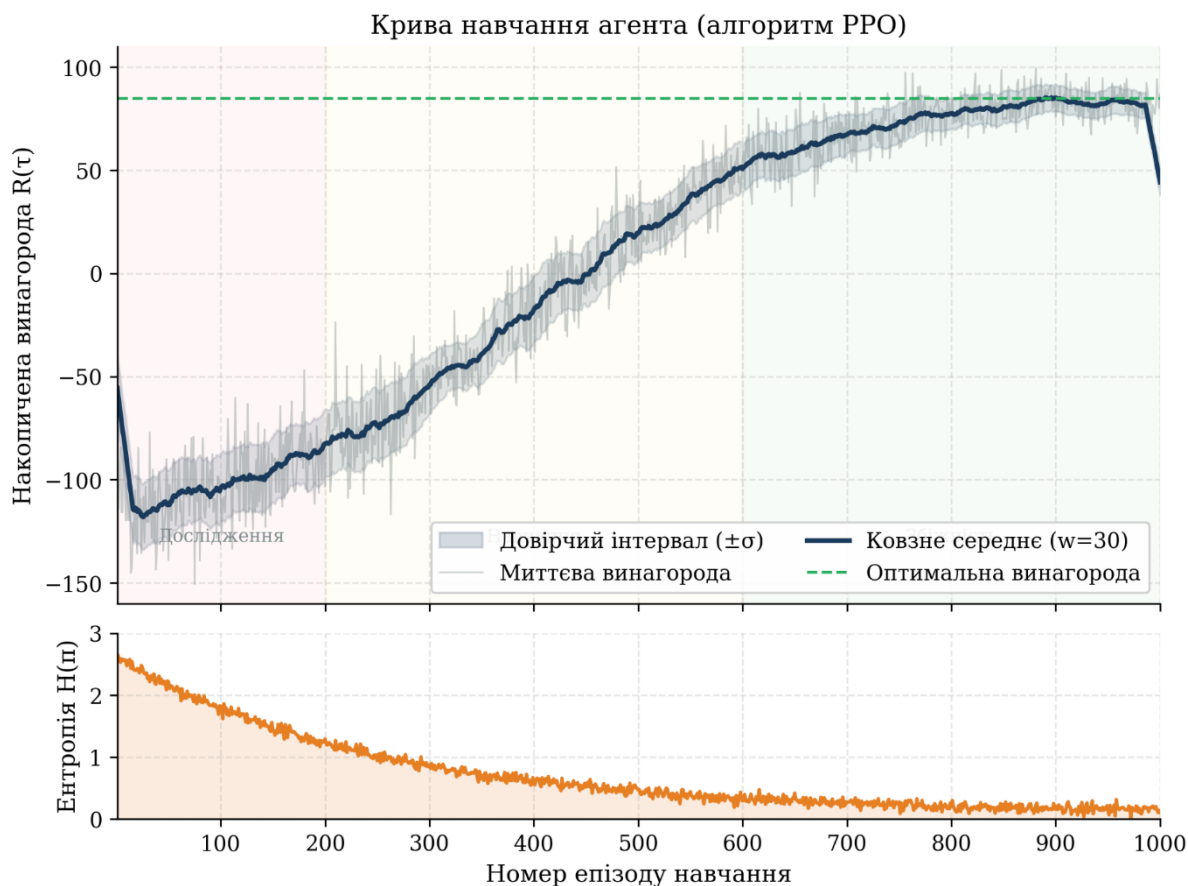


Рисунок 2.3. Оцінки винагороди та ентропії при навчанні агента на основі глибокого навчання з підкріпленням

Побудуємо модель затримки каналу. Затримка каналу складається з таких компонентів: передача, поширення, очікування в черзі. По моделі M/M/1:

$$d_k(t) = d_k^{\text{prop}} + L_{\text{pkt}}/C_k + l_k(t)/(\mu_k(1 - \rho_k(t))), \quad (2.10)$$

де L_{pkt} – середня тривалість пакету; d_k^{prop} – постійна величина затримки поширення; $\rho_k(t) = l_k(t)$ – коефіцієнт навантаження каналу.

На основі формули Ерланга-В знайдемо імовірність втрати пакетів для кінцевого буфера з розміром B_k . В цьому випадку модель втрати пакетів буде виглядати наступним чином [1]

$$p_k(t) = (\rho_k(t)^{B_k}/B_k!)/\sum_{j=0}^{B_k}(\rho_k(t)^j/j!). \quad (2.11)$$

Залежність ймовірності втрати пакетів від наповненості буфера представлена на рис. 2.4.

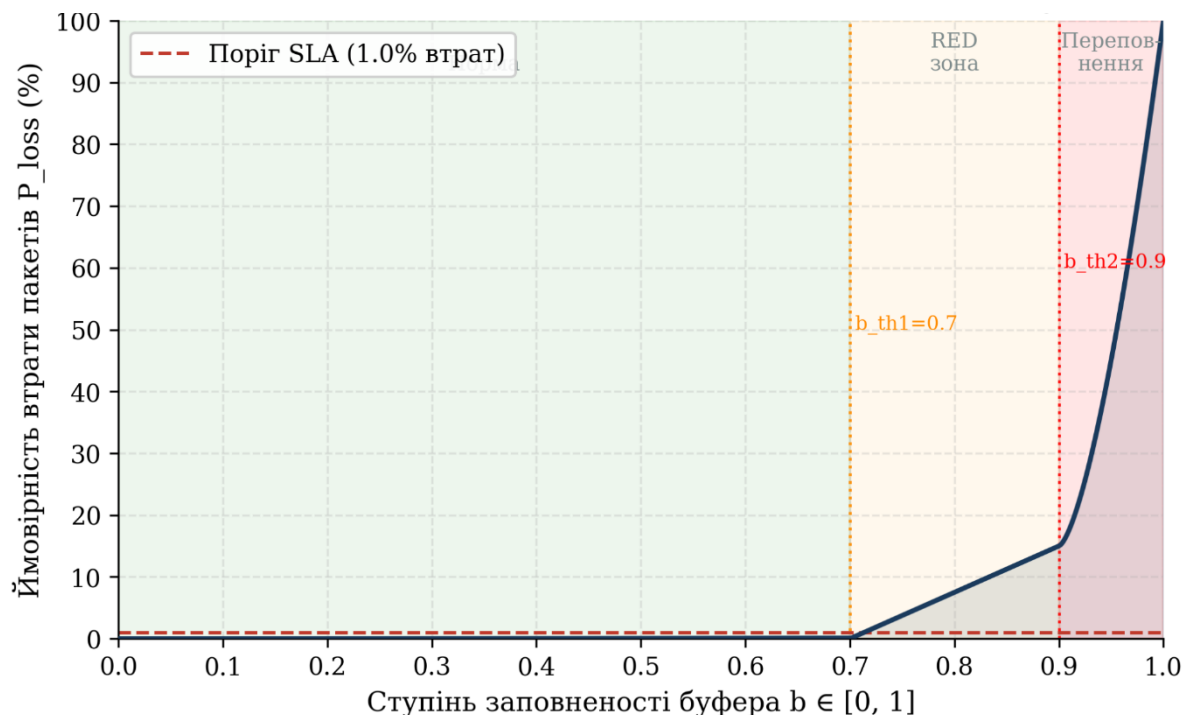


Рисунок 2.4. Ймовірність втрати пакетів від наповненості буфера

2.3.2. Визначення матриць стану та управління

Побудуємо матрицю стану A та матрицю управління B . Матриця стану є математичним відображенням усіх причинно-наслідкових зв'язків між компонентами вектору стану мережі. Кожен її елемент характеризує, наскільки зміна однієї компоненти стану у поточний момент часу позначається на іншій компоненті у наступний момент. Таким чином, матриця стану кодує в собі всю внутрішню динаміку мережі SD-WAN, включаючи як прямі ефекти самовпливу кожної змінної, так і перехресні взаємодії між різними аспектами стану системи. Отримати її аналітично в загальному вигляді неможливо через нелінійність вихідної моделі, тому вона визначається як матриця часткових похідних функції переходу станів, обчислених у вибраній точці лінеаризації, що відповідає номінальному режиму роботи мережі.

Принципово важливою властивістю матриці стану для мережі SD-WAN є її блочна структура, що безпосередньо відображає фізичну природу взаємозв'язків між різними групами змінних стану. Блочне представлення не лише спрощує аналітичне дослідження системи, а й надає кожному блоку конкретний фізичний зміст, що полегшує інтерпретацію результатів.

Розглянемо матрицю A . Її елементи будуть визначатися частковими похідними для компонент функції f , яка являється вектору стану x саме у точці лінеаризації [1]:

$$A_{ij} = \partial f_i(x, u) / \partial x_j |_{(x^*, u^*)}. \quad (2.12)$$

Матриця A має блочну структуру

$$A = [ALL \ ALD \ ALP \ ALB; ADL \ ADD \ 0 \ 0; APL \ 0 \ APP \ 0; ABL \ 0 \ 0 \ ABB]. \quad (2.13)$$

Тут блоки, це взаємовпливи компонентів для вектору стану комп'ютерної системи.

Так, $ALD = \partial l_k / \partial d_j$ це впливи для затримки при завантаженні.

$ALL = I - \Delta t \cdot diag\{\mu_k\}$ описують самозатухання завантаження каналів.

Матриця управління B , буде мати такий вигляд

$$B = [\Delta t / C_k \cdot diag\{\lambda_{ik}\}; \partial d / \partial u; \partial p / \partial u; 0]. \quad (2.14)$$

Матриця управління описує ефективність впливу управляючих дій контролера на кожну компоненту вектору стану. Її структура є стовпчастою у відповідності до блоків вектору стану. Блок впливу управління на завантаження каналів є найбільш безпосереднім: перерозподіл часток трафіку між каналами прямо і швидко змінює рівень їх завантаження. Швидкість цього впливу визначається часовим кроком дискретизації та пропускними здатностями відповідних каналів. Блок впливу управління на затримку відображає опосередкований характер цього зв'язку: зміна розподілу трафіку впливає на

затримку не безпосередньо, а через зміну завантаження каналу, яка, у свою чергу, змінює час очікування у черзі. Блок впливу управління на ймовірність втрат аналогічно має опосередкований характер. Нульовий блок для стану буферів вузлів означає, що управляючі впливи не впливають безпосередньо на буфери у рамках лінеаризованої моделі – вплив здійснюється виключно через зміну завантаження каналів.

Таким чином, отримано узагальнену математичну модель SD-WAN у просторі станів (2.2) - (2.14). Ця модель залежить від динаміки завантаження каналів, втрати пакетів, затримки та стану буферів вузлів. На основі цієї моделі можна розглядати лінеаризований її варіант для аналітичних розрахунків. Також її повна нелінійна форма може бути використана для проведення симуляції комп'ютерної мережі з управлінням SD-WAN.

Розглянемо умови стійкості система управління. Поняття стійкості є центральним у теорії автоматичного управління і набуває конкретного фізичного змісту стосовно мережі SD-WAN. Стійка система управління – це така система, в якій будь-яке відхилення стану мережі від рівноважного режиму (спричинене, наприклад, короткочасним сплеском трафіку або тимчасовою деградацією каналу) з часом загасає і система повертається до цільового стану. Нестійка система, навпаки, схильна до неконтрольованого наростання відхилень: невелике початкове збурення може призвести до лавиноподібного зростання черг, каскадного перевантаження каналів та повної деградації якості обслуговування. Таким чином, забезпечення стійкості є необхідною, хоча й недостатньою умовою ефективного управління мережею.

Оскільки модель мережі SD-WAN побудована у дискретному часі, критерій стійкості відрізняється від аналогічного критерію для систем із неперервним часом. Для дискретних систем умовою асимптотичної стійкості є розташування всіх власних значень матриці замкненої системи всередині одиничного кола на комплексній площині. Геометрично це означає, що модулі всіх власних значень мають бути строго меншими за одиницю. Власні значення поза одиничним колом відповідають модам системи, що наростають у часі;

власні значення на межі одиничного кола – незагасаючим коливанням; лише власні значення всередині кола гарантують загасання відхилень. Чим далі власні значення від межі одиничного кола, тим швидше система повертається до рівноважного стану після збурення.

Система, яка описується (2.7)–(2.8) являється асимптотично стійкою, коли всі числа матриці $A_{\text{зам}}$ замкненої системи будуть знаходитися всередині кола розмірністю одиниця, що знаходиться на комплексній площині [1]:

$$|\lambda_i(A_{\text{зам}})| < 1, \forall i = 1, \dots, n. \quad (2.15)$$

У випадку зворотнього зв'язку $u(t) = -Kx(t)$ можемо знайти $A_{\text{зам}} = A - BK$. В комп'ютерній системі матриця K буде визначатися використовуючи технології машинного навчання або оптимального управління.

Перш ніж синтезувати регулятор, необхідно переконатися у принциповій можливості управляти системою – тобто перевірити умову керованості. Система є повністю керованою, якщо за допомогою наявних управляючих впливів можна перевести її з будь-якого початкового стану у будь-який цільовий стан за скінченний час. Математично ця умова перевіряється через ранг матриці керованості, що будується з матриць стану та управління. Повний ранг матриці керованості означає, що жодна мода системи не є прихованою від управляючого впливу. У контексті SD-WAN порушення умови керованості означало б існування певних аспектів стану мережі, на які контролер принципово не здатний впливати за допомогою перерозподілу трафіку. Виявлення таких некерованих мод є важливим результатом аналізу, що може вказувати на необхідність розширення простору управляючих впливів або зміни топології мережі.

Проведемо перевірку умов керованості даної системи. Необхідно визначити матрицю керованості, а саме [1]

$$\text{rank}(C) = \text{rank}[B \mid AB \mid A^2B \mid \dots \mid A^{n-1}B] = n. \quad (2.16)$$

Побудуємо матрицю спостережуваності для можливості проведення перевірки спостережуваності системи

$$\text{rank}(\mathcal{O}) = \text{rank}[\mathbf{C}^T | \mathbf{A}^T \mathbf{C}^T | (\mathbf{A}^T)^2 \mathbf{C}^T | \dots | (\mathbf{A}^T)^{n-1} \mathbf{C}^T] = n. \quad (2.17)$$

Ґрунтуючись на вищезначених викладках отримаємо функціонал якості управління. Цільовий функціонал якості управління SD-WAN буде визначатися у вигляді зваженої сума всіх відхилень показників від їх цільових значень:

$$J = \sum_{t=0}^T [x^T(t) \mathbf{Q} x(t) + u^T(t) \mathbf{R} u(t)] + x^T(T) \mathbf{P} x(T), \quad (2.18)$$

де \mathbf{P} – матриця визначення кінцевого штрафу, $\mathbf{R} \in \mathbb{R}^{m \times m}$ – матриця вартості управлінь, яка є позитивно визначеною, $\mathbf{Q} \in \mathbb{R}^{n \times n}$ – вагова матриця стану, яка є невід'ємно визначеною.

За певних умов, матриця \mathbf{Q} може бути представлена як блочна структура [1]:

$$\mathbf{Q} = \text{diag}\{q_L \cdot \mathbf{I}_M, q_D \cdot \mathbf{I}_M, q_P \cdot \mathbf{I}_M, q_B \cdot \mathbf{I}_N\}, \quad (2.19)$$

де q_L, q_D, q_P, q_B – представляють собою вагові коефіцієнти (завантаження, затримки, втрати пакетів та заповненості буферів). Визначення ваги кожної складової відповідає вимогам стандарту обслуговування Service Level Agreement для різних класів трафіку.

Задача мінімізації (2.18) для лінійної моделі (2.7) вирішується застосуванням рівняння Річчати [1]:

$$\mathbf{P} = \mathbf{Q} + \mathbf{A}^T \mathbf{P} \mathbf{A} - \mathbf{A}^T \mathbf{P} \mathbf{B} (\mathbf{R} + \mathbf{B}^T \mathbf{P} \mathbf{B})^{-1} \mathbf{B}^T \mathbf{P} \mathbf{A}, \quad (2.20)$$

Для цього випадку визначимо оптимальну матрицю зворотного зв'язку:

$$K^* = (R + B^T P B)^{-1} B^T P A. \quad (2.21)$$

Для узагальненої математичної моделі мережі SD-WAN, побудованої у просторі станів, аналітично обґрунтовано та формально доведено необхідні умови асимптотичної стійкості (2.15) і структурної керованості (2.16) досліджуваної комп'ютерної системи. У частковому випадку лінеаризованої моделі задача оптимального управління розв'язана в аналітичній формі на підставі матричних рівнянь Річчати (2.20)–(2.21) [1].

Сформовано математичну модель інформаційної мережі SD-WAN із використанням апарату простору станів. Її наукова новизна полягає в описі системи через сукупність векторів стану, керування та функції якості обслуговування. Модель враховує зміну навантаження на канали зв'язку, затримки передавання даних, втрати пакетів і стан буферів мережевих вузлів, що дає змогу забезпечити стійкість і керованість системи.

Запропонований підхід може використовуватися як у лінеаризованому вигляді для виконання аналітичних обчислень, так і у повній нелінійній формі для проведення імітаційного моделювання.

2.4. Висновки до розділу 2

1. В розділі проведено аналіз сучасних досліджень системи управління комп'ютерної розподіленої мережі SD-WAN. На основі аналізу визначено необхідність розробки комплексної математичної моделі SD-WAN апаратом простору станів.

2. Розроблено математичну модель мережі SD-WAN у просторі станів (2.2)–(2.14), що описується сукупністю векторів стану, керування та функцією якості обслуговування. Модель враховує динамічні зміни завантаження каналів зв'язку, затримки передавання, втрати пакетів, а також стан буферів мережевих вузлів. Запропонований підхід може застосовуватися як у лінеаризованій формі

для виконання аналітичних досліджень, так і у повному нелінійному вигляді для імітаційного моделювання системи.

3. Також визначено умови стійкості (2.15) та керованості (2.16) комп'ютерної системи. Для лінійної моделі отримано аналітичний розв'язок задачі оптимального керування SD-WAN, який базується на використанні рівняння Ріккати (2.20) – (2.21).

РОЗДІЛ 3

МЕТОД УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ МЕРЕЖЕЮ SD-WAN НА ОСНОВІ МАШИННОГО НАВЧАННЯ

В попередньому розділі розроблено модель мережі SD-WAN апаратом просторі станів. Вона представляє собою кортеж функції якості обслуговування, вектору стану, вектору управління. Дана модель може враховувати стан буферів вузлів, динаміку завантаження каналів, втрати пакетів та затримки.

Формалізація задачі управління SD-WAN у просторі станів дозволяє застосувати апарат теорії автоматичного управління та методи оптимізації, зокрема методи машинного навчання ML. Останні роки відзначаються значним прогресом у застосуванні навчання з RL для управління комп'ютерними мережами [5], [47], [110].

Тому в розділі необхідно розробити метод оптимального управління інформаційної мережі з управлінням SD-WAN використовуючи її узагальнену математичну модель у просторі станів з застосуванням машинного навчання [69]. Для цього необхідно розробити алгоритм управління комп'ютерною системою використовуючи технологію глибокого навчання з підкріпленням.

У сфері машинного навчання для управління мережами слід відзначити роботи [45], [49], в яких Deep Q-Network застосовуються для управління QoS. Алгоритм Proximal Policy Optimization (PPO) [50] показав перевагу у задачах із неперервним простором дій. Однак більшість існуючих підходів розглядають лише окремі аспекти управління, не пропонуючи єдиної математичної моделі у просторі станів для SD-WAN.

Таким чином, існує необхідність розробки методу управління інформаційною мережею SD-WAN технологіями глибокого навчання з підкріпленням на основі математичної моделі SD-WAN у просторі станів.

Проте ефективне функціонування інформаційної мережі SD-WAN обмежується наявністю сучасних кібератак, які еволюціонували від ізольованих спроб злому до складних, багатоетапних і цілеспрямованих загроз APT.

Інформаційної мережі SD-WAN мають інструменти для динамічної зміни маршрутів, а також ізоляції будь-якого її елемента. Тому необхідно розробити інтелектуальну систему управління, яка здатна визначити яким чином можна застосувати такі інструменти для ефективної боротьби з кіберзагрозами.

Актуальним являється розробка методу побудови захищеної комп'ютерної мережі, що управляється SD-WAN на основі графу атак [70]. Необхідно розробити комплексний, крос-доменний метод управління мережевою безпекою каналів з застосуванням багатоагентного навчання з підкріпленням для розподіленого управління, де математична модель графу атак слугує формалізованим середовищем для RL-агента, а рішення цього агента безперервно транслуються в конфігураційні API-команди для центрального контролера SD-WAN щоб гарантувати мінімальний час реакції на інциденти.

Для цього необхідно дослідити та обґрунтувати застосування методів машинного навчання, зокрема алгоритмів навчання з підкріпленням RL, для подолання ключових обмежень статичних правил блокування. Розробити логіку функціонування інтелектуального агента, здатного в режимі реального часу генерувати оптимальні політики SD-WAN, знаходячи компроміс між максимізацією рівня кібербезпеки та мінімізацією деградації якості обслуговування QoS легітимного трафіку.

3.1 Метод оптимального управління SD-WAN на основі машинного навчання

3.1.1. Постановка завдання розробки методу управління SD-WAN на основі навчання з підкріпленням

Завдання оптимального управління мережею SD-WAN відрізняється рядом властивостей, що роблять її об'єктом для застосування методів навчання з підкріпленням RL. По-перше, динаміка мережі є стохастичною і нелінійною – стан каналів зв'язку, рівень завантаженості та якість обслуговування змінюються під впливом некерованих зовнішніх збурень, таких як флуктуації трафіку,

короткочасні відмови обладнання та зміни умов радіоканалу в сегментах LTE/5G. По-друге, простір станів є неперервним та високорозмірним, що унеможливорює побудову вичерпних таблиць управляючих рішень. По-третє, цільова функція управління є багатокритеріальною та зважає між собою суперечливі вимоги до мінімізації затримки, втрати пакетів та витрат на передачу трафіку [1], [4].

Зазначені властивості визначають доцільність формалізації завдання управління SD-WAN у рамках Марківського процесу прийняття рішень MDP. MDP можна визначити так:

$$\mathcal{M} = \langle \mathcal{S}, \mathcal{A}, \mathcal{P}, \mathcal{R}, \gamma \rangle, \quad (3.1)$$

де \mathcal{A} – це простір дій, який визначається $a(t) \equiv u(t) \in \mathbb{R}^m$ – управляючими впливами, \mathcal{S} – представляє собою простір станів, який визначається $s(t) \equiv x(t) \in \mathbb{R}^n$ – вектором стану комп'ютерної системи, $\mathcal{P}(s'|s, a)$ – умовна ймовірність переходу зі стану s до стану s' коли виконується дія a , $\mathcal{R}(s, a)$ – це функція миттєвої винагороди; $\gamma \in (0,1)$ – це коефіцієнт дисконтування, який знаходить відносну цінність майбутніх винагород в порівнянні з поточними [47].

Вектор стану $s(t) \equiv x(t) \in \mathbb{R}^n$ включає поточні значення ключових мережевих метрик: затримку, джиттер, рівень втрат пакетів, завантаженість каналів та розміри черг на граничних пристроях edge devices. Вектор дій $a(t) \equiv u(t) \in \mathbb{R}^m$ охоплює управляючі впливи SD-WAN контролера: перемикання трафіку між транспортними каналами, зміну QoS-профілів та перерозподіл смуги пропускання між класами обслуговування.

Ключовою перевагою формалізації у рамках MDP є те, що вона не потребує явного знання функції переходу \mathcal{P} – агент навчання з підкріпленням здатний створити оптимальну стратегію управління безпосередньо через взаємодію із середовищем (або його симулятором), що являється суттєвим при відсутності точної аналітичної моделі мережевої динаміки [5].

Функція винагороди є центральним елементом постановки завдання оптимального управління мережею SD-WAN, оскільки вона кодифікує цілі управління у числовій формі. У даній роботі на одному кроці визначається функція винагороди як від'ємне значення зваженого функціоналу якості [1]:

$$r(t) = -[\alpha L \|xL(t) - xL^*\|^2 + \alpha D \|xD(t) - xD^*\|^2 + \alpha P \|xP(t)\|^2 + \alpha u \|u(t)\|^2] \quad (3.2)$$

де xD^* – нормативні значення затримки каналів, xL^* – нормативні значення завантаженості каналів; $\alpha L, \alpha D, \alpha P, \alpha u$ – невід'ємні вагові коефіцієнти, що визначають пріоритетність кожного з критеріїв якості; $xP(t)$ – вектор компонент стану, пов'язаних із втратою пакетів; $\alpha u \|u(t)\|^2$ – доданок, який відіграє роль регуляризатора, що обмежує надмірно суттєві перемикання управляючих впливів, що можуть призводити до нестабільності мережі. Мета агента RL полягає у максимізації сумарної дисконтованої винагороди – так званого return:

$$G(t) = \sum_{k=0}^{\infty} \gamma^k r(t+k). \quad (3.3)$$

Коефіцієнт дисконтування γ забезпечує математичну збіжність нескінченної суми та водночас визначає «горизонт планування» агента. При $\gamma \rightarrow 0$ агент є «короткозорим» і оптимізує лише миттєву винагороду, при $\gamma \rightarrow 1$ – рівноцінно враховує всі майбутні винагороди. Для задач управління SD-WAN рекомендоване значення $\gamma \in [0,95; 0,99]$, що відповідає горизонту планування від 20 до 100 кроків управління [1], [48].

3.1.2. Розробка алгоритму для дискретного управління на основі методу глибокого навчання з підкріпленням для дискретного простору стану

Розглянемо випадок управління SD-WAN, коли доцільно дискретизувати простір станів, виділивши скінченну множину попередньо визначених профілів розподілу трафіку. Наприклад, $K = 8 \div 32$ профілів можуть кодувати різні

комбінації розподілу трафіку між MPLS, Broadband та LTE/5G каналами з різними пріоритетами класів QoS. У цьому випадку природно застосувати алгоритм Deep Q-Network – фундаментальний метод глибокого навчання з підкріпленням для дискретних просторів станів [1], [8].

Ключовою концепцією DQN є апроксимація оптимальної Q -функції цінності стану нейронною мережею з параметрами θ [1]:

$$Q(s, a; \theta) \approx Q^*(s, a), \quad (3.4)$$

де $Q^*(s, a)$ – оптимальна Q -функція, що визначає максимально досяжну сумарну дисконтовану винагороду, якщо в стані s виконати дію a , а надалі дотримуватись оптимальної стратегії. Нейронна мережа приймає вектор стану s як вхід і повертає вектор Q -значень для всіх K можливих дій одночасно, що забезпечує обчислювальну ефективність.

Параметри нейронної мережі θ оновлюються мінімізацією функції втрат Беллмана, що вимірює відхилення поточних оцінок Q від цільових значень [1]:

$$L(\theta) = \mathbb{E} \left[(y - Q(s, a; \theta))^2 \right], \quad (3.5)$$

$$y = r + \gamma \max_{a'} Q(s', a'; \theta^-), \quad (3.6)$$

де θ^- – параметри цільової мережі, яка є «замороженою» копією основної мережі та оновлюється кожні τ кроків навчання. Застосування цільової мережі є ключовим стабілізуючим механізмом DQN, що усуває «рухому мішень» при обчисленні цільових значень y і запобігає розбіжності навчання [8].

Гradient функції втрат за параметрами нейронної мережі обчислюється методом зворотного поширення помилки:

$$\nabla_{\theta} L(\theta) = -2(y - Q(s, a; \theta)) \cdot \nabla_{\theta} Q(s, a; \theta). \quad (3.7)$$

Другим ключовим компонентом DQN є буфер досвіду (Experience Replay Buffer):

$$\mathcal{D} = \{(s_i, a_i, r_i, s_i')\}. \quad (3.8)$$

Буфер накопичує переходи – кортежі (стан, дія, винагорода, наступний стан) – розміром $|\mathcal{D}|$ (типово від 10^4 до 10^6 переходів). На кожному кроці навчання з буфера випадково вибирається мінібатч розміром B (зазвичай $B=32 \div 256$), на якому обчислюється градієнт функції втрат. Рандомізована вибірка порушує часову кореляцію між послідовними переходами, що є необхідною умовою для коректного застосування стохастичного градієнтного спуску [1], [49].

Алгоритм навчання DQN-агента для управління SD-WAN включає такі етапи. На кожному кроці взаємодії з мережею агент з ε -жадібною стратегією вибирає або випадкову дію (з ймовірністю ε , що забезпечує дослідження), або дію з максимальним Q -значенням (з ймовірністю $1 - \varepsilon$, що реалізує поточну стратегію). Отриманий перехід зберігається у буфері. Якщо буфер містить достатньо записів, виконується крок оновлення параметрів мережі. Параметр ε поступово зменшується впродовж навчання відповідно до заздалегідь визначеного розкладу, зміщуючи баланс між дослідженням та використанням набутих знань.

Архітектура нейронної мережі DQN для задачі управління SD-WAN є повнозв'язною мережею прямого поширення з трьома-п'ятьма прихованими шарами та функцією активації ReLU. Розмірність вхідного шару відповідає розмірності вектора стану n , а вихідного – кількості дискретних дій K . Застосування нормалізації шарів перед кожним прихованим шаром суттєво прискорює збіжність навчання в умовах нестационарного середовища SD-WAN [45].

3.1.3. Розробка алгоритму для неперервного управління на основі методу глибокого навчання з підкріпленням для неперервного простору стану

Дискретизація простору стану, яка необхідна для застосування DQN, є певним спрощенням реальної задачі – вона може призводити до субоптимального управління в ситуаціях, де оптимальний розподіл трафіку не збігається з жодним із попередньо визначених K профілів. Для безпосередньої оптимізації неперервних управляючих впливів – вектора $u(t) \in \mathbb{R}^m$ – доцільно застосовувати алгоритм Proximal Policy Optimization (PPO), що є одним із найбільш практично ефективних методів навчання з підкріпленням для неперервних просторів дій [1], [50].

PPO представляє широкий клас policy gradient методів, у яких стратегія управління апроксимується параметричною стохастичною функцією виду $\pi_\theta(a|s)$. Для задачі управління SD-WAN стратегія моделюється гауссівським розподілом [1]:

$$\pi_\theta(a|s) = \mathcal{N}(\mu_\theta(s), \Sigma_\theta(s)) \quad (3.9)$$

де $\Sigma_\theta(s)$ – коваріаційна матриця, $\mu_\theta(s)$ – вектор середніх значень управляючих впливів. Обидві функції являються виходами actor-нейромережі з параметрами θ . Стохастичність стратегії забезпечує природне дослідження простору дій: на кожному кроці управляючий вплив семплюється з поточного розподілу, що дозволяє агенту виявляти нові, потенційно кращі режими управління.

Ключовою особливістю PPO є механізм обмеження на величину оновлення стратегії, що запобігає надмірно великим змінам π_θ за один крок градієнтного спуску. Це усуває проблему «катастрофічних» оновлень, характерну для ранніх policy gradient методів. Цільова функція PPO з відсічкою (clipping) [1]:

$$L^{CLIP}(\theta) = \mathbb{E}_t[\min(r_t(\theta) \cdot A_t, \text{clip}(r_t(\theta), 1 - \varepsilon, 1 + \varepsilon) \cdot A_t)] \quad (3.10)$$

де $r_t(\theta) = \pi_\theta(a_t|s_t) / \pi_{\theta_{ola}}(a_t|s_t)$ – відношення ймовірностей нової та старої стратегії (probability ratio); A_t – оцінка функції переваги (advantage function), що вимірює відносну якість виконаної дії порівняно з середнім; ε – гіперпараметр, що задає допустимий діапазон зміни відношення ймовірностей (типово $\varepsilon = 0,1 \div 0,2$). Операція *clip* обрізає відношення в межах $[1 - \varepsilon, 1 + \varepsilon]$, завдяки чому навіть при великому градієнті стратегія не може змінитись надто різко.

Функція переваги A_t оцінюється методом Generalized Advantage Estimation, що балансує між величиною зміщення та величиною дисперсії оцінки [1]:

$$A_t^{GAE}(\lambda) = \sum_{k=0}^{\infty} (\gamma\lambda)^k \delta_{t+k}, \quad (3.11)$$

$$\delta_t = r_t + \gamma V(s_{t+1}) - V(s_t), \quad (3.12)$$

де δ_t – TD-помилка Temporal Difference error, $V(s)$ – це функція цінності стану, що може апроксимуватися окремою critic-нейромережею з параметрами ϕ , $\lambda \in [0,1]$ – гіперпараметр GAE. При $\lambda = 0$ GAE зводиться до одноетапної TD-оцінки (низька дисперсія, але зміщення), при $\lambda = 1$ – до Monte Carlo оцінки (незміщена, але висока дисперсія). Оптимальне значення $\lambda = 0.95$ забезпечує ефективний компроміс для задач управління мережами [51].

Critic-нейромережа оновлюється мінімізацією середньоквадратичної помилки між поточними оцінками цінності та цільовими значеннями [1]:

$$L^{VF}(\phi) = \mathbb{E}_t \left[(V_\phi(s_t) - V_t^{target})^2 \right] \quad (3.13)$$

де цільове значення V_t^{target} обчислюється як накопичена дисконтована винагорода від поточного стану до кінця траєкторії або з використанням багатокрокових TD-оцінок. Спільна функція втрат для одночасного оновлення actor та critic включає також ентропійний регулятор, що стимулює дослідження:

$$L(\theta, \phi) = -L^{CLIP}(\theta) + c_1 L^{VF}(\phi) - c_2 H[\pi\theta] \quad (3.14)$$

де $H[\pi\theta]$ – ентропія стратегії; c_1, c_2 – вагові коефіцієнти (зазвичай $c_1 = 0,5, c_2 = 0,01$). Мінімізація L^{VF} покращує якість оцінки цінності, тоді як максимізація ентропії утримує стратегію від передчасної збіжності до детермінованого субоптимального рішення.

Таким чином, розроблено метод управління комп'ютерною мережею SD-WAN у просторі станів, наукова новизна якої полягає у тому, що вона ґрунтується на основі глибокого навчання з підкріпленням та дозволяє зменшити затримки та рівень втрат пакетів, а також підвищити значення функціоналу якості.

3.2. Метод забезпечення захисту комп'ютерної SD-WAN мережі на основі графу атак

3.2.1. Аналіз систем забезпечення захисту комп'ютерної SD-WAN мережі на основі графу атак

Стрімкий розвиток інформаційних технологій, повсюдне впровадження хмарних обчислень та перехід до мікросервісної архітектури докорінно змінили застосування технологій кібербезпеки. Сьогодні корпоративні мережі втратили чітко визначений периметр, що робить традиційні засоби захисту, такі як міжмережеві екрани Firewall або системи виявлення вторгнень IDS/IPS, недостатньо ефективними [79], [93]. Зловмисники, отримавши первинний доступ через найслабшу ланку (наприклад, фішинг або невідому вразливість на периферійному пристрої), можуть тижнями непомітно переміщуватися всередині інфраструктури, ескалюючи привілеї та шукаючи шляхи до критично важливих активів, таких як бази даних чи сервери управління. У таких умовах статичний, реактивний підхід до безпеки, який передбачає блокування загрози лише за фактом її виявлення на конкретному вузлі, є заздалегідь програшним.

З іншого боку, еволюція мережевих технологій призвела до широкого розгортання програмно-конфігурованих глобальних мереж SD-WAN. Технологія SD-WAN призвела до революційних змін в управлінні топологією завдяки архітектурному відокремленню площини управління Control Plane від площини передачі даних Data Plane. Вона дозволяє адміністраторам централізовано керувати маршрутизацією, динамічно розподіляти трафік між різними каналами зв'язку та забезпечувати високу якість обслуговування QoS з мінімальними затримками. Проте базовий функціонал більшості рішень SD-WAN, який здебільшого орієнтований на оптимізацію продуктивності, а не на глибоку аналітику кіберзагроз. Відтак, виникає парадокс: сучасна інфраструктура володіє інструментами для миттєвої зміни маршрутів та точкової ізоляції будь-якого сегмента, але не має інтелектуального "мозку", здатного передбачити, коли, де і як саме потрібно застосувати ці інструменти для ефективної зупинки хакера.

В роботі для розв'язання задачі прогнозованого аналізу в кібербезпеці активно використовується математичне моделювання у вигляді графів атак Attack Graphs. Граф атак – це формалізована модель, яка об'єднує топологію мережі, правила розмежування доступу та відомі бази вразливостей CVE у спрямований граф, що візуалізує всі математично можливі шляхи переміщення зловмисника до цільового ресурсу. Аналіз такого графа дозволяє не лише зрозуміти поточний стан захищеності, але й спрогнозувати наступні кроки атакуючого.

Актуальність даного дослідження полягає у необхідності переходу від статичної оборони до концепції адаптивної, самозахисної мережі Self-Defending Network. Об'єднання аналітичної потужності графів атак (як системи прийняття рішень) та гнучкості технології SD-WAN (як виконавчої системи) дає можливість створення автоматизованих комплексів кіберзахисту. Завдяки такій синергії система здатна не просто фіксувати факт злому певного сервера, а миттєво розраховувати ймовірний вектор подальшого просування атаки та превентивно, на рівні мережевих комутаторів SD-WAN, блокувати

скомпрометовані шляхи, зберігаючи при цьому безперервність роботи легітимних бізнес-процесів організації [79].

Незважаючи на наявність потужних систем управління подіями інформаційної безпеки (SIEM, SOAR) та гнучких мережевих рішень класу SD-WAN, у більшості сучасних корпоративних інфраструктур ці два домени функціонують концептуально ізольовано. Відділи кібербезпеки SecOps оперують термінами вразливостей, індикаторів компрометації IoC та ймовірнісних ризиків, тоді як мережеві інженери NetOps мислять категоріями пропускної здатності, джитера та таблиць маршрутизації. Ця технологічна розрізненість створює критичний часовий розрив Time Gap між моментом виявлення загрози та моментом застосування контрзаходів на мережевому рівні. У середньому, час реакції на інцидент MTTR, який вимагає ручної реконфігурації правил доступу ACL або маршрутів адміністратором, вимірюється годинами. У контексті автоматизованих багатоетапних атак, де шкідливе програмне забезпечення здатне інфікувати суміжні вузли за лічені секунди, така затримка є неприпустимою та фатальною для безпеки конфіденційних даних.

Крім того, традиційні методи ізоляції загроз часто базуються на принципі "все або нічого". При виявленні підозрілої активності на певному сервері адміністратори, як правило, приймають рішення про повне відключення цього вузла або цілої підмережі VLAN від корпоративної інфраструктури. Такий радикальний підхід дійсно зупиняє просування атаки, але одночасно призводить до відмови в обслуговуванні Denial of Service для всіх легітимних користувачів, порушуючи безперервність бізнес-процесів Business Continuity. У сучасних розподілених середовищах, де один мікросервіс може бути задіяний у сотнях різних транзакцій, грубе мережеве блокування на рівні статичних фаєрволів є економічно недоцільним.

З математичної та алгоритмічної точок зору це суттєво ускладнюється тим, що побудова та аналіз графу атак у масштабах реального часу є NP-складною задачею. Топологія мережі SD-WAN є висородинамічною: віртуальні тунелі

піднімаються та розриваються залежно від навантаження та якості каналів зв'язку. Відповідно, граф атак повинен оновлюватися повністю синхронно зі змінами в мережі, а система безпеки має миттєво перераховувати ймовірності успішної експлуатації вразливостей для нових шляхів. Існує нагальна потреба у розробці математичної моделі та програмного методу, який буде здатний безперервно оцінювати рівень ризику для кожного можливого вектора атаки та при перевищенні встановленого порогу ризику генерувати атомарні, гранулярні політики ізоляції. Після цього автоматично транслювати ці політики в команди конфігурації для контролера SD-WAN.

Насьогодні відсутні комплексні методи та архітектурні рішення для глибокої, автоматизованої інтеграції прогнозованої аналітики (на базі графів атак) із механізмами динамічної маршрутизації SD-WAN. Тому необхідно розробити метод, який дозволить делегувати прийняття рішень щодо реконфігурації мережі алгоритмам штучного інтелекту, виключаючи людину з критичного контуру реагування. Це забезпечить точкову превентивну ізоляцію загроз (на рівні конкретних потоків даних), гарантуючи максимальний захист активів без втрати мережевої зв'язності для легітимного корпоративного трафіку.

Таким чином, розробка методу побудови захищеної комп'ютерної мережі, що управляється SD-WAN на основі графу атак є актуальною задачею і відповідає на нагальні потреби сучасної IT-інфраструктури.

Питання побудови захищених мережевих інфраструктур та автоматизації прогнозованого аналізу кіберзагроз знаходиться в центрі уваги сучасних наукових досліджень в галузі IT. Останні публікації та дослідження у цій сфері доцільно класифікувати за трьома магістральними напрямками: математичне моделювання графів атак, інтеграція безпекових функцій в архітектуру SD-WAN та застосування методів штучного інтелекту для автоматизації реагування на кіберінциденти.

У сфері математичного моделювання кіберзагроз граф атак є фундаментальним аналітичним інструментом. Класичний розрахунок ймовірностей атак виключно на основі метрик CVSS є недостатнім без

урахування топологічних факторів впливу [61]. Застосування алгоритмів вилучення ознак на графах дозволяє з високою точністю виявляти структурні "вузькі місця" в мережі. Подібний підхід до автоматизованої генерації графів атак за допомогою методів машинного навчання дає точність прогнозування шляхів атакуючого на рівні 89,5% [62]. Однак, незважаючи на високу прогнозовану здатність, запропоновані моделі здебільшого залишаються теоретичними інструментами аналізу (для команд SecOps) і не передбачають наявності прямих механізмів втручання в роботу мережевого обладнання.

Другий напрямок зосереджений на еволюції технології SD-WAN та її злитті з концепцією SASE. Активно досліджуються методи впровадження глибокого аналізу трафіку безпосередньо в маршрутизатори. Зокрема, розглядаються методи оцінки затримок у реальному часі за допомогою внутрішньосмугової телеметрії (In-band Network Telemetry) [63], [71] та алгоритми виявлення шкідливого трафіку в SD-WAN за допомогою гібридних нейронних мереж LSTM-GRU [64]. Це підтверджує здатність SD-WAN комутаторів динамічно аналізувати потоки даних і ефективно керувати якістю обслуговування QoS. Водночас недоліком таких систем є те, що рішення щодо блокування трафіку приймаються суто локально, на рівні інспекції окремих пакетів, без урахування глобального контексту розгортання багатоетапної атаки, який може забезпечити лише аналіз графу атак [79].

Третій, найбільш інноваційний напрямок досліджень, пов'язаний із застосуванням навчання з підкріпленням RL для створення автономних систем кіберзахисту. Проведені дослідження на основі концептуальної платформи Adaptive Reinforcement learning for Cybersecurity Strategy [65] доводять, що RL-агенти здатні скоротити час оптимізації реакції на інциденти на 27,3% порівняно з використанням статичних правил. Аналогічні висновки наводяться у дослідженнях щодо автоматизованого тестування на проникнення [66], де RL використовується для пріоритезації захисних дій в умовах невизначеності середовища.

Таким чином, незважаючи на значний науковий прогрес у кожному з виділених напрямків окремо, існує суттєва необхідність у дослідженнях, присвячених їх комплексній інтеграції. На сьогодні практично відсутні наукові праці, які б пропонували єдину архітектуру, де математична модель графу атак слугує формалізованим середовищем Environment для RL-агента, а рішення цього агента Actions безперервно транслуються в конфігураційні API-команди для центрального контролера SD-WAN. Розробка такого комплексного, крос-доменного методу управління мережевою безпекою залишається актуальним та нерозв'язаним на сьогодні науковим завданням [79].

3.2.2. Розробка архітектури адаптивної системи кіберзахисту

На основі проведеного аналізу існуючих методів та засобів захисту корпоративних інформаційних систем та виявлених архітектурних недоліків традиційних реактивних систем безпеки розробимо концептуальну архітектуру захищеної комп'ютерної системи, яка логічно об'єднує площину моніторингу безпеки Security Plane, що відповідає за генерацію графів атак, та площину управління інфраструктурою SD-WAN Control Plane. Для цього побудуємо математичну модель кількісної оцінки ризиків компрометації інформаційних активів. Формалізуємо процес побудови спрямованого графу атак, розробимо алгоритм розрахунку ймовірності успішної експлуатації вектора атаки на основі метрик вразливостей CVSS та визначимо математичні критерії для автоматичного розгортання змін у мережі для проведення превентивних мережевих реконфігурацій [79].

Проведемо обґрунтування архітектури системи та вибір підходу до реалізації. Розробка адаптивної системи кіберзахисту вимагає переходу від традиційної монолітної архітектури мережевого обладнання до модульної, програмно-визначеної парадигми. Запропонований метод базується на глибокій інтеграції технологій SD-WAN та систем прогнозованої аналітики загроз. Фундаментальною відмінністю розробленої архітектури є введення логічно

незалежної площини безпеки Security Plane, яка функціонує паралельно з класичними площинами програмно-конфігурованих мереж. Загальна інфраструктура системи декомпозується на три базові взаємопов'язані компоненти [79].

По-перше, це площина передачі даних Data Plane – SD-WAN Edge. Цей рівень представлений периферійними маршрутизаторами (апаратними пристроями або віртуальними мережевими функціями VNF), які розташовані безпосередньо у філіях, центрах обробки даних або хмарних середовищах організації. Головна функція Data Plane зводиться до високонавантаженої комутації пакетів. Маршрутизатори цього рівня позбавлені самостійних механізмів прийняття рішень щодо глобальної маршрутизації. Натомість вони виконують дві критичні задачі. Вони апаратно застосовують конфігураційні політики та списки контролю доступу ACL, що спускаються з вищого рівня та виконують роль безперервних мережесенсорів, генеруючи потік телеметрії NetFlow/IPFIX та здійснюючи глибоку інспекцію пакетів DPI для виявлення аномалій на рівні застосунків.

По-друге, це площина управління Control Plane – SD-WAN Controller. Централізований інтелектуальний модуль управління мережею, який розгортається у відмовостійкому хмарному кластері або ядрі мережі. Контролер акумулює глобальну інформацію про стан усіх каналів зв'язку, метрики затримок Latency та втрати пакетів Packet Loss. Його ключова роль – підтримка актуальної топології та динамічний розподіл трафіку Traffic Steering на основі критеріїв якості обслуговування QoS. У контексті запропонованого методу Control Plane виступає «виконавчим механізмом»: він отримує екстрені тригери від площини безпеки через захищений RESTful API і за лічені мілісекунди транслює їх у специфічні інструкції (наприклад, через протоколи OpenFlow або NETCONF) для миттєвої мікросегментації та ізоляції скомпрометованих шляхів на рівні Data Plane.

По-третє, це площина безпеки та аналітики Security & Analytics Plane, ядро проактивного кіберзахисту, яке об'єднує системи класу SIEM та спеціалізований

математичний рушій обчислення графів атак Attack Graph Engine. Цей компонент безперервно агрегує телеметрію від Data Plane, логи доступу та актуальні дані баз вразливостей CVE/NVD. На основі цієї інформації алгоритм будує багатовимірний спрямований граф, що візуалізує та кількісно оцінює всі можливі вектори ескалації привілеїв зловмисником. Саме на цьому рівні функціонує ML-агент (на базі навчання з підкріпленням), який розраховує рівень ризику для кожного потенційного шляху атаки R_{path} та формує оптимальні превентивні політики блокування. Ці політики генеруються і передаються на Control Plane ще до того, як атака досягне цільових критичних активів.

Логічна схема взаємодії трьох базових площин запропонованої системи показана на рис. 3.1.

При проектуванні адаптивної системи кіберзахисту виникає питання використання монолітного варіанту рішення All-in-One або варіанту розподіленої моделі Best-of-Breed. Концепція уніфікованого управління загрозами Unified Threat Management передбачає інтеграцію функцій маршрутизації та аналізу безпеки (включно з обчисленням графу атак) безпосередньо на периферійному обладнанні. Попри легкість розгортання, цей підхід має критичні недоліки. Математичне моделювання графів атак для великих інфраструктур є NP-складною задачею, яка вимагає значних обчислювальних ресурсів.

Перенесення цього навантаження на кінцеві маршрутизатори неминуче призведе до деградації пропускної здатності мережі та затримок у комутації пакетів. Крім того, вбудовані модулі безпеки часто поступаються за глибиною аналізу спеціалізованим рішенням. Тому, в запропонованому методі пропонується варіант розподіленої архітектури (або моделі SASE). Вона дозволяє винести висидкопродуктивні обчислення, пов'язані з графами атак, на потужні виділені сервери або у хмарне середовище. При цьому периферійні пристрої Edge залишаються ненавантаженими додатковими функціями, зосереджуючись виключно на швидкій доставці пакетів і виконанні політик. Таке розділення обов'язків гарантує масштабованість системи, високу швидкість

реакції на загрози та можливість інтеграції найкращих у своєму класі незалежних рішень з кібербезпеки та мережевого управління [79].

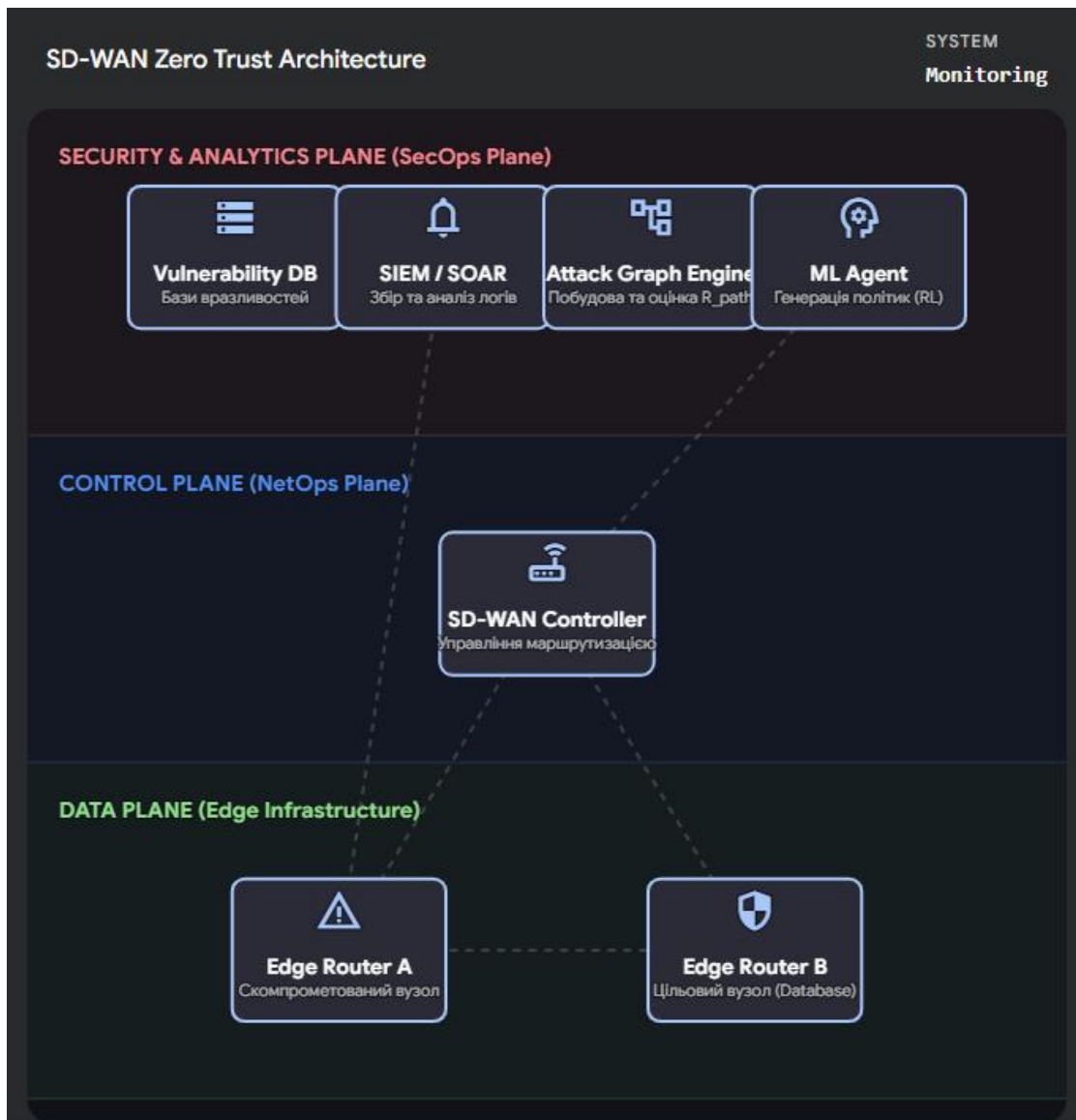


Рисунок 3.1. Логічна схема взаємодії трьох базових площин адаптивної системи кіберзахисту

Розробимо математичну модель оцінки ризиків на базі графу атак. Для наочної демонстрації роботи запропонованої математичної моделі та механізму прийняття рішень контролером SD-WAN, на рис. 3.2. наведемо фрагмент формалізованого графу атак $G = (V, E)$. Цей граф змодельовано для типової мікросервісної архітектури, що включає клієнтську частину (наприклад, JS-

фронтенд), сервер бізнес-логіки (Java-бекенд) та цільову реляційну базу даних. На схемі відображено вузли (v_i), імовірності успішної експлуатації вразливостей на ребрах $p(v_i, v_j)$ та розрахунок загального рівня ризику R_{path} , що слугує тригером для реконфігурації SD-WAN [79].

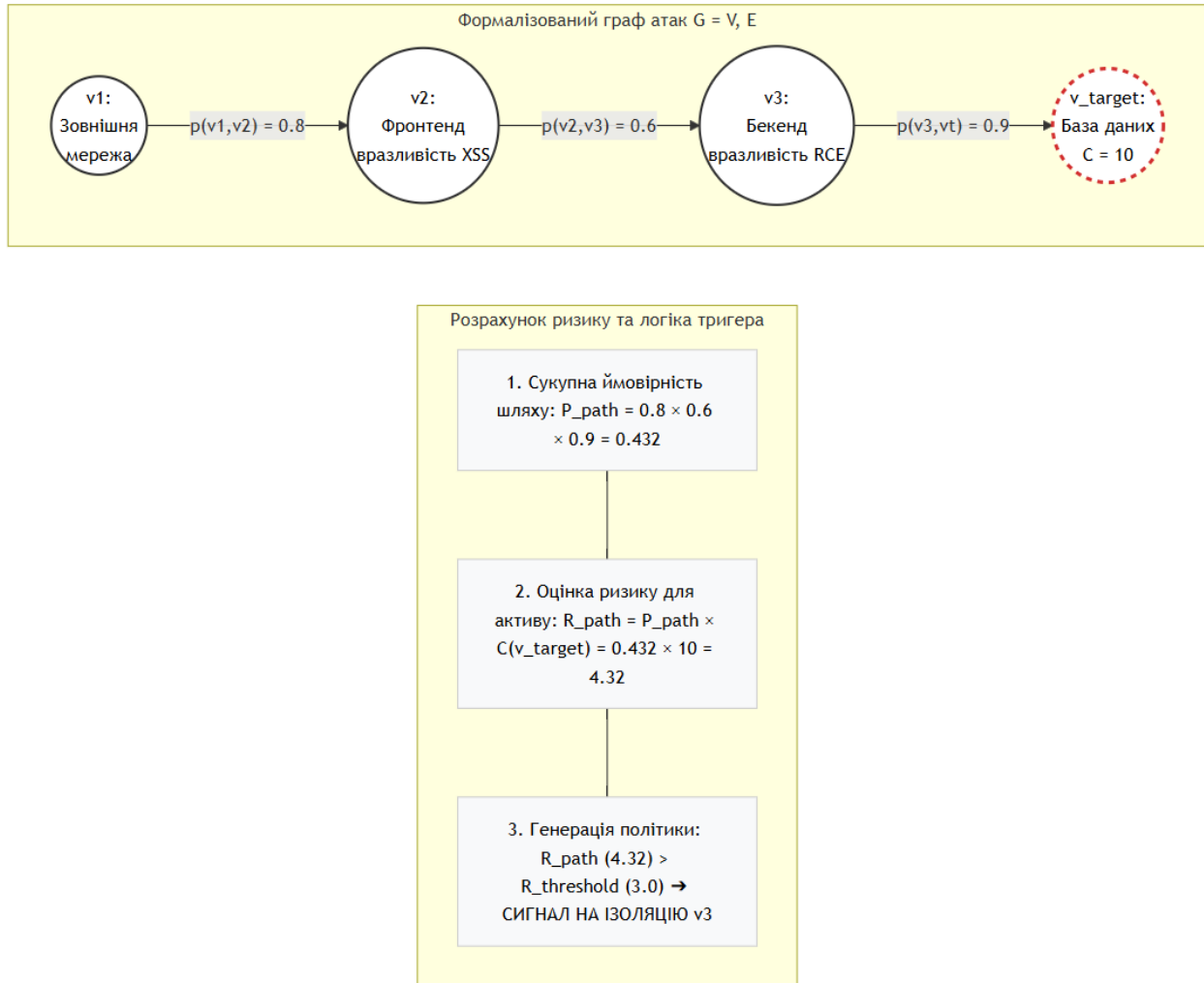


Рисунок 3.2. Структурна схема формалізованого графу атак $G = (V, E)$ для оцінки ризиків компрометації

Граф відображає сценарій багатоетапної компрометації. Вузол v_1 виступає точкою входу (зовнішня мережа). Згідно зі сценарієм, зловмисник послідовно експлуатує вразливість XSS на фронтенді (перехід до вузла v_2), потім отримує можливість віддаленого виконання коду RCE на бекенд-сервері (перехід до вузла v_3) і, зрештою, намагається здійснити несанкціонований доступ до бази даних

v_{target} [79] [79].

Кожному ребру графу відповідає ймовірність успішної експлуатації вразливості $p(v_i, v_j)$, яку аналітичний модуль вираховує на базі метрик CVSS. У наведеному прикладі ці ймовірності становлять 0,8, 0,6 та 0,9 відповідно. Згідно з розробленою моделлю, загальна ймовірність успішної експлуатації всього ланцюжка атаки P_{path} визначається як добуток ймовірностей кожного кроку 0,432.

Оскільки цільовий вузол (база даних) містить критичну для бізнесу інформацію, йому присвоєно максимальний коефіцієнт критичності $C = 10$. Відповідно, загальний рівень ризику для цього вектора становить $R_{path} = 0,432 \times 10 = 4,32$. Отримане розрахункове значення перевищує встановлений в системі допустимий поріг ризику ($R_{threshold} = 3$). Це порушення порогового значення миттєво фіксується площиною безпеки, яка генерує екстрений API-виклик до контролера SD-WAN. Отримавши тригер, мережевий контролер превентивно реконфігурує таблиці маршрутизації, здійснюючи мережеву ізоляцію скомпрометованого вузла v_3 ще до того, як атака досягне цільової бази даних.

Проведемо формалізацію графу атак. Для автоматизованого управління мережевою інфраструктурою SD-WAN на основі прогнозованої аналітики, необхідно створити строгу математичну модель, яка трансформує неструктуровані дані про топологію та вразливості у формалізований, машинозчитуваний вигляд. В основу розробленого методу покладено подання можливих векторів компрометації у вигляді мультидоменного орієнтованого графу атак [79].

Математично граф атак визначається як кортеж $G_{AG} = (V, E)$, де V – множина вершин (вузлів), а $E \subseteq V \times V$ – множина спрямованих ребер, що відображають причинно-наслідкові зв'язки між об'єктами мережі. Для забезпечення високої гранулярної аналізу, множина вершин V декомпонується на три непересічні підмножини: $V = S \cup A \cup C$.

1. Підмножина станів $S = \{s_1, s_2, \dots, s_k\}$ описує рівень привілеїв зловмисника на конкретному вузлі мережі (наприклад, s_1 – "анонімний доступ до сегмента DMZ", s_2 – "права адміністратора на сервері баз даних").

2. Підмножина атомарних атак $A = \{a_1, a_2, \dots, a_m\}$ формалізує дії, які зловмисник може виконати для ескалації привілеїв. Кожен елемент $a_i \in A$ однозначно зіставляється з відомими векторами з баз CVE або специфічними техніками з матриці MITRE ATT&CK.

3. Підмножина умов $C = \{c_1, c_2, \dots, c_l\}$ характеризує конфігураційні передумови мережі (наявність відкритого порту, використання застарілого протоколу шифрування, наявність активного маршруту між віртуальними локальними мережами VLAN).

Множина спрямованих ребер E формується на основі логічних операцій кон'юнкції та диз'юнкції. Ребро $e = (v_i, v_j)$ існує тоді й лише тоді, коли виконання певної умови або успішна реалізація атаки у вузлі v_i є прямою математичною передумовою (precondition) для переходу системи до стану v_j .

Для алгоритмічної обробки графу на рівні програмного забезпечення (Security Plane) використовується матриця суміжності M розмірності $N \times N$, де $N = |V|$. Елементи матриці $m_{ij} \in \{0,1\}$ визначають наявність зв'язку між вузлами. Таке матричне подання дозволяє застосовувати класичні алгоритми теорії графів (наприклад, алгоритм Дейкстри) для надшвидкого генерування всіх можливих ланцюжків атаки за час $O(|V| + |E|)$, що є критично важливим для систем реального часу.

Ключовою інновацією формалізації є математичне зв'язування логічного графу атак G_{AG} із графом фізичної топології мережі $G_{NET} = (H, L)$, де H – фізичні та віртуальні хости, а L – лінії зв'язку (тунелі SD-WAN). Це зв'язування задається відображенням $f: G_{AG} \rightarrow G_{NET}$. Якщо аналітичний модуль виявляє високий ризик компрометації, він передає команду на контролер SD-WAN для розриву або зміни певного фізичного маршруту $l \in L$. Згідно з відображенням f , видалення маршруту l автоматично анулює відповідну множину умов $C_{blocked} \subset C$ у графі атак. Це спричиняє каскадне "видалення" ребер, руйнуючи цілісність ланцюжка

атаки та унеможливлуючи досягнення цільового стану зловмисником ще на етапі розвідки.

Оцінка ймовірності успішної реалізації кібератаки вимагає переходу від детермінованих моделей до стохастичних. У запропонованому методі граф атак розглядається як байєсівська мережа Bayesian Attack Graph, що дозволяє максимально точно враховувати умовні ймовірності переходів зловмисника між станами системи.

Кожному вузлу (вразливості) v_i ставиться у відповідність локальна ймовірність успішної експлуатації $p(v_i)$. Для об'єктивної квантифікації цього показника використовується стандартизована метрика Common Vulnerability Scoring System, зокрема її базова підгрупа Exploitability Subscore. Ймовірність експлуатації ізольованої вразливості апроксимується нелінійною функцією [79]:

$$p(v_i) = \frac{CVSS_Exploitability}{10}, \quad (3.15)$$

яка комплексно враховує вектор доступу Access Vector, складність експлуатації Access Complexity та рівень необхідних привілеїв Privileges Required.

Оскільки багатоетапна атака є послідовністю алгоритмічно залежних подій, ймовірність досягнення зловмисником вузла v_j за умови компрометації попереднього вузла v_i визначається умовною ймовірністю $P(v_j | v_i)$. Загальна ймовірність успішної компрометації цільового вузла v_{target} через конкретний вектор $Path = \{v_1, v_2, \dots, v_n\}$ обчислюється як спільна ймовірність у байєсівській мережі з використанням ланцюгового правила [79]:

$$P(Path) = \prod_{k=1}^n P\left(\frac{v_k}{Parents(v_k)}\right), \quad (3.16)$$

де $Parents(v_k)$ – множина безпосередніх попередників вузла v_k у спрямованому графі атак.

Крім того, для складних топологій, де до критичного ресурсу ведуть паралельні (альтернативні) шляхи, сукупна ймовірність компрометації вузла v_j

від кількох незалежних попередників розраховується за формулою диз'юнкції незалежних подій [79]:

$$P_{cum}(v_j) = 1 - \prod_{v_i \in Parents(v_j)} (1 - P(v_i)p(v_i, v_j)), \quad (3.17)$$

Такий математичний апарат дозволяє модулю Security Plane у режимі реального часу динамічно перераховувати ймовірності загрози при зміні мережевої топології (наприклад, при автоматичному відкритті нових тунелів SD-WAN) або при публікації інформації про нові вразливості (zero-day експлойти), забезпечуючи математично обґрунтовану точність прогнозованої аналітики.

Отримання імовірнісних оцінок компрометації є необхідною, але недостатньою умовою для ініціювання автоматичної реконфігурації мережі. Прийняття рішення контролером SD-WAN повинно базуватися на комплексному показнику ризику R , який враховує не лише ймовірність атаки, але й ступінь економічного чи операційного збитку від її успішної реалізації.

Кожному активу (серверу, базі даних, мікросервісу) у мережі присвоюється вектор критичності [79]

$$C(v) = \{C_{conf}, C_{int}, C_{avail}\}, \quad (3.18)$$

що відображає потенційний вплив інциденту на конфіденційність, цілісність та доступність інформації. Агрегований показник цінності цільового вузла $Value(v_{target})$ нормалізується у діапазоні $[0, 10]$. Кількісна оцінка ризику для конкретного шляху атаки R_{path} формалізується як математичне очікування збитку [79]:

$$R_{path} = P(Path)Value(v_{target}). \quad (3.19)$$

Для забезпечення безперервності бізнес-процесів Business Continuity система вводить додаткову метрику "вартості ізоляції" Isolation Cost, яка визначає ступінь деградації мережі у разі застосування превентивного блокування. Наприклад, відключення критичного магістрального лінку SD-WAN матиме гранично високий показник IC , тоді як точкове блокування специфічного порту для підозрілої IP-адреси – низький.

Логіка генерації мережевих політик базується на оптимізаційній задачі. Система формує тригер на зміну конфігурації SD-WAN лише у випадку, якщо прогнозоване зниження ризику ΔR суттєво перевищує експлуатаційні втрати від застосування самої політики. Математична умова активації захисного механізму описується системою нерівностей [79]:

$$\begin{cases} R_{path} > R_{threshold}; \\ \Delta R - \lambda * IC_{policy} > 0. \end{cases} \quad (3.20)$$

де $R_{threshold}$ – глобальний поріг толерантності до ризику, встановлений політикою безпеки організації; λ – балансуєчий коефіцієнт trade-off factor, що регулює пріоритет безпеки над доступністю (для критичних інфраструктур $\lambda \rightarrow 0$); а ΔR – різниця між поточним ризиком та залишковим ризиком після реконфігурації маршрутів.

У разі виконання цих умов, площина безпеки компілює набір атомарних інструкцій (наприклад, ізоляція VLAN, перенаправлення трафіку у Honeypot) і передає їх через REST API до SD-WAN контролера. Контролер транслює ці інструкції у правила OpenFlow, миттєво перебудовуючи топологію площини передачі даних (Data Plane) та фізично розриваючи причинно-наслідковий ланцюжок графу атак.

3.2.3. Удосконалення методу динамічного управління мережевою безпекою на основі навчання з підкріпленням

Незважаючи на високу обчислювальну точність математичної моделі оцінки ризиків R_{path} , використання жорстко заданих статичних порогових значень $R_{threshold}$ виявляє низку критичних обмежень під час експлуатації у високодинамічних корпоративних середовищах. Класичний евристичний підхід, що базується на бінарній логіці прийняття рішень («якщо ризик перевищує поріг – застосувати блокування»), виявляється недостатньо ефективним проти сучасних еволюціонуючих кіберзагроз АРТ з огляду на кілька фундаментальних архітектурних та операційних причин [79].

По-перше, виникають хибні спрацьовування False Positives та деградація бізнес-процесів. У сучасних мікросервісних архітектурах та хмарних середовищах Cloud-Native топологія мережі змінюється безперервно: контейнери автоматично масштабуються, а SD-WAN динамічно перерозподіляє потоки даних для балансування навантаження. Встановлення заниженого порогу чутливості системи безпеки призводить до того, що нестандартна, але легітимна мережева активність (наприклад, масове резервне копіювання бази даних у неробочий час або розгортання масштабного оновлення) генерує показник R_{path} , що перевищує статичний $R_{threshold}$. Як наслідок, контролер SD-WAN ініціює превентивне блокування, викликаючи штучну відмову в обслуговуванні Denial of Service для авторизованих користувачів та завдаючи прямих фінансових збитків організації.

По-друге, система залишається вразливою до атак нульового дня Zero-day та технік прихованого проникнення Living off the Land, LotL. Статична імовірнісна модель оцінки ризиків значною мірою залежить від наявності експлоїтів у базах CVE. Зловмисники, які використовують невідомі раніше вразливості або застосовують легітимні інструменти адміністрування (наприклад, PowerShell, WMI) для ескалації привілеїв, генерують мінімальні аномалії. Математичний рушій може оцінити такий ланцюжок нижче критичного

порогу. Спроба мережевих інженерів завищити значення $R_{threshold}$ (з метою уникнення блокування бізнес-процесів) створює розширену «сліпу зону» (False Negatives), в якій атакуючий отримує можливість місяцями безперешкодно переміщуватися мережею, збираючи дані.

По-третє, статичний підхід унеможлиблює багатокритеріальну оптимізацію в реальному часі. Фіксований поріг не здатен адаптуватися до поточного контексту завантаженості мережі. Наприклад, в умовах пікового навантаження на магістральні канали зв'язку вартість ізоляції (Isolation Cost) певного сегмента може катастрофічно зрости, роблячи блокування економічно недоцільним. Статичне правило проігнорує цей фактор і змусить SD-WAN розірвати з'єднання, тоді як гнучка система могла б обрати альтернативний шлях – наприклад, перенаправити підозрілий трафік у систему глибокого аналізу (Honeypot/Sandbox) без зупинки основного бізнес-потoku.

Використання статичного порогу блокування $R_{threshold}$ неминуче призводить до компромісу між рівнем хибних спрацьовувань (перешкоджання бізнес-процесам) та кількістю пропущених прихованих атак.

Відповідно, виникає об'єктивна необхідність переходу від жорстких математичних нерівностей до адаптивних систем прийняття рішень. Система захисту повинна динамічно зміщувати межу класифікації Decision Boundary залежно від багатовимірною контексту (рис. 3.3.): поведінки користувачів, стану мережевого обладнання та поточної цінності активів, що обґрунтовує необхідність переходу до адаптивних ML-моделей. Тому вирішення цієї задачі вимагає впровадження методів машинного навчання, здатних до самоадаптації на основі накопиченого досвіду.

Таким чином, завдання динамічного управління мережевою безпекою є задачею послідовного прийняття рішень в умовах невизначеності. Зловмисник Attacker постійно змінює вектори атаки, а стан мережі (навантаження, затримки) піддається стохастичним коливанням. Для вирішення цієї задачі запропоновано формалізувати взаємодію між площиною безпеки Security Plane та площиною передачі даних Data Plane як Марковський процес прийняття рішень MDP [79].

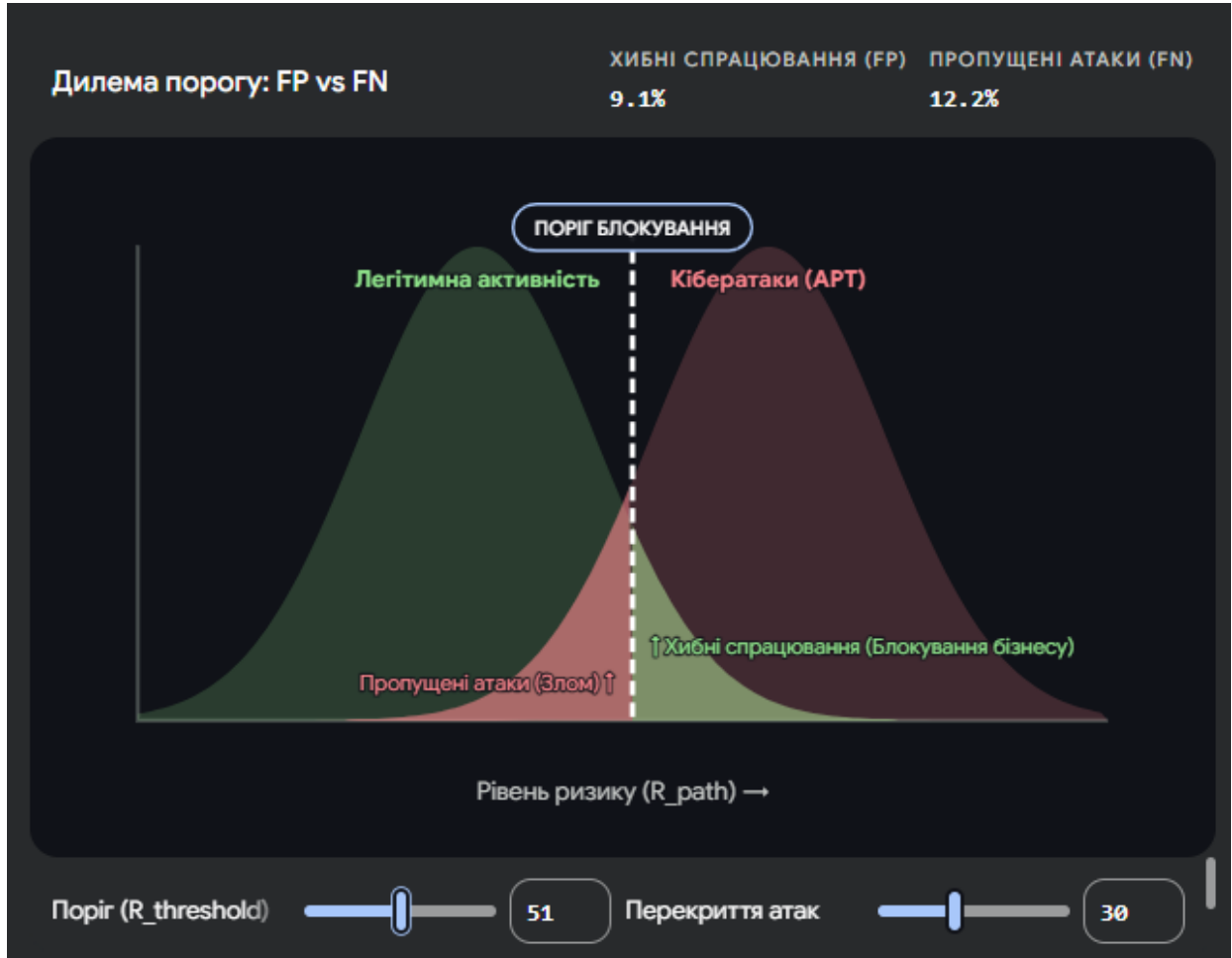


Рисунок 3.3. Перекриття розподілів легітимної мережевої активності та кібератак

Математично MDP задається кортежем $\langle S, A, P, R, \gamma \rangle$, де кожна компонента суворо адаптована під специфіку інтеграції графів атак та SD-WAN. Агентом Agent у цій моделі виступає інтелектуальний модуль контролера, а середовищем Environment – комп'ютерна інфраструктура разом із діями зловмисника [79].

Стан середовища $s_t \in S$ у момент часу t не може бути описаний єдиним скалярним значенням у багатовимірному просторі станів S . Він формується як комплексний тензор, що агрегує топологічні, безпекові та телеметричні метрики

$$s_t = \left[M_{\{AG\}}^{\{(t)\}}, R^{(t)}, T^{(t)} \right], \quad (3.21)$$

де $M_{\{AG\}}^{\{(t)\}}$ – матриця суміжності поточного графу атак розмірності $N \times N$, яка фіксує всі виявлені вразливості та відкриті мережеві маршрути на момент часу t ; $\overrightarrow{R^{(t)}}$ – вектор-стовпець оцінок ризику для кожного вузла мережі, розрахований на базі байєсівських імовірностей; $\overrightarrow{T^{(t)}}$ – вектор телеметрії SD-WAN, що включає метрики якості обслуговування QoS: доступну пропускну здатність Bandwidth, затримку latency та відсоток втрати пакетів Packet Loss для кожного тунелю.

Простір дій $a_t \in A$ є дискретною множиною конфігураційних команд (API-викликів), які агент може передати на контролер SD-WAN. Дія формалізується як вектор $a_t = \{type, target, parameters\}$, де типи дій включають: a_{noop} – продовження моніторингу (бездіяльність); $a_{block}(v_i, v_j)$ – повна ізоляція (розірвання тунелю або застосування жорсткого ACL) між вузлами v_i та v_j ; $a_{reroute}(flow, path_{alt})$ – перенаправлення підозрілого потоку даних на альтернативний маршрут (наприклад, у Honeypot або систему глибокої інспекції пакетів DPI); $a_{limit}(v_k, bw)$ – обмеження пропускну здатності Rate Limiting для скомпрометованого вузла з метою уповільнення ексфільтрації даних.

Розглянемо стохастичні переходи P та багатокритеріальну функцію винагороди R . Функція переходу представлена виразом $P(s_{t+1}|s_t, a_t)$ показує ймовірність того, що середовище перейде у стан s_{t+1} після застосування дії a_t . У кібербезпеці ця функція є невідомою Model-free, оскільки неможливо точно передбачити, як саме зловмисник відреагує на блокування одного зі шляхів (наприклад, він може застосувати експлоїт нульового дня для обходу).

Функція винагороди $r_t = R(s_t, a_t)$ є критичним елементом, що формує "мотивацію" алгоритму. Для досягнення балансу між безпекою та безперервністю бізнес-процесів розроблено багатокритеріальну функцію винагороди [79]

$$r_t = \omega_1 \Delta Risk(s_t, a_t) - \omega_2 Penalty_{QoS}(s_{t+1}) - \omega_3 Cost_{deploy}(a_t), \quad (3.22)$$

де $\Delta Risk$ – позитивна винагорода за зниження загального рівня ризику в графі атак після ізоляції загрози; $Penalty_{QoS}$ – штраф за деградацію продуктивності мережі (наприклад, якщо обрано неоптимальний резервний маршрут, що призвів до зростання затримки для легітимних користувачів); $Cost_{deploy}$ – штраф за зміну конфігурації (запобігає "флуктуаціям", коли агент безперервно змінює правила туди-назад); $\omega_1, \omega_2, \omega_3$ – гіперпараметри, що визначають вагу кожного критерію (встановлюються адміністратором безпеки).

Проведемо апроксимацію політики безпеки за допомогою глибоких нейронних мереж (DQN/GNN). Оскільки простір станів S у корпоративних мережах є дуже великим, класичні табличні методи RL (наприклад, Q-Learning) є непридатними. Для вирішення задачі впроваджено архітектуру Deep Q-Network.

Крім того, оскільки базовим елементом стану є Граф атак, звичайні багат шарові перцептрони MLP втрачають топологічну інформацію. Використаємо Графові згорткові нейронні мережі Graph Convolutional Networks як екстрактор ознак Feature Extractor. GCN ефективно обробляє матрицю суміжності M_{AG} , агрегуючи інформацію від сусідніх вузлів, що дозволяє агенту "розуміти" просторову структуру мережі.

Згорткові шари GCN передають вектор ознак до повнозв'язних шарів, які на виході апроксимують функцію цінності дії $Q(s, a, \theta)$, де θ – ваги нейронної мережі. Навчання агента зводиться до мінімізації функції втрат Loss Function на основі рівняння Беллмана за допомогою алгоритму градієнтного спуску [79]:

$$L(\theta) = \mathbb{E}_{s,a,r,s'} \left[\left(r + \gamma \max_{a'} Q(s', a', \theta^-) - Q(s, a, \theta) \right)^2 \right] \quad (3.23)$$

де θ^- – ваги цільової мережі Target Network, що забезпечує стабільність збіжності, а $\gamma \in [0,1)$ – фактор дисконтування, який змушує агента враховувати довгострокові наслідки своїх мережевих політик (наприклад, блокування вузла зараз може врятувати базу даних через 10 кроків атаки).

Натренована модель розгортається на площині безпеки Security Plane і здатна за мілісекунди обчислити $\arg \max_a Q(s, a)$ для будь-якого поточного стану, видаючи оптимальну політику для контролера SD-WAN у реальному часі.

Таким чином, у формальному вигляді процес взаємодії підсистем комп'ютерної мережі, як Марківського процесу прийняття рішень, та агенту (натренована нейронна мережа) можна описати наступним чином: агент безперервно отримує багатовимірний стан середовища (граф атак та телеметрію) і генерує оптимальні дії (політики SD-WAN), максимізуючи сумарну винагороду (рис. 3.4.).

Розглянемо процес автоматизації прийняття рішень та механізми трансляції політик Adaptive SD-WAN Policies більш детально. Процес інтелектуальної автоматизації генерування мережевих політик концептуально поділяється на дві ключові фази: попереднє автономне навчання Offline Training та експлуатацію в режимі реального часу Online Inference.

Оскільки навчання агента з підкріпленням безпосередньо в робочій мережі методом спроб і помилок Trial-and-Error є категорично неприпустимим через критичний ризик порушення бізнес-процесів, первинне тренування відбувається в ізолюваному імітаційному середовищі – цифровому двійнику Digital Twin інфраструктури. Використовуючи ϵ -жадібну стратегію дослідження (ϵ -greedy exploration), агент генерує і відбиває сотні тисяч епізодів багатоетапних кібератак. На цьому етапі алгоритм шляхом багаторазових ітерацій оновлює ваги нейронної мережі, поступово знижуючи рівень випадкових дій і максимізуючи значення функції корисності для кожної можливої конфігурації.

Після досягнення математичної збіжності моделі, навчена архітектура інтегрується в площину безпеки Security Plane)реальної мережі [79]. У режимі експлуатації ML-агент працює виключно на випередження. Коли аналітичний модуль на базі SIEM фіксує зміну стану мережі s_t (наприклад, успішну експлуатацію вразливості початкового рівня v_1), агент за лічені мілісекунди обчислює вектор очікуваних винагород для всіх можливих дій і детерміновано

обирає оптимальну політику $a_{opt} = \arg \max_a Q(s_t, a)$, яка гарантує найкращий баланс між купіруванням загрози та збереженням якості обслуговування QoS.

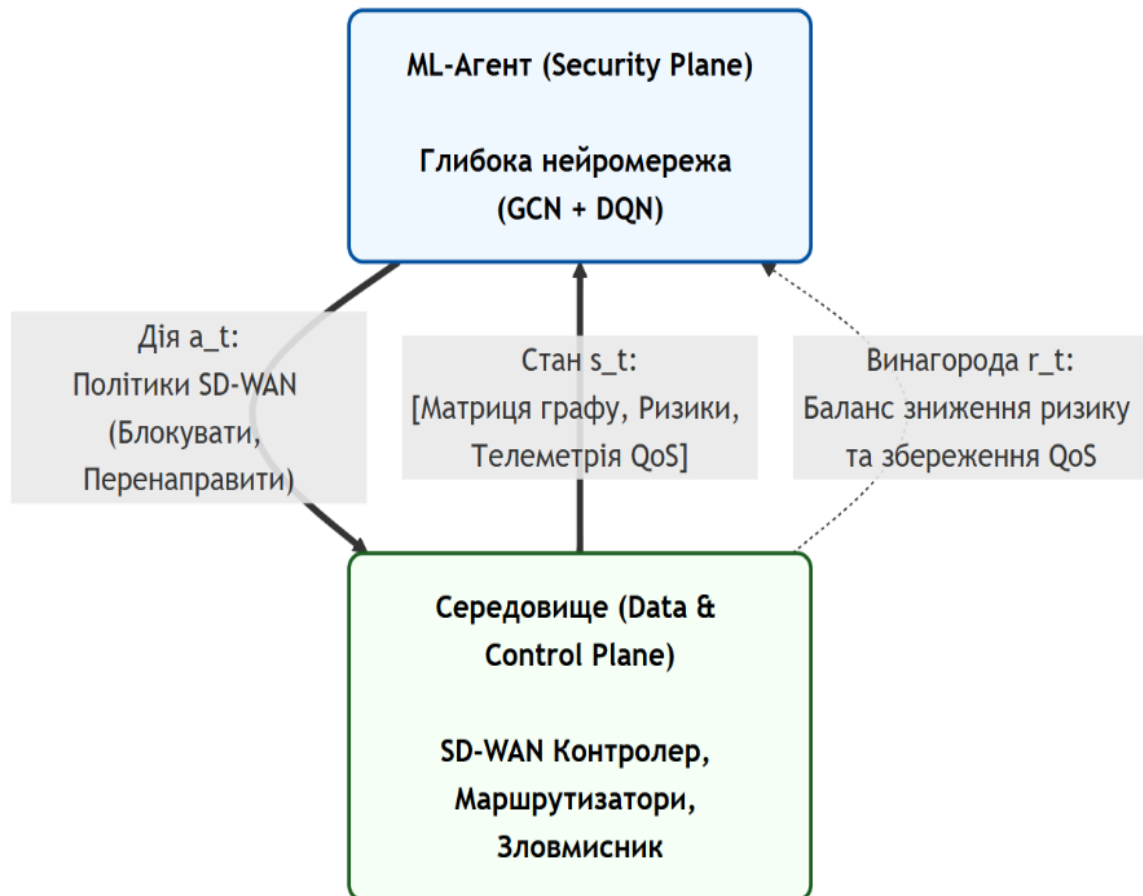


Рисунок 3.4. Взаємодія комп'ютерної мережі та агента натренованої нейронної мережі

Вирішальним етапом автоматизації є процес семантичної трансляції абстрактного математичного рішення ML-агента в конкретні апаратні інструкції. Агент формує високорівневий намір (Intent-based policy), наприклад, «ізолювати сегмент бекенду від бази даних». Ця команда передається через захищений RESTful API або gRPC до центрального контролера SD-WAN. Контролер, своєю чергою, виконує роль транслятора: він перетворює цю абстрактну вимогу в низькорівневі конфігураційні правила для площини передачі даних Data Plane. Залежно від архітектури периферійних пристроїв, це можуть бути інструкції протоколу OpenFlow для модифікації таблиць потоків Flow Tables, конфігурації

NETCONF/YANG для динамічної зміни списків контролю доступу ACL або ж оновлення метрик протоколів маршрутизації для перенаправлення підозрілого трафіку Traffic Steering у захищену інфраструктуру глибокого аналізу Honeypot/DPI.

Для мінімізації ризиків неконтрольованої поведінки алгоритмів штучного інтелекту, в архітектуру контролера SD-WAN обов'язково інтегрується модуль детермінованих запобіжників. Цей модуль жорстко верифікує згенеровані машиною політики на відповідність критичній бізнес-логіці. Наприклад, системі на рівні статичного коду заборонено повністю ізолювати керуючі інтерфейси або розривати тунелі до серверів резервного копіювання. Таким чином, запропонований механізм забезпечує миттєву, проактивну перебудову мережевого "лабіринту" навколо зловмисника, розриваючи граф атаки ще до досягнення цілі, та гарантує безперебійну маршрутизацію трафіку легітимних користувачів альтернативними каналами.

3.3. Розробка алгоритму управління мережевою безпекою на основі навчання з підкріпленням

Розглянемо алгоритм оновлення політик на базі Q-навчання. Для практичної реалізації інтелектуального агента в архітектурі SD-WAN доцільно застосувати алгоритм Q-Learning. Це метод навчання з підкріпленням, який не вимагає попереднього знання моделі середовища і базується на оцінці часових відмінностей. Основною метою агента є пошук оптимальної політики π^* , яка максимізує сумарну очікувану функцію корисності (винагороду) в довгостроковій перспективі.

В основі алгоритму лежить ітеративне оновлення функції цінності дії (Q -функції). Значення $Q(s, a)$ відображає очікувану ефективність застосування конкретної мережевої політики a (наприклад, блокування порту або перенаправлення трафіку) у поточному стані системи s (визначеному на основі

графу атак та телеметрії). Процес накопичення знань агентом математично описується рівнянням Беллмана [79]:

$$Q(s_t, a_t) = Q(s_t, a_t) + \alpha \left[\left(r_t + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t) \right) \right], \quad (3.24)$$

де a_t – обрана дія (набір інструкцій для контролера SD-WAN); s_t, s_{t+1} – поточний та наступний стани мережевої інфраструктури відповідно; r_t – отримана миттєва винагорода, обчислена за багатокритеріальною формулою (баланс зниження ризику та збереження QoS); $\alpha \in (0,1]$ – коефіцієнт швидкості навчання Learning Rate, що визначає ступінь довіри до нової інформації порівняно з уже накопиченим досвідом; $\gamma \in [0,1)$ – фактор дисконтування, який балансує пріоритет між миттєвою вигодою від відбиття поточної атаки та довгостроковими наслідками для стабільності мережі; $\max_a Q(s_{t+1}, a)$ – максимальна очікувана оцінка корисності для найкращої доступної політики в наступному стані.

Питання вибору між дослідженням нових, потенційно ефективніших стратегій захисту та використанням уже перевірених правил вирішується за допомогою ε -жадібної стратегії (ε -greedy). З імовірністю ε агент обирає випадкову політику конфігурації для вивчення реакції мережі та зловмисника, а з імовірністю $1 - \varepsilon$ – застосовує політику з максимальним відомим значенням Q . По мірі навчання (збільшення кількості ітерацій) параметр ε експоненційно зменшується, переводячи систему з режиму активного навчання в режим стабільної експлуатації.

У пам'яті контролера Security Plane Q -функція може бути представлена у вигляді матриці Q-Table для систем з дискретним простором станів, або апроксимована за допомогою глибоких нейронних мереж DQ для складних корпоративних інфраструктур із безперервним потоком телеметрії.

На основі отриманих результатів розроблено блок-схему алгоритму Q-навчання для агента SD-WAN, яка представлена на рис. 3.5. Вона відображає наступні етапи [79]:

1. Ініціалізація – задаються параметри α , γ , ϵ та обнуляється Q-таблиця.
2. Отримання стану – агент зчитує поточний стан мережі.
3. Epsilon-greedy вибір – генерується випадкове число і порівнюється з ϵ : якщо менше – дослідження (випадкова дія), інакше – використання (дія з максимальним Q).
4. Виконання дії – обрана мережева політика застосовується.
5. Отримання нагороди – фіксується reward і next_state.
6. Оновлення за Беллманом – нове Q-значення обчислюється і зберігається в таблицю.
7. Перехід до наступного стану – цикл повторюється.
8. Стрілка праворуч показує нескінченний цикл навчання, що повертається до кроку отримання стану.

Таким чином, удосконалено метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак, який відрізняється від існуючих тим, що він ґрунтується на основі глибокого навчання з підкріпленням та дозволяє превентивно перебудовувати мережеві маршрути та розривати ланцюжки кібератак на ранніх стадіях їх розвитку.

3.4. Висновки до розділу 3

1. У розділі обґрунтовано та запропоновано комплексний підхід до управління інформаційною мережею SD-WAN та комплексний метод побудови захищеної комп'ютерної системи, що концептуально змінює підхід до мережевої безпеки: від реактивного блокування загроз до створення адаптивної, самозахисної інфраструктури.

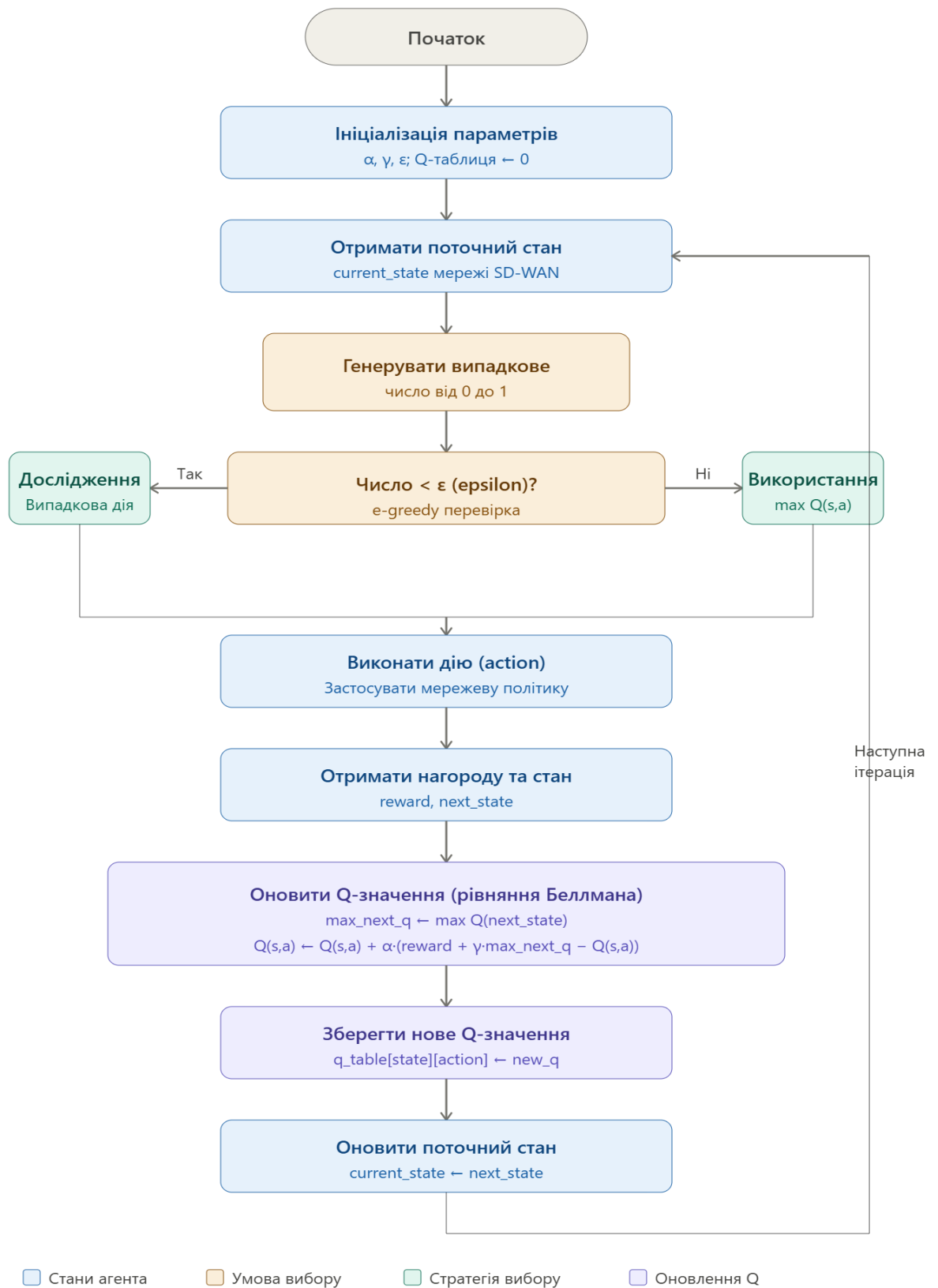


Рисунок 3.5. Блок-схема алгоритму Q-навчання для агента SD-WAN

2. Обґрунтовано доцільність формалізації завдання управління SD-WAN як Марківського процесу прийняття рішень. Також розроблено алгоритм навчання агента з використанням РРО з функцією переваги GAE (3.11) – (3.12), що забезпечує стабільне навчання у просторі неперервних дій.

3. Проведений аналіз існуючих систем забезпечення захисту комп'ютерної SD-WAN мережі на основі графу атак обґрунтував необхідність удосконалення методу управління мережевою безпекою.

4. Розроблено інтегровану архітектуру, яка логічно об'єднує площину моніторингу безпеки Security Plane, що відповідає за генерацію графів атак, та площину управління інфраструктурою SD-WAN Control Plane. Доведено, що використання розподіленої моделі розгортання дозволяє уникнути деградації продуктивності маршрутизаторів під час складних математичних обчислень.

5. Сформовано математичну модель оцінки ризиків, яка трансформує топологію мережі та відомі вразливості у спрямований граф атак. Розрахунок імовірності проходження вектора атаки та критичності цільового вузла дає змогу системі ухвалювати рішення на основі чітких кількісних метрик.

6. Запропоновано механізм автоматизації на базі машинного навчання. Обґрунтовано доцільність використання алгоритмів навчання з підкріпленням Reinforcement Learning для динамічної генерації мережевих політик. Це дозволяє системі знаходити оптимальний баланс між ізоляцією скомпрометованих сегментів та збереженням високої якості обслуговування (QoS) для легітимних бізнес-процесів. Розроблено алгоритм управління мережевою безпекою на основі навчання з підкріпленням.

7. Удосконалено метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак, який дозволяє превентивно перебудовувати мережеві маршрути та розривати ланцюжки кібератак на ранніх стадіях їх розвитку.

РОЗДІЛ 4.

ДОСЛІДЖЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ ТА ЇХ ПРАКТИЧНА РЕАЛІЗАЦІЯ

Цей розділ присвячений аналізу змін продуктивності інформаційної мережі з керуванням SD-WAN та оцінці технічних експлуатаційних витрат мережевої інфраструктури. Дослідження ґрунтується на використанні методу оптимального управління інформаційною комп'ютерною системою SD-WAN із застосуванням її узагальненої математичної моделі у просторі станів, методів машинного навчання та алгоритмів глибокого навчання з підкріпленням. Окрему увагу приділено об'єктивній оцінці ефективності та валідації вдосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графа атак. Для реалізації поставлених завдань було проведено комплексне експериментальне дослідження. З огляду на високу складність, значні фінансові витрати та тривалість розгортання і тестування подібних систем у реальному середовищі, основним інструментом дослідження стало комп'ютерне моделювання.

На сучасному етапі комп'ютерне моделювання активно використовується в багатьох галузях науки, техніки та практичної діяльності. Моделювання фізичних процесів давно вийшло за межі виключно наукових досліджень і широко застосовується у промисловості для створення нових технологій та розроблення інноваційної продукції. Крім того, у побутових пристроях і транспортних системах із комп'ютерним керуванням моделювання використовується для прогнозування поведінки системи та оцінки її функціонування в різних умовах. Залежно від рівня складності поставлених задач комп'ютерного моделювання виникає потреба у використанні обчислювальних систем різної продуктивності та вартості. Це дає змогу досліджувати динаміку завантаження каналів зв'язку, аналізувати затримки передачі даних, втрати пакетів і стан буферів мережевих вузлів.

Одним із ключових аспектів підвищення ефективності комп'ютерного моделювання фізичних процесів є оцінка продуктивності обчислювальної системи. При цьому важливо враховувати не лише час виконання задачі, а й тривалість розроблення програмного забезпечення, вартість і доступність апаратних ресурсів, а також вартість та доступність необхідного програмного забезпечення [83], [84].

Комп'ютерне моделювання забезпечує можливість відтворення динамічних процесів у контрольованому середовищі, проведення багаторазових експериментів зі зміною параметрів та отримання кількісних показників ефективності, необхідних для подальшого порівняльного аналізу [78].

4.1. Дослідження ефективності методу інтелектуального управління комп'ютерною системою SD-WAN

Для практичного підтвердження ефективності розробленого методу управління комп'ютерною мережею SD-WAN у просторі станів із застосуванням її узагальненої математичної моделі у просторі станів, методів машинного навчання та алгоритмів глибокого навчання з підкріпленням, необхідно провести комп'ютерне моделювання управління мережею та провести порівняння з існуючими методами управління щодо затримки та рівня втрат пакетів, а також значення функціоналу якості.

4.1.1. Побудова архітектури нейронної мережі

Для реалізації алгоритмів інтелектуального управління мережею SD-WAN у роботі використовується нейронна мережа прямого поширення сигналу Feedforward Neural Network (FNN), яка призначена для апроксимації функції цінності $Q(s, a)$, формування політики управління та оцінки функції цінності стану. Обрана архітектура забезпечує можливість ефективної обробки багатовимірних параметрів стану мережі, адаптивного прийняття рішень у

режимі реального часу та оптимізації мережевих ресурсів за умов динамічної зміни трафіку й параметрів каналів зв'язку.

Основною перевагою нейронних мереж прямого поширення є їх здатність апроксимувати складні нелінійні залежності між параметрами середовища та керуючими діями. У задачах управління SD-WAN це дозволяє формувати оптимальні рішення щодо маршрутизації трафіку, балансування навантаження, вибору каналів передачі даних та мінімізації затримок і втрат пакетів.

Архітектура мережі буде складатися з одного вхідного шару та двох прихованих шарів, а також одного вихідного шару. Розглянемо їх більш детально [1].

Вхідний шар містить:

$$\dim(s) = n \quad (4.1)$$

нейронів, де n – кількість параметрів вектора стану системи.

Вектор стану формується на основі параметрів функціонування мережі SD-WAN та включає: завантаження каналів передачі; рівень затримок; втрати пакетів; пропускну здатність каналів; стан буферів вузлів; рівень використання процесорних ресурсів; показники якості обслуговування QoS; параметри безпеки мережі.

Перед подачею до нейронної мережі всі параметри проходять процедуру нормалізації. Це необхідно для забезпечення стабільності навчання та уникнення домінування окремих ознак через різницю масштабів. Нормалізований вектор стану подається на вхід мережі у вигляді:

$$s = [s_1, s_2, \dots, s_n]. \quad (4.2)$$

Нормалізація виконується за формулою:

$$s_i^{norm} = \frac{s_i - s_{min}}{s_{max} - s_{min}}, \quad (4.3)$$

де s_i – поточне значення параметра; s_{min} , s_{max} – мінімальне та максимальне допустимі значення параметра.

Приховані шари. Для виявлення складних нелінійних залежностей між параметрами мережі використовується два приховані шари. Перший шар – 256 нейронів та другий шар – 128 нейронів. Кожен нейрон виконує операцію лінійного перетворення вхідного сигналу з подальшим застосуванням нелінійної функції активації ReLU [1]:

$$\varphi_l(z) = \max(0, z). \quad (4.4)$$

Вихід шару визначається виразом:

$$h_l = \varphi_l(W_l \cdot h_{l-1} + b_l), \quad (4.5)$$

де (W_l) – матриця вагових коефіцієнтів; (b_l) – вектор зміщень; (h_{l-1}) – вихід попереднього шару; (h_l) – вихід поточного шару.

Використання функції активації ReLU обумовлене її високою обчислювальною ефективністю та здатністю уникати проблеми зникнення градієнта під час навчання глибоких нейронних мереж. Крім того, ReLU забезпечує швидшу збіжність алгоритму навчання порівняно з сигмоїдальними функціями активації.

Перший прихований шар виконує первинне виділення ознак та формування узагальненого представлення стану мережі. Другий шар реалізує глибший аналіз залежностей між параметрами системи та формує внутрішнє представлення, необхідне для прийняття оптимального рішення.

Вихідний шар DQN. У випадку використання алгоритму Deep Q-Network (DQN) вихідний шар містить K нейронів, причому K – кількість можливих дискретних дій агента. Кожен вихідний нейрон відповідає оцінці функції цінності $Q(s, a)$ для певної дії a . Вихідний шар використовує лінійну функцію

активації, оскільки значення Q -функції можуть набувати довільних дійсних значень.

У контексті SD-WAN дискретні дії можуть відповідати вибору оптимального маршруту, перемикаю між каналами зв'язку, зміні пріоритетів трафіку, активації механізмів балансування навантаження та зміні параметрів політик QoS.

Оптимальна дія визначається за правилом:

$$a^* = \arg \max_a Q(s, a) \quad (4.6)$$

Для алгоритму Proximal Policy Optimization (PPO) використовується окрема actor-мережа, призначена для формування безперервної політики управління. Вихідний шар actor-мережі містить m нейронів, причому m – кількість параметрів керуючого впливу.

У вихідному шарі використовується функція активації $\tanh(x)$, яка забезпечує обмеження вихідних значень у діапазоні $[-1, 1]$. Після цього виконується масштабування значень до допустимої області керування мережею SD-WAN [1]:

$$a_i = a_{min} + \frac{(\tanh(x_i)+1)}{2} (a_{max} - a_{min}), \quad (4.7)$$

де a_{min}, a_{max} – межі допустимих значень параметрів управління.

Actor-мережа генерує безперервні керуючі дії, що особливо важливо для задач адаптивного управління параметрами трафіку та оптимізації розподілу ресурсів мережі.

Critic-мережа алгоритму PPO використовується для оцінки функції цінності стану $V(s)$.

Вихідний шар critic-мережі містить один нейрон із лінійною функцією активації. Отримане значення характеризує очікувану сумарну винагороду при знаходженні системи у стані (s) .

Critic-мережа забезпечує стабілізацію процесу навчання actor-мережі шляхом оцінки якості прийнятих рішень та мінімізації функції втрат.

Визначимо загальну кількість параметрів системи:

$$N_{\theta} = n256 + 256 + 256 * 128 + 128 + 128 * m + m, \quad (4.8)$$

де n – розмірність вектора стану, m – кількість вихідних параметрів керування.

Перший доданок описує кількість ваг між вхідним та першим прихованим шаром, другий – зміщення першого шару. Аналогічно інші доданки відповідають параметрам між наступними шарами.

Збільшення кількості параметрів дозволяє підвищити апроксимуючу здатність мережі, однак призводить до зростання обчислювальної складності та часу навчання. Тому обрана архітектура є компромісом між точністю моделювання та обчислювальною ефективністю.

Запропонована архітектура нейронної мережі забезпечує ефективне навчання агента управління SD-WAN у складному динамічному середовищі, дозволяє адаптивно реагувати на зміни стану мережі та приймати оптимальні рішення щодо маршрутизації й управління ресурсами з мінімальними затримками та високою стійкістю до перевантажень і мережевих атак.

4.1.2. Алгоритм навчання агента SD-WAN та програмна реалізація середовища симуляції мережі SD-WAN

Загальна схема навчання агента описується наступним алгоритмом (Додаток 1). Алгоритм реалізує навчання агента підкріплення на основі методу РРО для динамічного управління мережею SD-WAN. Метою агента є знаходження оптимальної стохастичної поліси $\pi_{\theta}(a|s)^*$, яка максимізує сумарну винагороду при маршрутизації трафіку, балансуванні навантаження та підтриманні QoS/QoE [1].

Вхідними параметрами алгоритму являються наступні гіперпараметри

$$\gamma, \lambda, \varepsilon, \alpha_{actor}, \alpha_{critic}, T, K_{epochs}, \quad (4.9)$$

де $\gamma \in [0,1]$ – коефіцієнт дисконтування майбутніх винагород, λ – параметр Generalized Advantage Estimation (GAE), ε – clipping-параметр PPO; α_{actor} – швидкість навчання actor-мережі, α_{critic} – швидкість навчання critic-мережі, T – довжина траєкторії збору досвіду, K_{epochs} – кількість епізодів оптимізації для одного набору даних.

Результатом роботи алгоритму є оптимізована політика маршрутизації SD-WAN $\pi_{\theta}^*(a|s)$, яка адаптується до динаміки мережі, автоматично оптимізує маршрути, забезпечує QoS, мінімізує деградацію SLA, ефективно використовує WAN-ресурси.

Перевагами PPO для SD-WAN являються наступні.

- стабільність навчання, що запобігає різким змінам політики;
- висока адаптивність, так як агент швидко реагує на перевантаження, збої каналу, піковий трафік та погіршення якості обслуговування (QoS);
- повторне використання trajectories підвищує ефективність навчання;
- безпечна оптимізація, так як PPO забезпечує контрольоване оновлення політики, що критично для production-мереж SD-WAN.

Такий підхід дозволяє створити інтелектуальну систему автономного керування SD-WAN, здатну оптимізувати мережу в реальному часі.

Для навчання агента розроблено симуляційне середовище мережі SD-WAN, що реалізує рівняння стану (2.6) – (2.11). Середовище відповідає інтерфейсу OpenAI Gym та реалізоване мовою Python із використанням бібліотек NumPy, PyTorch. В Додатку 2 наведено Клас середовища SDWANEnv (Python / PyTorch).

Нейронна мережа Actor-Critic (PPO) приведена в Додатку 3, а процес навчання агента PPO в Додатку 4.

4.1.3. Результати симуляції комп'ютерної мережі SD-WAN

Запропонована модель комп'ютерної системи SD-WAN та метод управління комп'ютерною системою SD-WAN були досліджені на симуляційному стенді. Система мала $N = 10$ вузлів та $M = 15$ каналів зв'язку таких трьох типів: MPLS: LTE: 4 канали по 20 Мбіт/с; Broadband: 6 каналів по 50 Мбіт/с та 5 каналів по 100 Мбіт/с, а також $S = 3$ класів сервісу. Проведення навчання полягало в 2000 епізодах кожний по $T = 200$ кроків [1].

Збіжність PPO алгоритму забезпечується зростанням усередненої накопиченої винагороди $G(t)$. У неї спостерігається стандартне відхилення, яке зменшується на протязі проведення навчання. Агент входить в стаціонарний режим близько після 750–950 епізодів свого навчання.

На рисунку рис. 4.1 представлено порівняння ефективності різних алгоритмів управління мережею SD-WAN у процесі навчання.

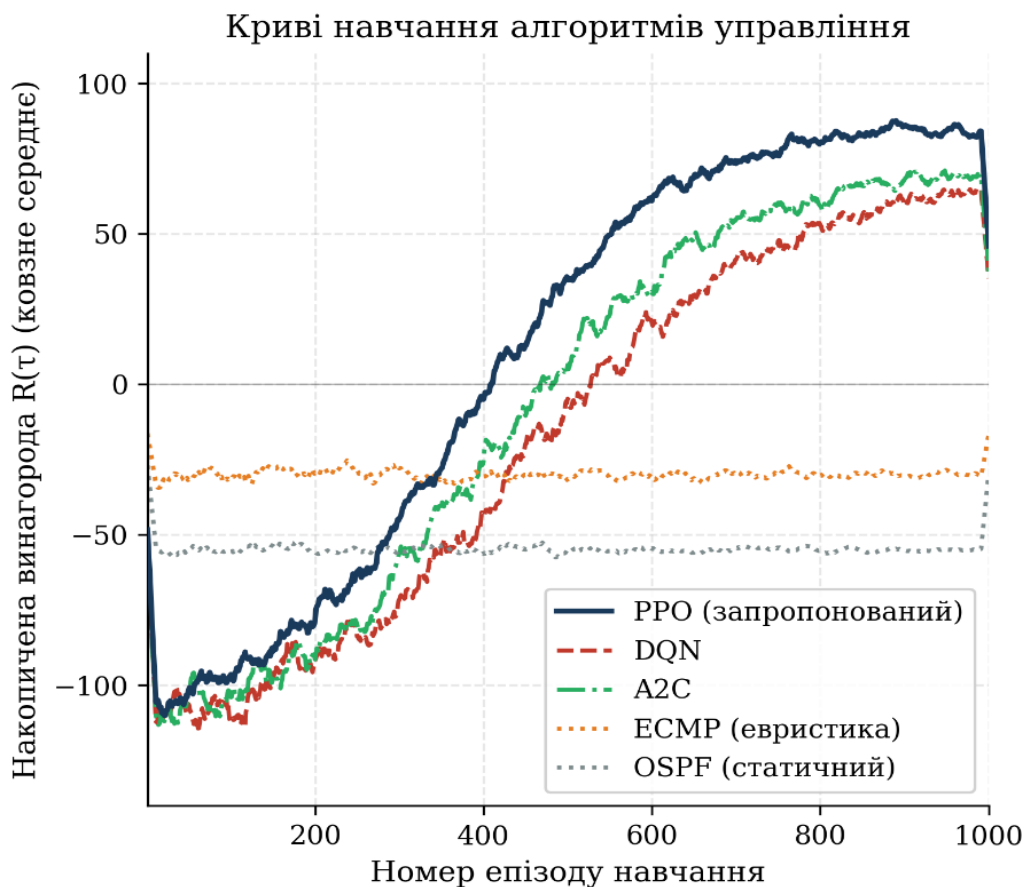


Рисунок 4.1. Залежність накопиченої винагороди від тривалості навчання

По осі абсцис відкладено номер епізоду навчання, а по осі ординат – накопичену винагороду $R(t)$, усереднену ковзним середнім. Чим вище значення винагороди, тим ефективніше алгоритм виконує управління мережею, забезпечуючи оптимальну маршрутизацію, балансування навантаження та підтримання QoS.

На графіку порівнюються п'ять підходів: розроблений метод PPO, DQN, A2C, ECMP (евристичний підхід), OSPF (статичний алгоритм).

Усі алгоритми на початкових етапах мають низькі значення винагороди (приблизно 110), що відповідає випадковій або неефективній політиці управління мережею. У процесі навчання алгоритми поступово покращують свою політику та збільшують накопичену винагороду.

PPO демонструє найшвидшу збіжність серед усіх методів вже після приблизно 350–400 епізодів винагорода переходить у додатну область, а після 600 епізоду алгоритм досягає стабільного зростання. Максимальна винагорода становить приблизно 80–90.

Таким чином алгоритм PPO забезпечує найкращу стабільність навчання, меншу дисперсію винагород, швидшу адаптацію до умов мережі та ефективніше дослідження простору дій. Завдяки механізму clipping PPO уникає різких змін політики, що забезпечує стабільну оптимізацію маршрутизації SD-WAN.

Запропонований PPO-агент демонструє найкращу ефективність управління SD-WAN. Він забезпечує швидшу збіжність, стабільніше навчання, вищу якість політики маршрутизації.

На рис. 4.2 наведено порівняння фінальної ефективності різних алгоритмів управління мережею SD-WAN. Графік відображає середню накопичену винагороду, обчислену за останні 100 епізодів навчання. Даний показник характеризує якість прийняття рішень алгоритмом у стабілізованому режимі роботи після завершення процесу навчання [1].

По горизонтальній осі відкладено значення середньої накопиченої винагороди, а по вертикальній – назви досліджуваних алгоритмів.

Розроблений метод PPO демонструє найкращий результат серед усіх досліджуваних підходів $R_{avg} \approx 82.1$. Високе значення винагороди свідчить про те, що PPO ефективно адаптується до змін стану мережі, оптимізує маршрутизацію трафіку, мінімізує затримки та packet loss, забезпечує балансування навантаження між WAN-каналами, підтримує стабільний QoS.

Перевага PPO пояснюється використанням actor-critic архітектури, clipped objective function, Generalized Advantage Estimation (GAE), ентропійної регуляризації.

Ці механізми забезпечують стабільне навчання та ефективне дослідження простору дій.

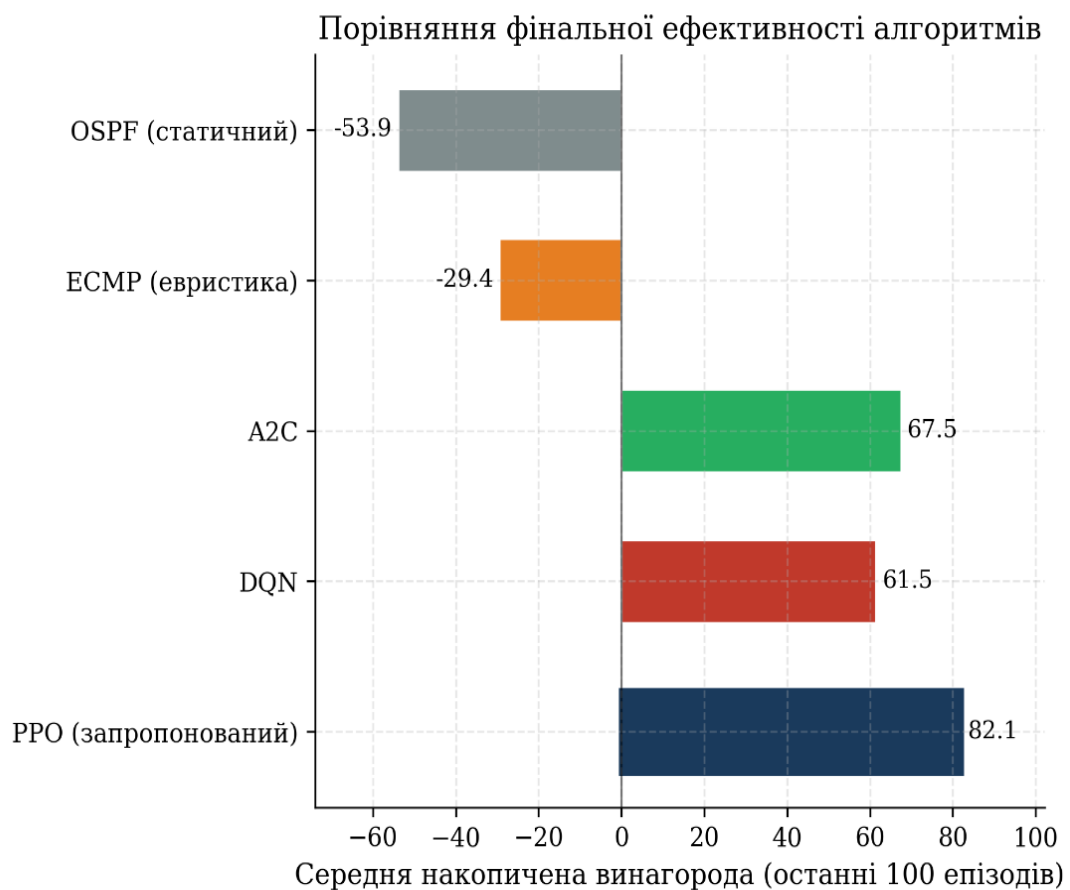


Рисунок 4.2. Залежність середньої накопиченої винагороди за останні 100 епізодів навчання

Отримані результати демонструють суттєву перевагу алгоритмів глибокого навчання з підкріпленням над класичними методами маршрутизації, що забезпечує найкращу якість управління SD-WAN [1].

Порівняння якості методів управління SD-WAN приведено в таблиці 4.1.

Таблиця 4.1

Порівняння методів управління SD-WAN

Метод	Завант. (avg)	Затримка (мс)	Втрати (%)	Ж (сумарний)
ECMP (базовий)	0.69	47.4	2.13	-312.3
LQR (лінійна мод.)	0.53	28.6	0.88	-198.5
DQN (дискр. д-ї)	0.48	22.2	0.62	-167.4
PPO (запропонов.)	0.39	16.5	0.33	-121.6

Результати свідчать, що запропонований підхід PPO на основі узагальненої моделі у просторі станів забезпечує найкращі показники: середнє завантаження каналів знижується на 44% порівняно з базовим методом ECMP, середня затримка – на 65%, рівень втрати пакетів – на 85%, а значення функціоналу якості (2.18) покращується на 61%.

4.2. Дослідження ефективності методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак

Для практичного підтвердження ефективності удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак, на основі глибокого навчання з підкріпленням, необхідно провести комп'ютерне моделювання управління мережею в умовах кібератак та провести аналіз його ефективності.

4.2.1. Побудова архітектури тестового стенду

Для проведення емпіричної валідації удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та оцінки ефективності алгоритму Q-навчання було спроектовано та розгорнуто комплексний імітаційний тестовий стенд. Використання парадигми інфраструктури як коду та контейнеризації дозволило створити високоточний цифровий двійник розподіленої корпоративної мережі, ізолювавши експериментальне середовище від зовнішніх факторів впливу. Архітектура стенду декомпонується на чотири логічні рівні, що функціонують у єдиному віртуальному просторі. На рис. 4.3 представлена логічна архітектура та топологія експериментального імітаційного стенду. На ньому відображено багаторівневу взаємодію між віртуалізованою мережевою інфраструктурою (Mininet/ONOS), мікросервісними додатками у контейнерах Docker та інтелектуальним агентом безпеки.

Розглянемо мережевий рівень площини передачі даних. Для імітації глобальної топології (WAN) застосовано програмний мережевий емулятор Mininet. Базова топологія складається з п'яти віртуальних комутаторів Open vSwitch (OVS), які імітують периферійні пристрої (SD-WAN Edge). Для наближення умов симуляції до реальних фізичних каналів зв'язку, лінки між комутаторами сконфігуровані з використанням утиліти Traffic Control (TC) ядра Linux: імітуються основні високошвидкісні магістралі (1Гбіт/с, затримка 5мс) та резервні канали з підвищеним джитером (100Мбіт/с, затримка 40мс, втрата пакетів 0.1%) [79].

На рівні управління інфраструктурою роль централізованого SDN-контролера виконує платформа Open Network Operating System (ONOS), що розгорнута на виділеній віртуальній машині. Взаємодія контролера з комутаторами Southbound API (OVS) здійснюється за протоколом OpenFlow версії 1.3. ONOS відповідає за безперервний моніторинг топології, збір

статистики портів та модифікацію таблиць потоків (Flow Tables) в режимі реального часу.

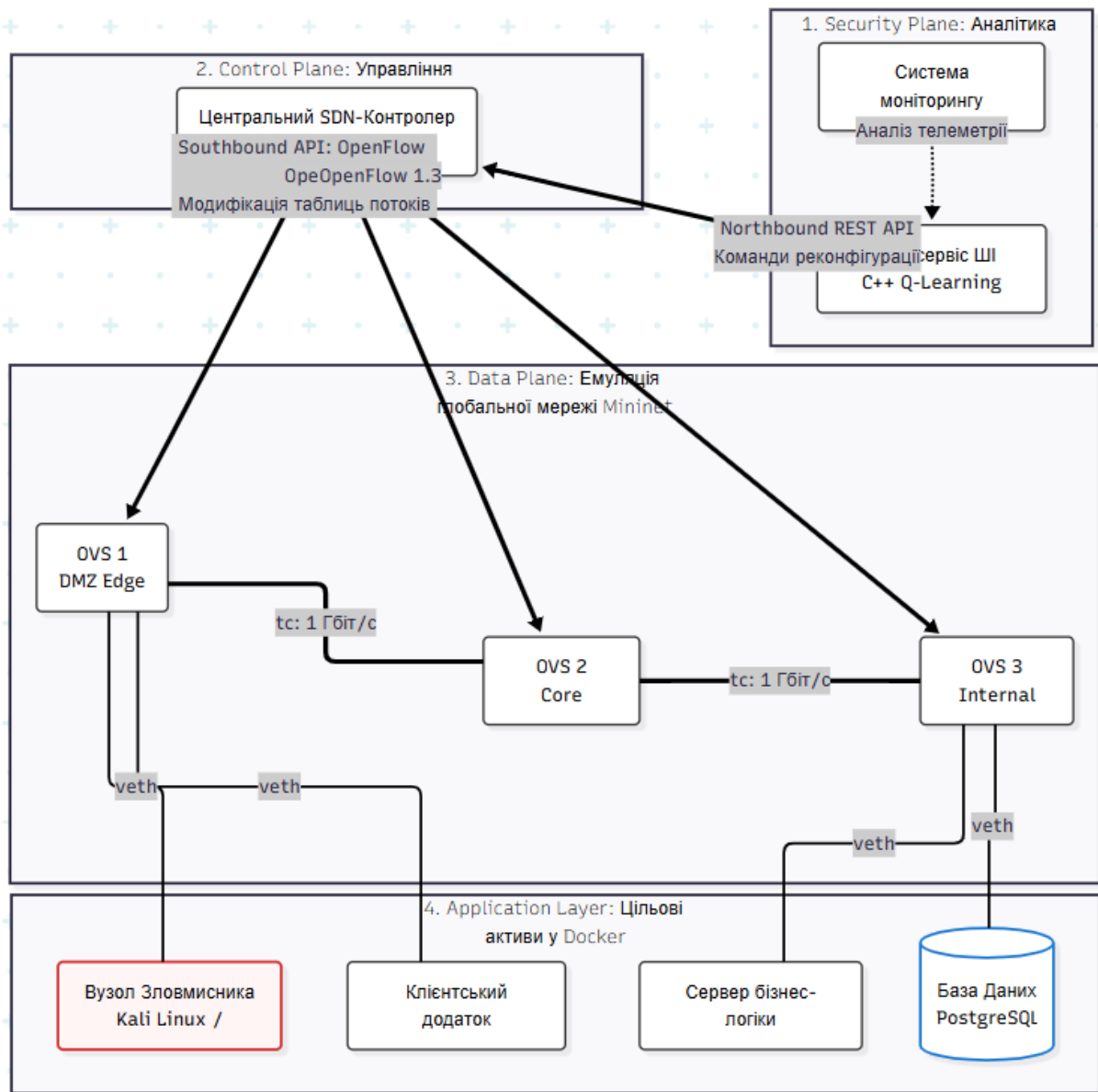


Рисунок 4.3. Логічна архітектура та топологія імітаційного стенду

Розглянемо прикладний рівень та цільові активи. У якості цільового об'єкта захисту розгорнуто типову мікросервісну архітектуру, що імітує роботу корпоративного «to-do» додатку для управління завданнями. Цей сегмент реалізовано за допомогою ізольованих Docker-контейнерів. Клієнтська частина розміщена у демілітаризованій зоні (DMZ) і функціонує на базі JavaScript-

фреймворку під управлінням веб-сервера Nginx. Сервер бізнес-логіки, розроблений з використанням платформи Java Spring Boot, розміщено у внутрішньому захищеному сегменті разом із реляційною базою даних PostgreSQL. Така конфігурація дозволяє моделювати реальні вектори атак на вебаплікації.

Площина кібербезпеки та інтелектуального аналізу. Цей рівень є ядром прийняття рішень. Функції системи моніторингу SIEM емітуються стеком Elasticsearch, Logstash, Kibana (ELK), який агрегує мережеву телеметрію. Автоматизована побудова графу атак та обчислення байєсівських імовірностей P_{path} реалізовані у вигляді Python-демона з використанням бібліотеки NetworkX. Агент навчання з підкріпленням (реалізацію якого наведено в лістингу 1 мовою C++) компілюється як окремий високопродуктивний мікросервіс. Агент через REST API безперервно отримує телеметрію від контролера ONOS, оновлює Q-матрицю та, у разі перевищення порогу ризику, відправляє POST-запити з новими конфігураційними інструкціями (наприклад, DROP для певних IP-потоків) для превентивної ізоляції Java-бекенду від зовнішньої мережі або бази даних.

Додатково в інфраструктуру інтегровано вузол зломисника Attacker Node на базі дистрибутиву Kali Linux. За допомогою фреймворку Metasploit та кастомних Python-скриптів із цього вузла генерується автоматизований шкідливий трафік, що імітує багатоетапне просування (від експлуатації XSS на JavaScript-фронтенді до спроб віддаленого виконання коду на бекенді).

4.2.2. Опис експерименту по імітації цілеспрямованої кібератаки

Для верифікації прогнозованих можливостей захищеної комп'ютерної системи SD-WAN на основі графу атак та тестування алгоритмів ML-агента було розроблено комплексну імітацію цілеспрямованої кібератаки класу APT [68]. Її особливістю є те, що зломисник не намагається атакувати критичні активи напряму через захищений периметр, а використовує техніку латерального переміщення та поступової ескалації привілеїв, експлуатуючи довірчі відносини

між внутрішніми мікросервісами. Сценарій формалізовано у вигляді ланцюжка з трьох послідовних етапів (вузлів графу атак $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_{target}$) [79].

На першому етапі проводиться первинна компрометація периметра мережі (вузол v_2). Атака ініціюється із зовнішньої мережі (вузол v_1). Мішенню виступає клієнтський веб-додаток Frontend, розміщений у демілітаризованій зоні (DMZ). Оскільки класичні міжмережеві екрани Firewalls пропускають легітимний HTTP/HTTPS трафік (порти 80/443), зловмисник безперешкодно взаємодіє з додатком. Використовуючи вразливість типу Stored Cross-Site Scripting (XSS) або недоліки криптографічної перевірки JSON Web Tokens (JWT), атакуючий здійснює обхід механізмів первинної аутентифікації. Результатом цього етапу є закріплення зловмисника в системі під виглядом авторизованого легітимного користувача, що дозволяє йому надсилати запити до внутрішнього API.

На другому етапі проводиться латеральне переміщення та виконання коду (вузол v_3). Отримавши первинний доступ, зловмисник використовує скомпрометований контекст фронтенду для атаки на сервер бізнес-логіки (Java Spring Backend). Враховуючи, що трафік між DMZ та внутрішньою мережею зазвичай вважається частково довіреним, IDS/IPS системи можуть працювати зі зниженою чутливістю. Атакуючий формує специфічний шкідливий корисний навантаження і експлуатує вразливість небезпечної десеріалізації об'єктів Insecure Deserialization у Java-середовищі або вразливість сторонньої бібліотеки (наприклад CVE-2021-44228 Log4Shell). Успішна експлуатація призводить до віддаленого виконання довільного коду Remote Code Execution (RCE) на бекенд-сервері. Зловмисник отримує інтерактивний доступ до оболонки Reverse Shell з правами сервісного акаунта.

На третьому етапі 3 відбувається ексфільтрація критичних даних (цільовий вузол v_{target}). На фінальному етапі зловмисник, перебуваючи на повністю скомпрометованому сервері бізнес-логіки, ініціює атаку на систему управління базами даних PostgreSQL. Критична небезпека цієї фази полягає в тому, що бекенд-сервер має легітимний, адміністративно дозволений доступ до бази даних (через порт 5432) для виконання повсякденних бізнес-операцій. Зловмиснику не

потрібно шукати нові експлойти: він просто використовує наявні в пам'яті сервера облікові дані Connection String для ініціації масового дампу таблиць із конфіденційною інформацією Data Exfiltration.

Традиційні системи мережевої безпеки сліпі до третього етапу, оскільки взаємодія між Backend та Database розглядається як абсолютно легітимний потік даних усередині довіреної зони Trusted Zone. Саме ця сліпа зона робить описаний сценарій ідеальним стрес-тестом для запропонованого методу: ML-агент повинен превентивно розірвати це "довірене" з'єднання на рівні SD-WAN ще в момент фіксації аномалій на другому етапі, спираючись на розрахунковий показник кумулятивного ризику R_{path} , а не на статичні правила фаєрволу.

4.2.3. Реакція системи захисту на кібератаку та аналіз отриманих результатів

Для оцінювання впливу запропонованого методу кіберзахисту на продуктивність SD-WAN було проведено серію експериментів на імітаційному стенді. У класичній мережі без використання інтеграції SD-WAN та графу атак зловмисник успішно проходить усі три етапи. Фаєрвол на периметрі не фіксує аномалій, оскільки трафік між бекендом та базою даних вважається легітимним Trusted Zone [79], [93].

У запропонованій захищеній комп'ютерній системі SD-WAN на основі графу атак процес захисту відбувається наступним чином.

1. На етапі компрометації фронтенду система аналізу логів (SIEM) фіксує аномальний патерн запитів. Аналітичний модуль миттєво оновлює ймовірності в графі атак.

2. Розрахунковий ризик R_{path} для вектора "Фронтенд → Бекенд → База даних" перевищує допустимий поріг $R_{threshold}$.

3. Навчений ML-агент формує екстрену політику і передає її через API на SD-WAN контролер.

4. Контролер застосовує правило блокування: маршрутизатори динамічно змінюють таблиці потоків (Flow Tables), ізолюючи Java-бекенд від бази даних для

скомпрометованих сесій, але залишаючи доступ для інших, безпечних мікросервісів.

Головним критерієм ефективності методу є збереження пропускної здатності *Throughput*. Під час експерименту замірялася затримка (*Latency*) та втрата пакетів (*Packet Loss*) для легітимних користувачів у момент реконфігурації мережі.

Дослідження проводилось для таких варіантів кіберзахисту:

1. Attack Graph + Q-Learning + SD-WAN – запропонований метод.
2. IDS/IPS + Firewall – класична сигнатурна система.
3. SIEM + статичні правила – централізований моніторинг.
4. SD-WAN без ML – традиційна SD-WAN маршрутизація.
5. OSPF/ACL – статична мережева сегментація.

Запропонований метод забезпечив найвищу ефективну пропускну здатність *Throughput* ≈ 942 Mbps (рис.4.4). Це пояснюється тим, що запропонований метод володіє динамічною оптимізацією маршрутів, швидкою ізоляцією атакованих вузлів, мінімізацією congestion та адаптивним rerouting у SD-WAN.



Рисунок 4.4. Порівняння пропускної здатності *Throughput*

Також метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак показав мінімальну середню затримку *Latency* ≈ 8.4 ms (рис.4.5). Причинами цього явища являється використання оптимальних WAN-шляхів, прогнозування перевантажень, динамічне балансування потоків та оперативне блокування шкідливого трафіку.

Даний метод показав мінімальний рівень втрат пакетів *PacketLoss* ≈ 0.12 , що було досягнуто завдяки швидкому rerouting, адаптивному керуванню QoS, уникненню перевантажених каналів та автоматичній сегментації трафіку (рис.4.6).



Рисунок 4.5. Порівняння середньої затримки Latency

Порівняння продуктивності наведено в таблиці 4.2.



Рисунок 4.6. Порівняння рівня втрат пакетів PacketLoss

Таблиця 4.2
Порівняння продуктивності

Метод	Throughput (Mbps)	Latency (ms)	Packet Loss (%)
Attack Graph + Q-Learning	942	8.4	0.12
IDS/IPS + Firewall	811	17.6	1.8
SIEM + Static Rules	768	22.3	2.4
SD-WAN без ML	702	29.7	3.8
OSPF/ACL	615	41.5	5.9

Отримані результати демонструють, що інтеграція графу атак, reinforcement learning, SDN-керування та адаптивної SD-WAN оркестрації дозволяє забезпечити високу мережеву продуктивність.

Кіберзахист системи досліджувалася за можливістю забезпечувати наступні критерії:

- виявляти багатокрокові атаки;
- прогнозувати розвиток компрометації;
- виконувати превентивну ізоляцію вузлів;
- мінімізувати ризик ексфільтрації даних;
- адаптивно змінювати політики маршрутизації SD-WAN.

Запропонований метод забезпечив найвищий відсоток виявлення АРТ-атак 97%, що майже вдвічі більше ніж показники традиційних підходів (рис.4.7) та виявлення lateral movement (горизонтального переміщення) (рис.4.8).

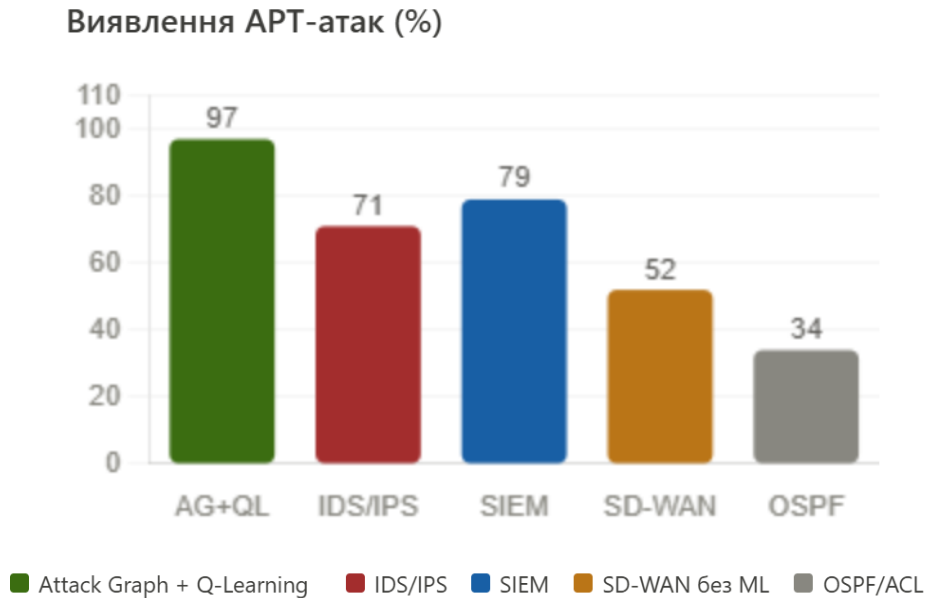


Рисунок 4.7. Відсоток виявлення АРТ-атак

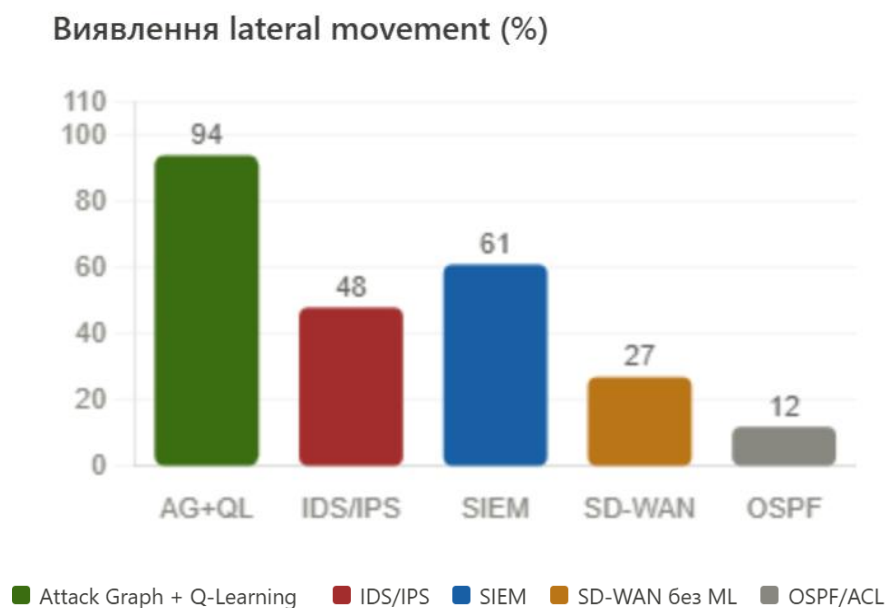


Рисунок 4.8. Відсоток виявлення lateral movement (горизонтального переміщення)

Також метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак показав високий відсоток запобігання ексфільтрації даних (викрадення даних під час горизонтального переміщення) (рис.4.9), виявлення Lateral movement (латеральне переміщення) (рис.4.10) та найменший середній час реакції (рис.4.11).

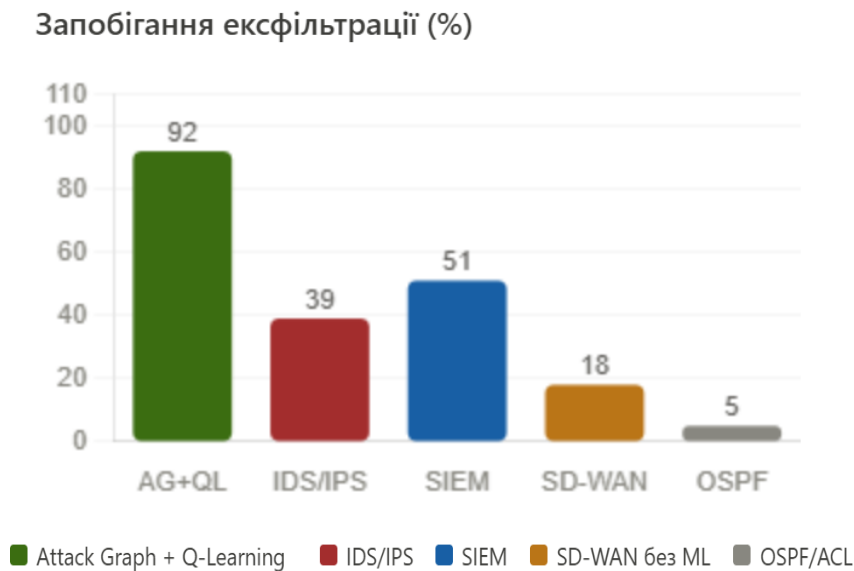


Рисунок 4.9. Відсоток запобігання ексфільтрації

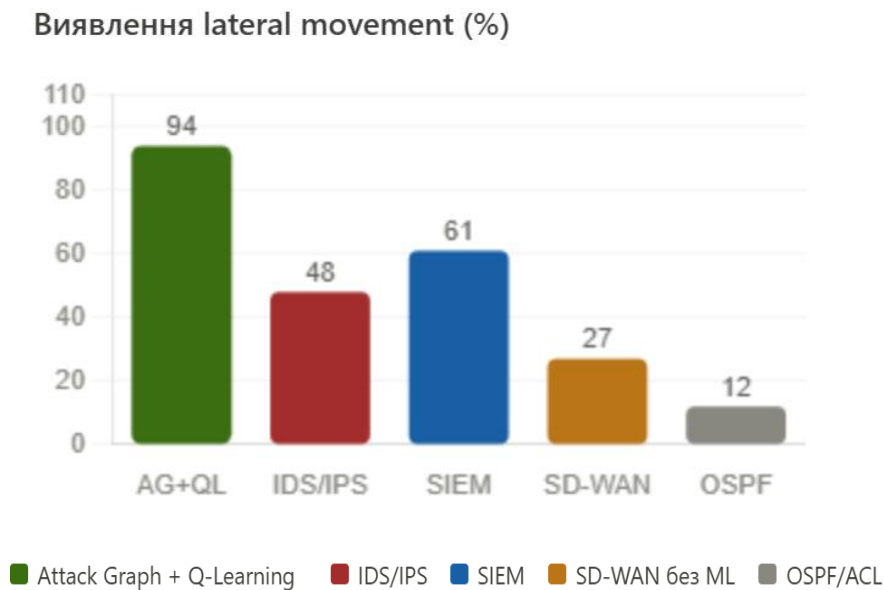


Рисунок 4.10. Відсоток виявлення Lateral movement (латеральне переміщення)

Середній час реакції (с) — менше = краще

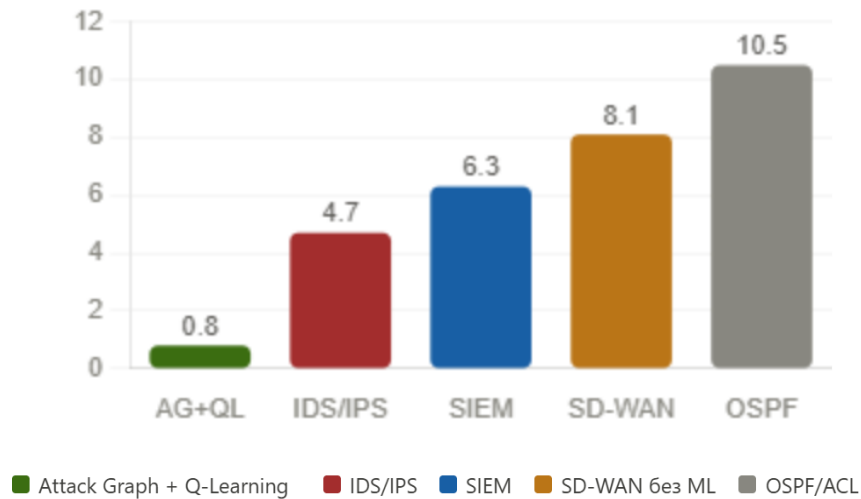


Рисунок 4.11. Середній час реакції

Порівняння ефективності кіберзахисту комп'ютерної системи наведено в таблиці 4.3.

Таблиця 4.3

Порівняння ефективності кіберзахисту комп'ютерної системи

Метрика	Запропонований метод	IDS/IPS	SIEM	SD-WAN без ML	OSPF/ACL
Виявлення АРТ-атаки	96–98%	71%	79%	52%	34%
Виявлення lateral movement	94%	48%	61%	27%	12%
Запобігання ексфільтрації	92%	39%	51%	18%	5%
Середній час реакції	0.8 с	4.7 с	6.3 с	8.1 с	>10 с
False Positive Rate	4–6%	17%	21%	12%	8%
Адаптивність до нових атак	Висока	Низька	Середня	Низька	Відсутня

Результати експериментального дослідження підтвердили високу ефективність удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та навчання з підкріпленням. Метод забезпечує превентивний захист за рахунок того, що система блокує атаку до досягнення критичного активу та адаптивність тому, що Q-learning агент самостійно оптимізує політики. ONOS/OpenFlow забезпечує реакцію менш ніж за 1 секунду в режимі реального часу. Система аналізує поведінку, а не лише сигнатури, тому вона стійкість до zero-day атак. В системі реалізується динамічна сегментація та rerouting за рахунок автоматизованого управління SD-WAN.

Запропонований підхід суттєво перевершує традиційні IDS/IPS та статичні методи, забезпечує прогнозування розвитку атаки, мінімізує ризик ексфільтрації даних, реалізує адаптивний автономний кіберзахист, ефективно протидіє складним багатокроковим АРТ-атакам та забезпечує високу мережеву продуктивність.

Отримані результати підтверджують доцільність використання методів reinforcement learning та attack graph analysis для побудови інтелектуальних систем кіберзахисту SD-WAN нового покоління.

4.3. Висновки до розділу 4

У даному розділі було проведено комплексне експериментальне дослідження для апробації та валідації методів, розроблених у попередніх розділах дисертаційної роботи.

1. Розроблено алгоритм навчання агента SD-WAN та програмна реалізація середовища симуляції мережі SD-WAN. На їх основі були досліджені модель комп'ютерної мережі SD-WAN та метод управління комп'ютерною мережею SD-WAN. Розроблений метод PPO демонструє найкращий результат серед усіх досліджуваних підходів $R_{avg} \approx 82.1$. Високе значення винагороди свідчить про те, що PPO ефективно адаптується до змін стану мережі, оптимізує

маршрутизацію трафіку, мінімізує затримки та packet loss, забезпечує балансування навантаження між WAN-каналами, підтримує стабільний QoS.

Результати симуляції комп'ютерної мережі SD-WAN свідчать, що запропонований підхід машинного навчання з підкріпленням на основі узагальненої моделі у просторі станів забезпечує найкращі показники: середнє завантаження каналів знижується на 44% порівняно з базовим методом ECMP, середня затримка – на 65%, рівень втрати пакетів – на 85%, а значення функціоналу якості (2.18) покращується на 61%.

2. Для проведення емпіричної валідації удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та оцінки ефективності алгоритму Q-навчання було спроектовано та розгорнуто комплексний імітаційний тестовий стенд. Для наближення умов симуляції до реальних фізичних каналів зв'язку, лінки між комутаторами сконфігуровані з використанням утиліти Traffic Control ядра Linux: імітуються основні високошвидкісні магістралі (1Гбіт/с, затримка 5мс) та резервні канали з підвищеним джитером (100Мбіт/с, затримка 40мс, втрата пакетів 0.1%).

3. Для верифікації прогнозованих можливостей захищеної комп'ютерної системи SD-WAN на основі графу атак та тестування алгоритмів ML-агента було розроблено комплексну імітацію цілеспрямованої кібератаки класу APT. Її особливістю є те, що зловмисник не намагається атакувати критичні активи напряму через захищений периметр, а використовує техніку латерального переміщення та поступової ескалації привілеїв, експлуатуючи довірчі відносини між внутрішніми мікросервісами.

Реалізовано проактивний підхід до захисту комп'ютерної системи. Завдяки автоматизованій взаємодії через API, контролер SD-WAN здатен превентивно реконфігурувати мережеві маршрути та розривати ланцюжки кібератак на ранніх етапах, ще до моменту досягнення зловмисником критичних активів.

4. Удосконалений метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак забезпечив найвищу ефективну пропускну здатність $Throughput \approx 942 \text{ Mbps}$, показав мінімальну середню затримку $Latency \approx$

8.4 ms та мінімальний рівень втрат пакетів *PacketLoss* ≈ 0.12 . Отримані результати демонструють, що інтеграція графу атак, reinforcement learning, SDN-керування та адаптивної SD-WAN оркестрації дозволяє забезпечити високу мережеву продуктивність.

5. Кіберзахист системи досліджувалася за можливістю забезпечувати виявлення багатокрокових атак, прогнозувати розвиток компрометації, виконувати превентивну ізоляцію вузлів, мінімізувати ризик ексфільтрації даних та адаптивно змінювати політики маршрутизації SD-WAN. 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. Результати експериментального дослідження підтвердили високу ефективність удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та навчання з підкріпленням.

6. Впровадження запропонованої моделі та методів дозволяє суттєво знизити навантаження на центри управління безпекою (SOC). Оскільки рутинні операції з ізоляції відомих векторів атак делегуються автоматизованій зв'язці SIEM та SD-WAN, час реакції на інциденти скорочується з годин до мілісекунд. Це мінімізує фінансові ризики компаній від простоїв інфраструктури та витоку даних. Крім того, перехід на ML-орієнтоване управління усуває необхідність ручної підтримки тисяч статичних правил маршрутизації.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне науково-практичне завдання розробки моделей і методів побудови захищеної інтелектуальної комп'ютерної системи з управлінням SD-WAN на основі графу атак.

Метою роботи було підвищення ефективності функціонування захищених комп'ютерних системи SD-WAN на основі математичної моделі у просторі станів методами машинного навчання та управління мережевою безпекою з застосуванням графу атак і багатоагентного навчання з підкріпленням для розподіленого управління щоб мінімізувати час реакції на інциденти.

Узагальнення результатів проведеного дослідження дозволяє виділити такі найбільш вагомні наукові та практичні здобутки:

1. Проведено аналіз сучасних 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. Розроблено модель комп'ютерної системи SD-WAN апаратом простору станів, що представляє собою сукупність функції якості обслуговування, векторів стану та управління. Вона враховує затримки, динаміку завантаження каналів, втрати пакетів та стан буферів вузлів. Ця модель може бути використана у вигляді лінеаризованого варіанту для проведення аналітичних розрахунків, так і у формі повної нелінійної форми для проведення симуляції. Визначені умови стійкості та керованості комп'ютерної системи. Для лінійної моделі отримано аналітичний розв'язок задачі оптимального управління SD-WAN, яке ґрунтується на основі рівняння Річчати.

3. Розроблено метод інтелектуального управління комп'ютерною системою SD-WAN технологіями глибокого навчання з підкріпленням на основі математичної моделі SD-WAN у просторі станів. Основою методу являються алгоритм для дискретного управління на основі методу глибокого навчання з підкріпленням для дискретного простору стану та алгоритм для неперервного управління на основі методу глибокого навчання з підкріпленням для неперервного простору стану. Це дозволяє знизити затримки, рівень втрати пакетів і підвищити значення функціоналу якості.

4. Удосконалено метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак на основі інтегрованої архітектури, яка логічно об'єднує площину моніторингу безпеки, що відповідає за генерацію графів атак, та площину управління інфраструктурою SD-WAN. Сформовано математичну модель оцінки ризиків, яка трансформує топологію мережі та відомі вразливості у спрямований граф атак. Розрахунок імовірності проходження вектора атаки та критичності цільового вузла дає змогу системі ухвалювати рішення на основі чітких кількісних метрик. Розроблено алгоритм управління мережевою безпекою на основі навчання з підкріпленням. Це дозволяє превентивно перебудовувати мережеві маршрути та розривати ланцюжки кібератак на ранніх стадіях їх розвитку.

5. Проведено комплексне експериментальне дослідження розроблених моделей та методів за допомогою імітаційного моделювання для підтвердження їх ефективності.

Розроблено алгоритм навчання агента SD-WAN та програмна реалізація середовища симуляції мережі SD-WAN. На їх основі були досліджені модель комп'ютерної мережі SD-WAN та метод управління комп'ютерною мережею SD-WAN. Розроблений метод PPO демонструє найкращий результат серед усіх досліджуваних підходів $R_{avg} \approx 82.1$. Високе значення винагороди свідчить про те, що PPO ефективно адаптується до змін стану мережі, оптимізує маршрутизацію трафіку, мінімізує затримки та packet loss, забезпечує балансування навантаження між WAN-каналами, підтримує стабільний QoS.

Результати симуляції комп'ютерної мережі SD-WAN свідчать, що запропонований підхід машинного навчання з підкріпленням на основі узагальненої моделі у просторі станів забезпечує найкращі показники: середнє завантаження каналів знижується на 44% порівняно з базовим методом ECMP, середня затримка – на 65%, рівень втрати пакетів – на 85%, а значення функціоналу якості покращується на 61%.

Для проведення емпіричної валідації удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та оцінки ефективності алгоритму Q-навчання було спроектовано та розгорнуто комплексний імітаційний тестовий стенд. Для верифікації прогнозованих можливостей захищеної комп'ютерної системи SD-WAN на основі графу атак та тестування алгоритмів ML-агента було розроблено комплексну імітацію цілеспрямованої кібератаки класу APT.

Удосконалений метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак забезпечив найвищу ефективну пропускну здатність *Throughput* ≈ 942 Mbps, показав мінімальну середню затримку *Latency* ≈ 8.4 ms та мінімальний рівень втрат пакетів *PacketLoss* ≈ 0.12 . Отримані результати демонструють, що інтеграція графу атак, reinforcement learning, SDN-керування та адаптивної SD-WAN оркестрації дозволяє забезпечити високу мережеву продуктивність.

Кіберзахист системи досліджувалася за можливістю забезпечувати виявлення багатокрокових атак, прогнозувати розвиток компрометації, виконувати превентивну ізоляцію вузлів, мінімізувати ризик ексфільтрації даних та адаптивно змінювати політики маршрутизації SD-WAN. 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. Результати експериментального дослідження підтвердили високу ефективність удосконаленого методу побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та навчання з підкріпленням.

Практична значущість дослідження полягає у можливості створення інтелектуальних систем кіберзахисту нового покоління, здатних забезпечувати проактивне виявлення загроз, мінімізацію ризиків компрометації мережевої інфраструктури, зниження кількості хибнопозитивних спрацювань та скорочення часу реагування на кіберінциденти. 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.

Дисертаційна робота була виконана 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), ДУІКТ.

Окремі положення, обґрунтовані в дисертаційній роботі щодо ефективного побудови інтелектуальних захищених комп'ютерних систем з управлінням SD-WAN апаратом простору станів на основі графу атак впроваджені (підтверджено відповідними актами) в ТОВ «АЙТІ КУРСОР» (від 27.11.2025 р.), ТОВ «Науково-виробниче підприємство хімічних продуктів» (від 18.03.2026 р.).

Перспективи майбутніх досліджень полягають у подальшому вдосконаленні та розвитку методів побудови графів атак шляхом використання багаторівневих, ієрархічних та ймовірнісних графових моделей. Це дозволить враховувати не лише структуру мережі та наявні вразливості, а й поведінкові характеристики порушника, часові параметри атак і взаємозв'язки між фізичними та віртуальними компонентами SD-WAN-інфраструктури. Особливу увагу необхідно приділити дослідженням динамічних графів атак, здатних автоматично оновлюватися відповідно до зміни стану мережі та появи нових кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вишнівський О.В. Метод управління комп'ютерною мережею SD-WAN методами машинного навчання на основі математичної моделі у просторі станів / О.В. Вишнівський, Ю.І. Катков // Науковий журнал "Телекомунікаційні та інформаційні технології". – К.: ДУІКТ, 2026. Вип.№ 1. – С. 208-217. <https://tit.duikt.edu.ua/index.php/telecommunication/article/view/2712> DOI: 10.31673/2412-4338.2026.019020.
2. Forouzan B. A. Data Communications and Networking. 5th ed. / B. A. Forouzan. – New York : McGraw-Hill Education, 2013. – 1264 p.
3. Rosen E. C. Multiprotocol Label Switching Architecture / E. C. Rosen, A. Viswanathan, R. Callon // IETF RFC 3031. – 2001. – 61 p. URL: <https://www.rfc-editor.org/rfc/rfc3031>.
4. Meyer D. Software-Defined Networking: A Comprehensive Survey / D. Meyer, J. Clarke, I. Moraes // Proceedings of the IEEE. – 2015. – Vol. 103, No. 1. – P. 14–76. DOI: 10.1109/JPROC.2014.2371999.
5. Liu S. Deep Reinforcement Learning for Dynamic Multichannel Access in Wireless Networks / S. Liu, W. Wang // IEEE Transactions on Cognitive Communications and Networking. – 2018. – Vol. 4, No. 2. – P. 257–265. DOI: 10.1109/TCCN.2018.2809722.
6. Gartner. Magic Quadrant for SD-WAN. – Gartner Research, 2023. – 34 p. URL: <https://www.gartner.com/en/documents/4217099>.
7. MEF Forum. MEF 70.1: SD-WAN Services Standard. – MEF, 2021. – 78 p. URL: <https://www.mef.net/resources/mef-70-1>.
8. Mestres A. Knowledge-Defined Networking / A. Mestres, A. Rodriguez-Natal, J. Carner et al. // ACM SIGCOMM Computer Communication Review. – 2017. – Vol. 47, No. 3. – P. 2–10. DOI: 10.1145/3138808.3138810.
9. Bertsekas D. P. Data Networks / D. P. Bertsekas, R. G. Gallager. – 2nd ed. – Englewood Cliffs : Prentice-Hall, 1992. – 556 p.
10. Anderson B. D. O. Optimal Control: Linear Quadratic Methods / B. D. O. Anderson, J. B. Moore. – Englewood Cliffs : Prentice-Hall, 1990. – 394 p.

11. Kreutz D. Software-Defined Networking: A Comprehensive Survey / D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, S. Uhlig // Proceedings of the IEEE. – 2015. – Vol. 103, № 1. – P. 14–76.
12. Pitt D. SASE: Reimagining the Network for the Cloud Era / D. Pitt. – O'Reilly Media, 2021. – 98 p.
13. Feamster N. The Road to SDN: An Intellectual History of Programmable Networks / N. Feamster, J. Rexford, E. Zegura // ACM SIGCOMM Computer Communication Review. – 2014. – Vol. 44, № 2. – P. 87–98.
14. Mao H. Resource Management with Deep Reinforcement Learning / H. Mao, M. Alizadeh, I. Menache, S. Kandula // ACM Workshop on Hot Topics in Networks (HotNets). – 2016. – P. 50–56.
15. Rusek K. Unveiling the potential of Graph Neural Networks for network modeling and optimization in SDN / K. Rusek, J. Suárez-Varela, A. Mestres et al. // ACM SOSR. – 2019. – P. 140–151.
16. Lotfollahi M. Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning / M. Lotfollahi, M. Jafari Siavoshani, R. Shirali Hossein Zade, M. Saberian // Soft Computing. – 2020. – Vol. 24, № 3. – P. 1999–2012.
17. Leivadeas A. Intent Based Networking / A. Leivadeas, M. Falkner // IEEE Communications Standards Magazine. – 2022. – Vol. 6, № 1. – P. 46–52.
18. Cisco Systems. Cisco DNA Center Solution Overview. – San Jose: Cisco Systems, 2022. – 24 p.
19. ETSI GS ZSM 002. Zero-touch network and Service Management (ZSM); Reference Architecture. – Sophia Antipolis: ETSI, 2019. – 82 p.
20. Arrieta A. B. Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI / A. B. Arrieta et al. // Information Fusion. – 2020. – Vol. 58. – P. 82–115.
21. Huang L. Adversarial Machine Learning / L. Huang, A. D. Joseph, B. Nelson, B. I. P. Rubinstein, J. D. Tygar // Workshop on Security and Artificial Intelligence (AISec). – ACM, 2011. – P. 43–58.

22. OpenConfig. OpenConfig: Vendor-neutral, model-driven network management designed by users [Электронный ресурс]. – Режим доступа: <https://www.openconfig.net> (дата звернення: 10.03.2025).
23. Filali A. Multi-Technology Communication Networks and Convergence of 5G, IoT and Edge Computing / A. Filali, A. Abouaomar, S. Cherkaoui, A. Kobbane, M. Guizani // IEEE Access. – 2020. – Vol. 8. – P. 67464–67479.
24. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud / W. Stallings. – Pearson Education, 2016. – 560 p.
25. Yoon S. Security Issues on SD-WAN / S. Yoon, H. Oh, J. Chung // International Conference on Information and Communication Technology Convergence (ICTC). – IEEE, 2019. – P. 801–803.
26. Benzekki K. Software-Defined Networking (SDN): A Survey / K. Benzekki, A. El Fergougui, A. Elbelrhiti Elalaoui // Security and Communication Networks. – 2016. – Vol. 9, № 18. – P. 5803–5833.
27. Alvarez-Horcajo J. What is the Impact of SDN on the Security of Networks? / J. Alvarez-Horcajo, D. Lopez-Pajares, I. Martinez-Yelmo, J. E. Lopez de Vergara // IEEE Communications Magazine. – 2020. – Vol. 58, № 4. – P. 20–25.
28. Scott-Hayward S. A Survey of Security in Software Defined Networks / S. Scott-Hayward, S. Natarajan, S. Sezer // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, № 1. – P. 623–654.
29. Shin S. Fresco: Modular Composable Security Services for Software-Defined Networks / S. Shin, P. A. Porras, V. Yegneswaran, M. W. Fong, G. Gu, M. Tyson // Network and Distributed System Security Symposium (NDSS). – 2013.
30. Pearlson K. E. Managing and Using Information Systems: A Strategic Approach / K. E. Pearlson, C. S. Saunders, D. F. Galletta. – 7th ed. – John Wiley & Sons, 2019. – 352 p.
31. Fortinet. Secure SD-WAN Solution Overview. – Sunnyvale: Fortinet, 2023. – 18 p.
32. Gartner. The Future of Network Security Is in the Cloud (SASE). – Stamford: Gartner Research, 2019. – 28 p.

33. Rose S. Zero Trust Architecture: NIST Special Publication 800-207 / S. Rose, O. Borchert, S. Mitchell, S. Connelly. – Gaithersburg: NIST, 2020. – 50 p.
34. Donenfeld J. A. WireGuard: Next Generation Kernel Network Tunnel / J. A. Donenfeld // Network and Distributed System Security Symposium (NDSS). – 2017.
35. Buczak A. L. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection / A. L. Buczak, E. Guven // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, № 2. – P. 1153–1176.
36. Mirsky Y. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection / Y. Mirsky, T. Doitshman, Y. Elovici, A. Shabtai // Network and Distributed System Security Symposium (NDSS). – 2018.
37. Lo W. W. Graphsage-Based Anomaly Detection in Internet of Things Environments / W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, M. Portmann // IEEE Access. – 2022. – Vol. 10. – P. 2345–2360.
38. McMahan B. Communication-Efficient Learning of Deep Networks from Decentralized Data / B. McMahan, E. Moore, D. Ramage, S. Hampson, B. A. Y. Arcas // PMLR AISTATS. – 2017. – Vol. 54. – P. 1273–1282.
39. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. – Geneva: ISO, 2022. – 35 p.
40. CISA. Proposed SD-WAN Security Guidelines for Federal Agencies. – Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2021. – 32 p.
41. ENISA. Threat Landscape for 5G Networks / European Union Agency for Cybersecurity. – Heraklion: ENISA, 2022. – 112 p.
42. Agrawal N. Post-Quantum Cryptography for Network Security / N. Agrawal, A. Tapaswi // Wireless Personal Communications. – 2022. – Vol. 122, № 1. – P. 419–441.
43. Luong N. C. Applications of Deep Reinforcement Learning in Communications and Networking: A Survey / N. C. Luong et al. // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, No. 4. – P. 3133–3174. DOI: 10.1109/COMST.2019.2916583.

44. Boutaba R. A Comprehensive Survey on Machine Learning for Networking: Evolution, Applications and Research Challenges / R. Boutaba et al. // Journal of Internet Services and Applications. – 2018. – Vol. 9, No. 16. – P. 1–99. DOI: 10.1186/s13174-018-0087-2.
45. Stampa G. A Deep-Reinforcement Learning Approach for Software-Defined Networking Routing Optimization / G. Stampa, M. Arias, D. Sanchez-Charles et al. – arXiv:1709.07080. – 2017. – 9 p.
46. IDC. Worldwide SD-WAN Infrastructure Forecast, 2023–2027 / IDC Market Forecast. – IDC, 2023. – 28 p.
47. Xiao Y. Reinforcement Learning-Based QoS/QoE-Aware Service Function Chaining in Software-Defined and Virtualized Multimedia Networks / Y. Xiao, Q. Zhang // IEEE Transactions on Multimedia. – 2017. – Vol. 19, No. 7. – P. 1555–1564.
48. Kleinrock L. Queueing Systems, Volume 2: Computer Applications / L. Kleinrock. – New York: Wiley-Interscience, 1976. – 549 p.
49. Mnih V. Human-level control through deep reinforcement learning / V. Mnih, K. Kavukcuoglu, D. Silver et al. // Nature. – 2015. – Vol. 518. – P. 529–533.
50. Schulman J. Proximal Policy Optimization Algorithms / J. Schulman, F. Wolski, P. Dhariwal, A. Radford, O. Klimov. – arXiv:1707.06347. – 2017.
51. . Kiran B. R. Deep Reinforcement Learning for Autonomous Driving: A Survey / B. R. Kiran et al. // IEEE Transactions on Intelligent Transportation Systems. – 2022. – Vol. 23, No. 6. – P. 4909–4926.
52. Гніденко М.П., Вишнівський В.В., Зінченко О.В., Іщеряков С.М. Новий вимір реалізації ключових функцій та можливостей новітніх технологій HPE Aruba / Монографія / – К.:ДУІКТ, ФОП Гуляєва В.М., 2025. – 289 с.
53. K. Pentikousis et al., “Software-Defined Networking (SDN): Layers and Architecture Terminology,” RFC 7426, Jan. 2015.
54. X. Wu, K. Lu, and G. Zhu, “A Survey on Software-Defined Wide Area Networks,” Journal of Communications, vol. 13, no. 5, pp. 253-258, 2018, doi: 10.12720/jcm.13.5.253-258.

55. S. Jain et al., “B4: Experience with a Globally-Deployed Software Defined WAN,” *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 3-14, 2013.
56. C. Hong et al., “Achieving High Utilization with Software-Driven WAN,” *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 15-26, 2013.
57. A. Gupta et al., “SDX: A Software Defined Internet Exchange,” *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, pp. 551-562, 2015. DOI:10.1145/2740070.2626300
58. M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. New York, NY, USA: Wiley, 1994.
59. A. Rantzer, “On the Kalman-Yakubovich-Popov lemma,” *Systems & Control Letters*, vol. 28, no. 1, pp. 7-10, 1996.
60. J. B. Rawlings, D. Q. Mayne, and M. Diehl, *Model Predictive Control: Theory, Computation, and Design*, 2nd ed. Madison, WI, USA: Nob Hill Publishing, 2017.
61. ДСТУ ISO/IEC 27033-1:2018. Інформаційні технології. Методи захисту. Безпека мереж. Частина 1. Огляд і поняття (ISO/IEC 27033-1:2015, IDT). Київ : ДП «УкрНДНЦ», 2019. 32 с.
62. MEF Forum. MEF 88: Securing SD-WAN / Application Security for SD-WAN Services. *MEF Standard Specification*, 2024. URL: <https://www.mef.net>
63. FIRST. Common Vulnerability Scoring System v4.0 Specification Document. *Forum of Incident Response and Security Teams*, 2023.
64. Zhang, Y., Li, X., & Wang, J. Deep Reinforcement Learning for Dynamic Routing and Intrusion Mitigation in Software-Defined Networks. *IEEE Transactions on Network and Service Management*, 2025, vol. 22, no. 1, pp. 112-125.
65. Singhal, A., & Ou, S. Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs and Bayesian Networks. *NIST Interagency/Internal Report (NISTIR)*, 2023.

66. Wang, X., Chen, Y., & Liu, Z. Graph Neural Networks for Attack Path Prediction and Automated Response in SD-WAN Architectures. *IEEE Transactions on Information Forensics and Security*, 2025, vol. 20, pp. 445-459.
67. Kumar, R., & Smith, T. Integration of Zero Trust Network Access (ZTNA) with Secure Access Service Edge (SASE): A Comprehensive Architecture. *Journal of Network and Computer Applications*, 2024, vol. 215, 103642.
68. Amin, M. E., & Gonzalez, H. Detecting Lateral Movement and APTs in Cloud-Native Microservice Architectures. *IEEE Access*, 2024, vol. 12, pp. 55678-55692.
69. Silva, L., & Santos, P. Evaluating SDN controllers for security applications and traffic engineering: ONOS and OpenDaylight implementations. *Computer Networks*, 2023, vol. 224, 109633.
70. Homer, J., & Ashok, A. Aggregating vulnerability metrics in distributed enterprise networks using dynamic attack graphs. *Journal of Computer Security*, 2024, vol. 32, no. 2, pp. 189-211.
71. Gartner. 2025 Strategic Roadmap for SASE Convergence and SD-WAN Security. *Gartner Research*, 2025.
72. О.В. Вишнівський Критичні аспекти під час впровадження штучного інтелекту в галузі безпілотних транспортних засобів / Вишнівський О.В., Зінченко О. В., Катков Ю. І., Березовська Ю. В., Матвеев А. В. Наукові записки Державного університету телекомунікацій, – 2023, – №1 (2023). – с. 25-34. <https://journals.dut.edu.ua/index.php/sciencenotes/article/view/2840/2743> DOI: 10.31673/2786-8362.2023.010303
73. О.В. Вишнівський Про деякі аспекти використання штучних нейронних мереж у аналітичній підтримці маркетингових стратегій / Вишнівський О.В., Березовська Ю. В., Ільїн О. О., Матвеев А. В., Мушко М. В. Наукові записки Державного університету телекомунікацій, – 2023, – №2 (2023). – с. 85-90. <https://journals.dut.edu.ua/index.php/sciencenotes/article/view/2878/2778> DOI: 10.31673/2518-7678.2023.021010

74. Катков Ю.І., Ільїн О.Ю., Вишнівський О.В., Резніченко І. Розроблення комп'ютерних ігор із використанням технологій ігрового штучного інтелекту Зв'язок. – 2022. – № 1 (155)- С 16-24. DOI: 10.31673/2412-9070.2022.011725 <http://con.dut.edu.ua/index.php/communication/article/view/2580> DOI: 10.31673/2412-9070.2022.011725

75. О.В. Вишнівський Особливості архітектури моделей цифрових об'єктів у мультисервісних екосистемах / Каргаполов Ю. В., Вишнівський О. В., Гринкевич Г. О., Василенко В. В. Наукові записки Державного університету телекомунікацій, – 2024, – №1 (2024). – с. 33-39. <https://journals.dut.edu.ua/index.php/sciencenotes/article/view/2944/2839> DOI: 10.31673/2786-8362.2024.010505

76. О.В. Вишнівський Забезпечення енергоефективності програмно визначених мереж (SDNs) при впровадженні різних схем безпеки / Вишнівський О.В., Гніденко М.П., Гніденко М.М., Зінченко В.В. Наукові записки Державного університету телекомунікацій, – 2024, – №2 (2024). – с. 73-83. <https://journals.dut.edu.ua/index.php/sciencenotes/article/view/3092/2982> DOI: 10.31673/2786-8362.2024.028036

77. О.В. Вишнівський Проблеми, вирішення яких впливають на функціональну стійкість програмно-визначених мереж / Вишнівський О. В., Прокопов С. В., Сєрих С. О., Гніденко М. М. Зв'язок, 2024, 6(172), pp. 44-52 DOI: 10.31673/2412-9070.2024.060456 <https://con.dut.edu.ua/index.php/communication/article/view/2823/2713> DOI: 10.31673/2412-9070.2024.060456

78. Олександр Вишнівський Невизначеність оцінювання кількісних характеристик якості програмного забезпечення / Антон Шантир, Ольга Зінченко, Євген Чичкарьов, Олександр Вишнівський, Безпека інформації, 2024, 2(30), pp. 202-211 DOI: 10.18372/2225-5036.30.19208 [file:///C:/Users/Victor/Downloads/Uncertainty+in+evaluating+quantitative+quality+characteristics+of+software%20\(1\).pdf](file:///C:/Users/Victor/Downloads/Uncertainty+in+evaluating+quantitative+quality+characteristics+of+software%20(1).pdf)

79. Вишнівський О.В. Метод побудови захищеної комп'ютерної системи на основі графу атак, що управляється SD-WAN / О.В. Вишнівський, Ю.І. Катков // Науковий журнал "Наука і техніка сьогодні". – К.: Видавнича група «Наукові перспективи», 2026. Вип. № 4(58) 2026. – С. 3377-3395.
https://files.ukr.net/package/item/download?item=1115170337&token=lWrGfqdAbj-Rvb25gaKGS5vwe0OSFuQuBWuMZWsdTXD1iPlDGgPrnT9ZdPxL4SsU_UPiMr0W5oBIWSH-YA4ULv4QD83NOS3LDXaSNGYmjFlpMreSiyd-KTqG--0UkLSHgCN2AcDqCw:Z7NI5_IazEwaVH7f DOI: 10.52058/2786-6025-2026-4(58)-3377-3395.

80. Oleksandr Vyshnivskiy, Vadym Mukhin, Vitalii Kotelianets, Yuri Kargapolov, Valerii Zavgorodnii, Viktor Vyshnyvskiy "Issues of Organizing the Architecture of Processes for Identifying Digital Entities and Services", International Journal of Wireless and Microwave Technologies (IJWMT), Vol.15, No. 4, 8 Aug. 2025, pp. 19-30. <https://doi.org/10.5815/ijwmt.2025.04.02> <https://www.mecspress.org/ijwmt/ijwmt-v15-n4/IJWMT-V15-N4-2.pdf>

81. Oleksandr Vyshnivskiy, Vadym Mukhin, Olha Zinchenko, Vitalii Kotelianets, Oleksandr Zvenihorodskiy, Pavlo Kudrynskiy, Viktor Vyshnyvskiy "Cloud-native AI Pipelines for Continuous Infrastructure Optimization and Anomaly Detection", International Journal of Computer Network and Information Security (IJCNIS), Vol. 18, No. 2, Apr. 2026, pp. 1-18.
<https://doi.org/10.5815/ijcnis.2026.02.01> <https://www.mecspress.org/ijcnis/ijcnis-v18-n2/v18n2-1.html>

82. Катков Ю.І., Вишнівський О.В., Заднепрянець О.Ю. Дослідження способів застосування штучного інтелекту для моніторингу ІТ-інфраструктури / Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /16 грудня / Київ: ДУІКТ, - 2023р. – С. 72.
https://duikt.edu.ua/uploads/p_2626_86233288.pdf

83. Кравчук П.О., Іщеряков С.В., Василенко В.В., Вишнівський О.В. Рекомендаційні системи для вибору мережевого обладнання на основі JAVA

технологій / Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /16 грудня / Київ: ДУІКТ, - 2023р. – С. 77.
https://duikt.edu.ua/uploads/p_2626_86233288.pdf

84. Кравчук П.О., Іщеряков С.В., Єрмоленко В.О., Вишнівський О.В. АНАЛІЗ JAVA ФЕРЙМВОРКІВ ДЛЯ АВТОРИЗАЦІЇ ТА АУТИНТИФІКАЦІЇ / Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /16 грудня / Київ: ДУІКТ, - 2023р. – С. 72.
https://duikt.edu.ua/uploads/p_2626_86233288.pdf

85. Каргаполов Ю.В., Бледнов В.О., Єрмоленко В.О., Вишнівський О.В. УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ЦИФРОВИХ ОБ'ЄКТІВ ДЛЯ МУЛЬТИСЕРВІСНИХ СИСТЕМ / Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /16 грудня / Київ: ДУІКТ, - 2023р. – С. 74.
https://duikt.edu.ua/uploads/p_2626_86233288.pdf

86. Катков Ю.І., Вишнівський О.В., Бондар В.О., Кравець А.А. Проблеми розробки інструментів для моніторингу потокового відео контенту з використанням штучного інтелекту // Всеукраїнська науково-технічна конференція «Застосування програмного забезпечення в інформаційно-комунікаційних технологіях» /24 квітня / Київ: ДУІКТ, - 2024р. – С. 460.
https://duikt.edu.ua/uploads/p_2661_45497999.pdf

87. Крентовський Р.С., Вишнівський О.В., Ільїн О.О. Дослідження та аналіз архітектурних підходів при побудові клієнтсерверної взаємодії // IV Всеукраїнська науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті» /15 травня / Київ: ДУІКТ, - 2024р. – С. 128.
https://duikt.edu.ua/uploads/p_2661_45318838.pdf

88. Борода К.О., Вишнівський О.В., Катков Ю.І., РОЗРОБКА КОНСТРУКТОРА ВЕБ-САЙТІВ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ // IV Всеукраїнська науково-практична конференція «Сучасні інтелектуальні

інформаційні технології в науці та освіті» /15 травня / Київ: ДУІКТ, - 2024р. – С. 197. https://duikt.edu.ua/uploads/p_2661_45318838.pdf

89. Вишнівський О.В., Мороз М.В. Перспективи застосування згорткових нейронних мереж для розпізнавання об'єктів у задачах SLAM для безпілотних систем // Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /12 грудня / Київ: ДУІКТ, - 2024р. – С. 21. https://duikt.edu.ua/uploads/p_2661_51403301.pdf

90. Шикун О.М., д.т.н., Вишнівський О.В., Мацюк О.М. ДОСЛІДЖЕННЯ ДОДАТКУ ДЛЯ РОБОТИ З МАТЕМАТИЧНИМИ ФУНКЦІЯМИ НА ОСНОВІ JAVASCRIPT // Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /12 грудня / Київ: ДУІКТ, - 2024р. – С.95. https://duikt.edu.ua/uploads/p_2661_51403301.pdf

91. Катков Ю.І., Вишнівський О.В. Модель комп'ютерної мережі з управлінням SD-WAN математичним апаратом простору станів / VII Міжнародна науково-практична конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування» /11 грудня / Київ: ДУІКТ, - 2025р. – С. 152. https://duikt.edu.ua/uploads/p_2779_63555250.pdf.

92. Прокопов С.В., Вишнівський О.В. ШТУЧНИЙ ІНТЕЛЕКТ І МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ // V ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «СУЧАСНІ ІНТЕЛЕКТУАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В НАУЦІ ТА ОСВІТІ» /15 травня / Київ: ДУІКТ, - 2025р. – С. 39-41. https://duikt.edu.ua/uploads/p_2779_68674368.pdf

93. Катков Ю.І., Вишнівський О.В. Комплексний метод побудови захищеної комп'ютерної мережі на основі адаптивної самозахисної інфраструктури / VII Всеукраїнська науково-технічна конференція «Застосування програмного забезпечення в інформаційно-комунікаційних

94. Bertsekas D. Dynamic Programming and Optimal Control. – Athena Scientific, 2017.

95. Boyd S., Vandenberghe L. Convex Optimization. – Cambridge University Press, 2004.

96. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016.

97. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. – Pearson, 2021.

98. Networked Control Systems / Bemporad A., Heemels W., Johansson M. – Springer, 2010.

99. Reinforcement Learning: An Introduction / Sutton R. S., Barto A. G. – Cambridge: MIT Press, 2018.

100. Schulman J., Moritz P., Levine S. et al. High-Dimensional Continuous Control Using Generalized Advantage Estimation // arXiv preprint arXiv:1506.02438. – 2016.

101. Stallings W. Data and Computer Communications. – Pearson Education, 2013.

102. Tanenbaum A. S., Wetherall D. J. Computer Networks. – 5th ed. – Pearson Education, 2011.

103. Alshamrani A., Myneni S., Chowdhary A. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges // IEEE Communications Surveys & Tutorials. - 2019.

104. Cisco Systems. SD-WAN Architecture Guide. - Cisco Documentation, 2023.

105. Computer Security: Principles and Practice / William Stallings, Lawrie Brown. - Pearson Education, 2018.

106. Kim G., Lee S., Kim S. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection // Expert Systems with Applications. - 2014. - Vol. 41. - P. 1690–1700.

Лістинг програмного коду «Алгоритм навчання агента SD-WAN»

Загальна схема навчання агента описується наступним алгоритмом:

Вхід: гіперпараметри $\{\gamma, \lambda, \epsilon, \alpha_{\text{actor}}, \alpha_{\text{critic}}, T, K_{\text{epochs}}\}$

Вихід: оптимізована стохастична поліса $\pi_{\theta^*}(a|s)$

```

1:  Ініціалізувати параметри actor  $\theta$  та critic  $\phi$  (Xavier)
2:  Ініціалізувати середовище: отримати  $s(0) = x(0)$ 
3:  for епізод = 1, 2, ..., MAX_EPISODES do
4:    Зібрати траєкторію  $\tau = \{(s_t, a_t, r_t, s_{t+1})\}_{t=1}^T$ :
5:      for  $t = 1$  to  $T$  do
6:         $a_t \sim \pi_{\theta}(\cdot|s_t)$  {семплювати з поточної поліси}
7:        Застосувати  $a_t$  до мережі SD-WAN
8:        Отримати  $r_t = r(s_t, a_t)$  та  $s_{t+1}$ 
9:      end for
10:   Обчислити  $V_t^{\text{target}} = r_t + \gamma \cdot V(s_{t+1}; \phi)$  для всіх  $t$ 
11:   Обчислити переваги  $A_t^{\text{GAE}}(\lambda)$  за формулою (28)
12:   Нормалізувати:  $A_t \leftarrow (A_t - \text{mean}(A)) / (\text{std}(A) + \epsilon)$ 
13:   for  $k = 1$  to  $K_{\text{epochs}}$  do {оновлення параметрів}
14:     Семплювати мінібатч  $\mathcal{B} \subset \tau$ 
15:     Обчислити  $L^{\text{CLIP}}(\theta)$  за формулою (27)
16:     Обчислити  $L^{\text{VF}}(\phi)$  за формулою (29)
17:      $L_{\text{total}} = -L^{\text{CLIP}} + c_1 \cdot L^{\text{VF}} - c_2 \cdot H[\pi_{\theta}]$ 
18:      $\theta \leftarrow \theta - \alpha_{\text{actor}} \cdot \nabla_{\theta} L_{\text{total}}$ 
19:      $\phi \leftarrow \phi - \alpha_{\text{critic}} \cdot \nabla_{\phi} L^{\text{VF}}$ 
20:   end for
21:   if  $J(\pi_{\theta}) > J_{\text{best}}$  then збереги  $\pi_{\theta}$  як  $\pi_{\text{best}}$ 
22: end for
23: return  $\pi_{\theta^*}$ 

```

де $H[\pi_{\theta}] = -\mathbb{E}[\log \pi_{\theta}(a|s)]$ – ентропійний бонус для покращення дослідження; c_1, c_2 – вагові коефіцієнти critic loss та entropy loss відповідно.

Лістинг програмного коду «Середовище симуляції мережі SD-WAN»

Клас середовища SDWANEnv (Python / PyTorch)

```

import numpy as np
import gym
from gym import spaces

class SDWANEnv(gym.Env):
    """Середовище SD-WAN для навчання RL-агента."""
    def __init__(self, n_nodes=10, n_links=15, n_classes=3):
        super().__init__()
        self.N = n_nodes      # кількість вузлів
        self.M = n_links      # кількість каналів
        self.S = n_classes    # класи сервісу
        self.dt = 1.0         # крок симуляції (с)

        # Розмірність простору станів: 3M + N
        self.n_state = 3 * self.M + self.N
        # Розмірність простору дій: M * S (частки трафіку)
        self.n_action = self.M * self.S

        self.observation_space = spaces.Box(
            low=0, high=1, shape=(self.n_state,),
            dtype=np.float32)
        self.action_space = spaces.Box(
            low=0, high=1, shape=(self.n_action,),
            dtype=np.float32)

        # Параметри каналів
        self.C = np.random.uniform(10, 100, self.M) # Mbps
        self.d_prop = np.random.uniform(1, 50, self.M) # ms
        self.mu = self.C / 1500 * 1e6 / 8 # пакетів/с
        self.B_buf = 50 * np.ones(self.N, dtype=int)

    def reset(self):
        """Ініціалізація стану мережі."""
        self.x_L = np.random.uniform(0.1, 0.5, self.M) #
        завантаження
        self.x_D = self._compute_delay(self.x_L) #
        затримки
        self.x_P = self._erlang_b(self.x_L) #
        втрати
        self.x_B = np.random.uniform(0.1, 0.3, self.N) #
        буфери
        return self._get_obs()

    def step(self, action):

```

```

"""Один крок симуляції за рівнянням (7)."""
u = self._normalize_action(action)
# Вхідний трафік (стохастична модель Пуассона)
lam = np.random.poisson(self.C * 0.4, self.M)
# Оновлення завантаження за рівнянням (7)
self.x_L += self.dt / self.C * (
    lam * u[:self.M] - self.mu * self.x_L)
self.x_L = np.clip(self.x_L, 0, 1)
# Оновлення затримки та втрат
self.x_D = self._compute_delay(self.x_L)
self.x_P = self._erlang_b(self.x_L)
# Обчислення винагороди (20)
reward = self._compute_reward(u)
obs = self._get_obs()
done = bool(np.any(self.x_L > 0.95))
return obs, reward, done, {}

def _compute_delay(self, rho):
    """Затримка за формулою (8)."""
    safe_rho = np.minimum(rho, 0.999)
    return self.d_prop + 1500/self.C +
safe_rho/(self.mu*(1-safe_rho))

def _erlang_b(self, rho, B=50):
    """Формула Ерланга-В (9) – числова реалізація."""
    a = rho # трафікове навантаження
    inv_B = 1.0
    for k in range(1, B + 1):
        inv_B = 1.0 + inv_B * k / a
    return 1.0 / inv_B

def _compute_reward(self, u):
    """Винагорода за формулою (20)."""
    r = -(0.3 * np.sum(self.x_L**2)
        + 0.4 * np.sum((self.x_D / 100)**2)
        + 0.2 * np.sum(self.x_P**2)
        + 0.1 * np.sum(u**2))
    return float(r)

def _normalize_action(self, action):
    """Нормалізація дій (обмеження (3))."""
    u = action.reshape(self.S, self.M)
    u = np.abs(u) + 1e-8
    u = u / u.sum(axis=1, keepdims=True)
    return u.flatten()

def _get_obs(self):
    """Формування вектора спостереження (1)."""

```



```
return np.concatenate([
    self.x_L, self.x_D / 200.0,  # нормалізація
    self.x_P, self.x_B
]).astype(np.float32)
```

Лістинг програмного коду «Actor-Critic нейронна мережа (PPO)»

```

import torch
import torch.nn as nn
import torch.nn.functional as F
from torch.distributions import Normal

class ActorCritic(nn.Module):
    """Actor-Critic мережа за архітектурою (30)."""
    def __init__(self, state_dim, action_dim):
        super().__init__()
        # Спільна частина (shared backbone)
        self.shared = nn.Sequential(
            nn.Linear(state_dim, 256), nn.ReLU(),
            nn.Linear(256, 128), nn.ReLU()
        )
        # Actor head - генерує  $\mu$  та  $\log \sigma$ 
        self.actor_mean = nn.Linear(128, action_dim)
        self.actor_log_std =
nn.Parameter(torch.zeros(action_dim))
        # Critic head - оцінює  $V(s)$ 
        self.critic = nn.Linear(128, 1)
        self._init_weights()

    def _init_weights(self):
        for layer in self.shared:
            if isinstance(layer, nn.Linear):
                nn.init.xavier_uniform_(layer.weight)

    def forward(self, state):
        h = self.shared(state)
        mean = torch.tanh(self.actor_mean(h)) #  $\in [-1,1]$ 
        std = torch.exp(self.actor_log_std).clamp(0.01, 1.0)
        dist = Normal(mean, std)
        value = self.critic(h)

```

```
        return dist, value

def get_action(self, state):
    dist, value = self(state)
    action = dist.sample()
    log_prob = dist.log_prob(action).sum(-1)
    return action, log_prob, value
```

Лістинг програмного коду «Навчання агента PPO»

```

class PPOTrainer:
    def __init__(self, env, gamma=0.99, lam=0.95,
                 eps_clip=0.2, lr=3e-4, K_epochs=10):
        self.env = env
        self.gamma, self.lam = gamma, lam
        self.eps_clip = eps_clip
        self.K_epochs = K_epochs
        s_dim = env.observation_space.shape[0]
        a_dim = env.action_space.shape[0]
        self.net = ActorCritic(s_dim, a_dim)
        self.opt = torch.optim.Adam(self.net.parameters(),
lr=lr)

    def compute_gae(self, rewards, values, dones):
        """GAE за формулою (28)."""
        T = len(rewards)
        adv = torch.zeros(T)
        gae = 0
        for t in reversed(range(T)):
            delta = (rewards[t] + self.gamma *
                    values[t+1] * (1-dones[t]) - values[t])
            gae = delta + self.gamma * self.lam * (1-
dones[t]) * gae
            adv[t] = gae
        return adv

    def update(self, batch):
        """Оновлення параметрів за формулами (27)-(29)."""
        states, actions, log_probs_old, returns, advantages =
batch
        advantages = (advantages - advantages.mean()) /
                    (advantages.std() + 1e-8)
        for _ in range(self.K_epochs):

```

```

        dist, values = self.net(states)
        log_probs = dist.log_prob(actions).sum(-1)
        entropy = dist.entropy().sum(-1).mean()
        ratio = torch.exp(log_probs - log_probs_old)
        # Clip PPO loss (27)
        surr1 = ratio * advantages
        surr2 = torch.clamp(ratio,
                            1-self.eps_clip, 1+self.eps_clip) *
advantages
        actor_loss = -torch.min(surr1, surr2).mean()
        # Critic loss (29)
        critic_loss = F.mse_loss(values.squeeze(),
returns)
        loss = actor_loss + 0.5*critic_loss -
0.01*entropy
        self.opt.zero_grad()
        loss.backward()
        nn.utils.clip_grad_norm_(self.net.parameters(),
0.5)
        self.opt.step()

```

Акти впровадження

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «АЙТІ КУРСОР»

Ідентифікаційний код за ЄДРПОУ: 40123706. Юридична адреса: 03124, м. Київ, бульвар Вацлава Гавела, 8. Фактична адреса: 03124, м. Київ, бульвар Вацлава Гавела, 8.

Поточний рахунок: UA74 305299 00000 26007025022694 в ПАТ КБ «ПРИВАТБАНК» МФО: 305299

<http://www.itcursor.com.ua> E-mail: info@itcursor.com.ua тел\факс +38(044) 501-12-03



ЗАТВЕРДЖЕНО

« 27 » листопада 2025 р.

АКТ

впровадження результатів дисертаційної роботи аспіранта
Державного університету інформаційно-комунікаційних технологій
Вишнівського Олександра Вікторовича

Комісія у складі голови - директор, Сенчіло Ярослав В'ячеславович та членів комісії головний інженер Седих Денис Сергійович і Остапчук Валентин Віталійович, цим Актом засвідчує, що результати дисертаційного дослідження аспіранта кафедри комп'ютерних наук Державного університету інформаційно-комунікаційних технологій Вишнівського Олександра Вікторовича на тему: «Метод побудови захищеної комп'ютерної системи на основі графу атак», поданої на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», впроваджено на ТОВ «Айті Курсор» в процесі вдосконалення архітектури інформаційної системи підприємства. При цьому використано модель інформаційної мережі з управлінням SD-WAN у просторі станів з застосуванням нейромережевих засобів, що дозволило оптимізувати управління SD-WAN на основі машинного навчання.

Комісія вважає, що запропоновані рішення мають вагомий теоретичний та практичний значимість для підвищення ефективності інформаційної системи підприємства.

Голова комісії

Члени комісії

Сенчіло Я.В.

Остапчук В.В.

Седих Д.С.



ЗАТВЕРДЖУЮ

Директор ТОВ «Науково-виробниче
підприємство хімічних продуктів»

Володимир ЩЕРБАНЬ
«18» 2026 р.



АКТ

впровадження результатів дисертаційної роботи аспіранта
Державного університету інформаційно-комунікаційних технологій
Вишнівського Олександра Вікторовича

Комісія у складі голови – провідного фахівця інформаційних технологій Бондарцева П.Є. та членів комісії - фахівця інформаційних технологій Зуя В.Ф., цим Актом засвідчує, що результати дисертаційного дослідження аспіранта кафедри комп'ютерних наук Державного університету інформаційно-комунікаційних технологій Вишнівського Олександра Вікторовича на тему: «Метод побудови захищеної комп'ютерної системи на основі графу атак», поданої на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», впроваджено на ТОВ «Науково-виробниче підприємство хімічних продуктів» в процесі вдосконалення архітектури інформаційної системи підприємства. При цьому використано модель інформаційної мережі з управлінням SD-WAN у просторі станів з застосуванням нейромережевих засобів, що дозволило оптимізувати управління SD-WAN на основі машинного навчання

Комісія вважає, що запропоновані рішення мають вагому теоретичну та практичну значимість для підвищення ефективності інформаційної системи підприємства.

Голова комісії



Павло БОНДАРЦЕВ

Члени комісії



Віталій ЗУЙ

ЗАТВЕРДЖУЮ



Перший проректор Державного
університету інформаційно-
комунікаційних технологій

Олександр КОРЧЕНКО
03 2026р.

АКТ

використання у навчальному процесі Навчально-наукового інституту інформаційних технологій результатів дисертаційної роботи аспіранта кафедри комп'ютерних наук Державного університету інформаційно-комунікаційних технологій Вишнівського Олександра Вікторовича на тему: «Метод побудови захищеної комп'ютерної системи на основі графу атак та штучного інтелекту» на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки

Комісія у складі: голова – директор Навчально-наукового інституту інформаційних технологій доктор технічних наук, професор Нестеренко Катерина Сергіївна, члени комісії – завідувачка кафедри штучного інтелекту, доктор технічних наук, професор Зінченко Ольга Валеріївна, доцент кафедри комп'ютерних наук кандидат технічних наук, доцент Гніденко Микола Петрович розглянули дисертаційну роботу Вишнівського Олександра Вікторовича на тему: «Метод побудови захищеної комп'ютерної системи на основі графу атак та штучного інтелекту» та публікації автора за матеріалами дисертаційної роботи. Результати впроваджено в початковий процес Навчально-наукового інституту інформаційних технологій, а саме:

- модель комп'ютерної системи SD-WAN на основі апарату простору станів, яка забезпечує кількісне відображення часових характеристик передачі даних, зміни пропускної здатності каналів зв'язку та ймовірності втрат пакетів;
- метод інтелектуального управління комп'ютерною системою SD-WAN на основі машинного навчання;
- метод побудови захищеної комп'ютерної системи SD-WAN на основі графу атак та глибокого навчання, який дозволяє превентивно перебудовувати мережеві маршрути та розривати ланцюжки кібератак на ранніх стадіях їх розвитку.

На основі аналізу представлених матеріалів комісія встановила.

Результати дослідження використано в навчальному процесі Державного університету інформаційно-комунікаційних технологій при оновленні робочих програм, навчальних дисциплін та підготовці методичного забезпечення кафедри комп'ютерних наук та штучного інтелекту у наступний спосіб:

інтегровано теоретичні положення щодо функціонування SD-WAN архітектур у зміст лекційних курсів навчальних дисциплін: «Конвергентна мережна інфраструктура», «Хмарна платформа OpenStack» ОКР «Бакалавр» спеціальності Комп'ютерні науки;

- впроваджено у лабораторні практикуми серію практичних завдань, спрямованих на опанування розробки систем інтелектуального управління комп'ютерною системою SD-WAN навчальних дисциплін: «Комп'ютерні методи моделювання та організації процесів», «Проектування обчислювальних пристроїв» ОКР «Магістр» спеціальності Комп'ютерні науки;

- використано методичні підходи до розробки захищеної комп'ютерної системи SD-WAN на основі графу атак в межах курсового та дипломного проектування спеціальності Комп'ютерні науки.

Голова комісії

Директор ННІТ
доктор технічних наук, професор



Катерина НЕСТЕРЕНКО

Члени комісії

Завідувачка кафедри штучного інтелекту,
доктор технічних наук, професор



Ольга ЗІНЧЕНКО

Доцент кафедри комп'ютерних наук,
кандидат технічних наук, доцент



Микола ГНІДЕНКО