УДК 681.3

DOI: 10.18372/2073-4751.81.20129

Кулаков Ю.О., д.т.н.,
orcid.org/0000-0002-8981-5649,
e-mail: ya.kulakov@gmail.com,
Обозний Д.М.,
orcid.org/0000-0003-0108-4587,
e-mail: dobozniy@gmail.com

АЛГОРИТМ ОРКЕСТРАЦІЇ ШИФРОВАНОГО ТРАФІКУ В МЕРЕЖАХ SDN

**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**

Вступ

Стрімке зростання обсягів мережевого трафіку в традиційних комп'ютерних мережах призводить до зниження ефективності їх функціонування, ускладнення реконфігурації та зменшення гнучкості керування. Збільшення кількості різноманітних типів трафіку погіршує якість обслуговування як для кінцевих користувачів, так і для критичних бізнес-систем, що робить проблему керування навантаженням у мережах особливо актуальною. Одним з ефективних підходів до розв'язання зазначених проблем є використання програмно визначених мереж (*Software-Defined Networking*, *SDN*). Такий підхід дозволяє централізовано керувати топологією та маршрутизацією, підвищуючи відмовостійкість, модульність та масштабованість мережі. Дослідження [1] підтверджують переваги *SDN* у зниженні складності керування мережею та зменшенні впливу зовнішніх атак на критичні компоненти інфраструктури. Одним з ключових напрямів розвитку *SDN* є реалізація ефективного механізму розподілення навантаження. Завдяки централізованому контролю та гнучкості політик, *SDN* забезпечує зручні засоби для балансування трафіку. Проте, на практиці, ефективність таких методів часто знижується через високий рівень шифрування сучасного трафіку, що ускладнює його класифікацію. А відсутність точного розподілу за типами призводить до перевантаження мережевих ресурсів і втрати критичних даних.

Таким чином, виникає потреба у створенні рішень, які забезпечують розподілення навантаження в *SDN*-мережах із урахуванням характеристик шифрованого трафіку. Це дозволить підвищити якість обслуговування, покращити надійність систем і забезпечити стійкість до перевантаження в умовах інтенсивного трафіку.

Метою даної роботи є розробка алгоритму розподілення навантаження в *SDN*-мережах на основі класифікації шифрованого трафіку з використанням *DPI*-технологій, що дозволяє покращити обслуговування пріоритетних потоків і підвищити загальну відмовостійкість мережі.

Огляд існуючих рішень

Основними напрямками досліджень у сфері програмно визначених мереж (*SDN*) є забезпечення якості обслуговування (*QoS*), зменшення затримок, ефективне управління чергами, а також адаптивна маршрутизація трафіку. Особливу увагу приділено розробці алгоритмів, що дозволяють динамічно керувати потоком даних у реальному часі на основі змін у навантаженні мережі.

Зокрема, у статті [2] запропоновано модель оцінки затримки в черзі з урахуванням реального трафіку та наскрізного контролю шляху передачі даних. Реалізовано програмне рішення для динамічного управління затримкою, яке забезпечує перемикання потоків у відповідні черги відповідно до вимог *QoS*. Експериментальні результати підтвердили високу точність моделі та її придатність для практичного застосування в *SDN*-середовищах. Підхід

орієнтований на забезпечення стабільного рівня сервісу шляхом гнучкого реагування на перевантаження та зміни трафіку.

Інше рішення представлено у статті [3], де автори розробили адаптивний механізм маршрутизації потокового відео на основі *QoS* із використанням технології резервування ресурсів (*VQoSRR*). Запропонований алгоритм перенаправляє потоки у випадку зниження *QoE* та здійснює динамічний розподіл ресурсів залежно від характеристик відеопотоку. Методика виявилася ефективною для систем відеоспостереження в умовах «розумного міста», однак її застосування обмежується лише мультимедійним трафіком, що зменшує універсальність у змішаних або зашифрованих мережах.

Автори дослідження [4] порівняли ефективність застосування різних технологій машинного навчання для задач класифікації мережевого трафіку, оптимізації маршрутизації та підвищення якості користувацького досвіду. Результати продемонстрували потенціал таких технологій для динамічної адаптації мережевої політики до змін умов трафіку.

У статті [5] описано фреймворк динамічного *QoS*-управління, який базується на глибинному навчанні. Він використовує глобальний моніторинг мережевого стану в *SDN* та централізоване управління ресурсами для оптимізації мережевої затримки та пропускної здатності. Запропоноване рішення дозволяє оперативно адаптувати параметри обслуговування залежно від поточної ситуації в мережі. У статті [6] проведено порівняння різних алгоритмів класифікації трафіку. Найкращі результати показав алгоритм *k*-ближчих сусідів, що досяг точності класифікації 0.94. Підхід базується на виявленні схожості між пакетами різних потоків і може використовуватись для автоматичного створення нових міток трафіку.

Попри ефективність зазначених рішень, всі вони мають низку обмежень. Зокрема, алгоритми, що базуються на машинному навчанні, потребують великих обсягів даних для навчання та постійного оновлення моделей з урахуванням еволюції мережевого трафіку. Додатково, стрімке поширення шифрування, зокрема й у внутрішньокорпоративних мережах, значно ускладнює процес класифікації, навіть при наявності інтелектуальних засобів аналізу.

Таким чином, аналіз наявних підходів демонструє їх ефективність у вузько спеціалізованих сценаріях – наприклад, для чітко класифікованого або відкритого трафіку. Проте в умовах інтенсивного навантаження та шифрування виникає потреба у більш гнучких та універсальних рішеннях, здатних працювати в реальному часі.

Одним із найважливіших напрямів подальших досліджень є створення алгоритмів, що забезпечують динамічне розподілення навантаження в *SDN*-мережах із урахуванням характеристик зашифрованого трафіку та потреб критичних сервісів у стабільному *QoS*.

Математичне обґрунтування проблеми передачі шифрованого трафіку без урахування пріоритетів в високонавантажених мережах

Високе навантаження в мережі, може викликати збільшення часу обробки пакетів, заповнення черги та перевантаження пристрою мережі в цілому. Розглянемо комутатор рівня передачі *SDN* мережі, як $M/M/1/K$ систему масового обслуговування, де K – максимальна ємність буферу пристрою.

Дослідження теорії черг та зміну характеристик черги описані авторами робіт [7, 8]. В ньому можна побачити, що збільшення черги відбувається в середньому через час приходу пакету в чергу, що характеризується інтенсивністю λ – кількість надісланих пакетів клієнтом за одиницю часу. В свою чергу мережевий пристрій оброблює пакети з інтенсивнюстю μ. Збільшення інтенсивності пакетів від клієнта при сталій інтенсивності обробки збільшує час очікування пакетів в черзі через збільшення довжини черги. Також оскільки черга має кінцеву довжину, при її

переповненні нові пакети відхиляються пристроєм. Для порівняння роботи звичайного алгоритму обробки пакетів в мережі та модифікованого розглянемо основні кількісні показники, якими можна охарактеризувати роботу мережі:

Коєфіцієнт завантаження системи:

$$\rho = \frac{\lambda}{\mu}, \quad (1)$$

де, λ – інтенсивність пакетів, μ – інтенсивність обслуговування.

Ймовірність простою пристрою:

$$P_0 = \frac{1-\rho}{1-\rho^{K+1}}. \quad (2)$$

Ймовірність втрати пакета:

$$P_{loss} = \frac{(1-\rho)\rho^K}{1-\rho^{K+1}}. \quad (3)$$

Ймовірність знаходження в системі n пакетів:

$$P_n = \left(\frac{\lambda}{\mu}\right)^n \left(1 - \frac{\lambda}{\mu}\right), n \geq 1. \quad (4)$$

Інтенсивність пакетів, які потрапили в чергу:

$$\lambda_{eff} = \lambda(1 - P_{loss}). \quad (5)$$

Загальна середня кількість пакетів в системі включаючи пакети в черзі та обробці:

$$L = \sum_{n=0}^{K} nP_n, \quad (6)$$

$$L = \sum_{n=0}^{K} n \frac{\left(\frac{\lambda}{\mu}\right)^n}{\left(\frac{1-\left(\frac{\lambda}{\mu}\right)^{K+1}}{1-\frac{\lambda}{\mu}}\right)}, \quad (7)$$

$$L = \frac{\frac{\lambda}{\mu}\left(1-\left(\frac{\lambda}{\mu}\right)^K\right)}{1-\frac{\lambda}{\mu}} \quad (8)$$

та середня кількість пакетів в черзі:

$$L_q = L - \frac{\lambda}{\mu}, \quad (9)$$

$$L_q = \frac{\lambda}{\mu-\lambda} * \left(\left(\frac{\lambda}{\mu}\right)^K - \frac{\lambda}{\mu}\right). \quad (10)$$

Середній час знаходження пакета в черзі:

$$W_q = \frac{L_q}{\lambda}. \quad (11)$$

Формула 1 дозволяє розрахувати наскільки відсотків завантажений пристрій. Якщо коефіцієнт $\rho = 1$ система повністю завантажена. При $\rho > 1$ система перевантажена і пакети які надходять втрачаються. Формула 2 описує ймовірність ситуації, коли у пристрою взагалі відсутні будь-які задачі. Збільшення ймовірності простою пристрою свідчить про неоптимальне використання інфраструктури та потребу в більш рівномірному розподілі трафіку в мережі. Формула 3 описує ймовірність ситуації, коли пакет, який надійшов на пристрій буде втрачений. При збільшенні навантаженності пристрою, або зменшенню розміру черги ймовірність цією події буде рости, що в свою чергу призведе до деградації інфраструктури. Формула 4 визначає ймовірність, коли в системі буде рівно n пакетів. Ця формула дозволяє зрозуміти, яка ймовірність знаходження в системі певної кількості пакетів при заданих інтенсивностях пристрою та пакетів від клієнта. Формули 8 та 10 дозволяють розрахувати середню кількість пакетів в черзі з урахуванням оброблюваного пакета та без.

Оскільки зазвичай мережевий пристрій не є гнучким з точки зору вертикального мастабування, то інтенсивність обробки мережевих пакетів є стала величина. Тому співвідношення інтенсивностей обробки пакетів пристроєм та надходження їх до черги є першочерговою задачею для забезпечення відмовостійкості мережі.

При досягненні значення інтенсивності до значення пропускної здатності, пакети почнуть відхилятись пристроєм і це призведе до втрати пакетів пріоритетного трафіку. Це призведе до деградації бізнес-систем та погіршенні якості обслуговування в мережі. Для вирішення цієї задачі, слід розділяти трафік на пріоритетний та непріоритетний. Це призведе до покращення показників СМО для пріоритетного трафіку та при певних ситуаціях, погіршить показники для непріоритетного трафіку. Проте загальна відмовостійкість системи збільшиться.

Оскільки в основному трафік є шифрованим, його слід класифікувати, для визначення оптимальних умов передачі та пріоритетної обробки в системі.

Модифікований метод визначення параметрів передачі шифрованого трафіку з використанням технології DPI

Основним завданням є поліпшення умов передачі даних для критичних систем, які використовують програмно-визначену мережу. Такими системами можуть бути бази даних, системи контролю версій, голосовий зв'язок. Такі види трафіку залежні від показників затримки і потребують зменшення цього параметру. В інакшому випадку це призводить до деградації таких систем: розсинхронізація баз даних, переривання аудіо потоку при дзвінках.

Таким чином введення поняття пріоритетності трафіку дозволяє розподілити ресурси програмно-визначеної мережі більш ефективно для поліпшення умов передачі критично важливих даних. Основною задачею мережі є обробка пріоритетного трафіку та поліпшення умов його передачі, а передача непріоритетного трафіку є другорядною задачею. Погіршення умов передачі непріоритетного трафіку не впливають на роботу бізнес-систем.

Розглянемо основні показники для пріоритетного та непріоритетного трафіку:

Завантаженість системи є ключовим параметром, який дозволяє зрозуміти наскільки пристрій здатен обробити поток трафіку в певний момент часу від клієнта:

$$\rho_p = \frac{\lambda_p}{\mu}, \quad (12)$$

$$\rho_n = \frac{\lambda_n}{\mu - \lambda_p}, \quad (13)$$

де, λ – інтенсивність пакетів, μ – інтенсивність обслуговування.

Співвідношення середньої кількості пакетів у черзі:

$$\frac{L_q^p}{L_q^n} = \frac{\lambda_p(\mu-\lambda_p-\lambda_n)}{\lambda_n(\mu-\lambda_p)} * \frac{\left(\left(\frac{\lambda_p}{\mu}\right)^K - \frac{\lambda_p}{\mu}\right)}{\left(\left(\frac{\lambda_n}{\mu-\lambda_p}\right)^K - \frac{\lambda_n}{\mu-\lambda_p}\right)}. \quad (14)$$

Співвідношення середнього очікування пакетів в черзі:

$$\frac{W_q^p}{W_q^n} = \frac{\lambda_p(\mu-\lambda_p-\lambda_n)}{\lambda_n(\mu-\lambda_p)} * \frac{\left(\left(\frac{\lambda_p}{\mu}\right)^K - \frac{\lambda_p}{\mu}\right)}{\left(\left(\frac{\lambda_n}{\mu-\lambda_p}\right)^K - \frac{\lambda_n}{\mu-\lambda_p}\right)} * \frac{\lambda_n}{\lambda_p}. \quad (15)$$

Ймовірність втрати пакета при буфері розміром K:

$$\frac{P_{loss}^p}{P_{loss}^n} = \frac{\left(1-\frac{\lambda_p}{\mu}\right)\left(\frac{\lambda_p}{\mu}\right)^K}{1-\left(\frac{\lambda_p}{\mu}\right)^{K+1}} * \frac{1-\left(\frac{\lambda_n}{\mu-\lambda_p}\right)^{K+1}}{\left(1-\frac{\lambda_n}{\mu-\lambda_p}\right)\left(\frac{\lambda_n}{\mu-\lambda_p}\right)^K}. \quad (16)$$

При збільшенні навантаження непріоритетного трафіку, параметри обслуговування для пріоритетного будуть залишатись незмінними. Проте пакети непріоритетного трафіку, при будуть втрачатись при заповненні буферу. Це дозволить підвищити відмовостійкість мережі. Але втрата пакетів непріоритетного трафіку не означає повну відмову в обслуговуванні, а у випадку *TCP* трафіку буде відбуватись повторна передача пакетів, після зменшення інтенсивності λ для пріоритетного виду трафіку.

Розпізнавання та класифікація шифрованого трафіку

Задача класифікації шифрованого мережевого трафіку є складною задачею з точки зору потреби ресурсів для її вирішення. Вона складається з декількох етапів:

- Збір зразків пакетів мережевого трафіку.
- Передача в ЦОД.
- Аналіз та класифікація на основі технології *DPI*.
- Зберігання інформації про трафік у вигляді метрик.

Існує декілька методик розпізнавання мережевого трафіку з метою його класифікації:

- Отримання інформації з заголовків пакету трафіку.
- Аналіз службових пакетів інших службових протоколів, які використовуються для передачі досліджуваного трафіку.

- Аналіз вторинних ознак пакетів мережевого трафіку.

Оскільки пакети трафіку шифровані то однозначно класифікувати їх стає все складніше. Найбільш точним є комплексний підхід в якому використовуються усі описані методики разом для підвищення точності класифікацію. Такий підхід використовує технології машинного навчання для класифікації трафіка по вторинним ознакам, проте потребує дуже великої кількості даних для навчання моделі.

Автор у роботі [9] описав різницю в розпізнаванні та класифікації шифрованого трафіку. Для пришвидшення процесу розпізнавання, дуже важливо класифікувати перший пакет з потоку даних. Завдяки використанню механізму кешування у протоколі *NBAR* використовуючи аналіз *DNS* запитів, заголовків *L*3 рівня, та сокетів *L*4. Тільки, якщо розпізнавання та класифікація на рівні *data plane* неможлива за допомогою кешування, пакет відправляється на контролер на рівні *control plane*. Там здійснюється більш детальний аналіз пакету з використанням більшого каталогу застосунків та подальшим оновленням кешу на *data plane* рівні.

Блок-схему алгоритму класифікації шифрованого трафіку зображено на рис. 1.

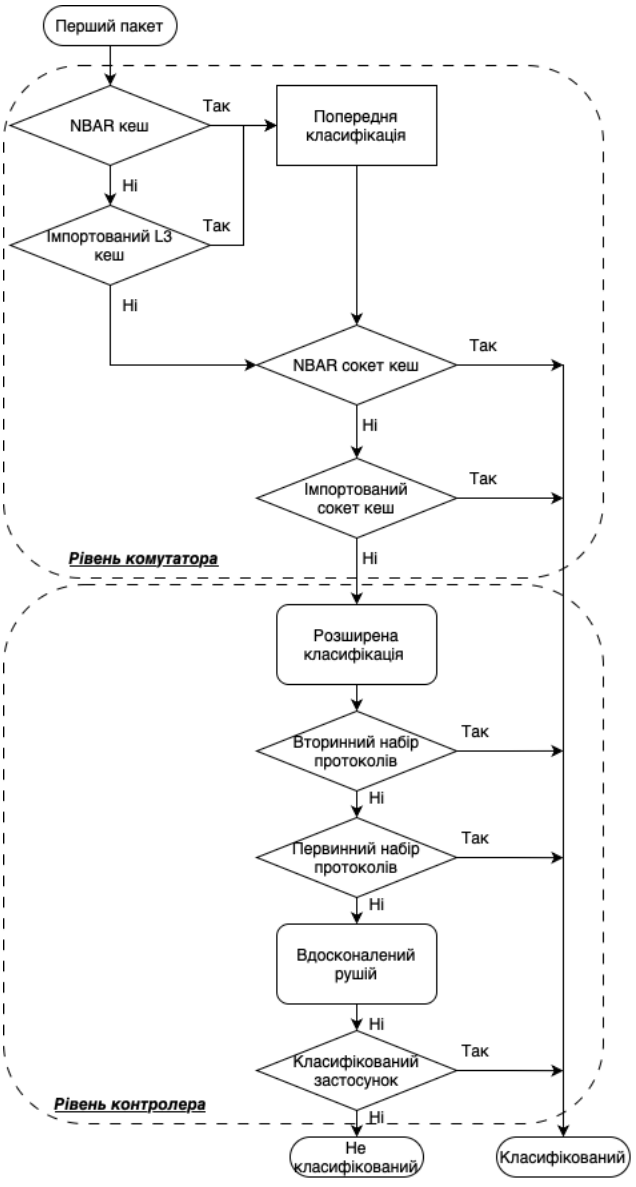

Рис. 1. Алгоритм класифікації шифрованого трафіку з використанням *Cisco NBAR* та *Cisco AVC*

Постійний збір наборів даних з подальшим їх аналізом та формуванням оновлень набору протоколів дозволяють *Cisco* постійно збільшувати точність класифікації трафіку. Використання технологій *NBAR* та *AVC* дає змогу при зменшеному навантаженні на контролер та збільшеній швидкості розпізнавання трафіку отримати більшу точність.

Застосування політик обмеження для балансування навантаження

В умовах зростання навантаження виникає потреба розподілення ресурсів мережі між пріоритетними та непріоритетними видами трафіку. Проте для бізнесу критичним ж робота пріоритетних видів трафіку. Вони повинні обслуговуватись з найменшими показниками затримки, джитеру та найбільшою швидкістю.

Таким чином окрім першочергової обробки пакетів пріоритетного трафіку, слід також зменшувати швидкість передачі непріоритетного трафіку. Загальне навантаження на мережу буде зменшуватись, а вивільнені ресурси будуть використані для передачі пріоритетних видів трафіку.

Застосування такого підходу дозволяє зменшити використання буферу мережевих пристроїв та дозволяє ефективно розподілити навантаження в мережі.

Висновки

У даній роботі було розглянуто проблему перевантаження *SDN*-мереж у контексті зростаючої частки зашифрованого трафіку, що ускладнює ефективне балансування навантаження та забезпечення якості обслуговування. Запропоновано алгоритм розподілення навантаження, який базується на класифікації шифрованого трафіку з використанням технологій *DPI*, *NBAR* та *Cisco AVC*.

Розроблений підхід передбачає розділення трафіку на пріоритетний та непріоритетний, адаптивне обмеження другорядних потоків і пріоритетну обробку критичних даних. В основі методики лежить поєднання математичної моделі системи масового обслуговування та практичних засобів для ідентифікації трафіку без розшифрування вмісту пакетів. Використання гібридного механізму класифікації дозволяє знизити навантаження на *SDN*-контролер, прискорити обробку нових потоків і підвищити загальну відмовостійкість мережі. Це особливо актуально для інфраструктур із підвищеними вимогами до *QoS*, зокрема в системах зв'язку, фінансового сектору та промислових рішеннях.

У подальших дослідженнях доцільно зосередитись на:

- емпіричній перевірці запропонованого алгоритму у віртуальних середовищах (наприклад, *Mininet*);
- розширенні набору ознак для класифікації зашифрованого трафіку з використанням методів машинного навчання;
- автоматизації формування;
- політик обмеження на основі поведінкового аналізу мережевих потоків.

Література

1. Calabrese M., Curbo J., Falco G. A Software Defined Networking Architecture for Time Triggered Ethernet in Space Systems. *2024 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)* : proceedings, Daytona Beach, FL, USA, 16–18 December 2024 / IEEE. 2024. P. 207–212. DOI: 10.1109/WiSEE61249.2024.10850170.

2. Haiyan M. et al. Towards SDN based queuing delay estimation. *China Communications*. 2016. Vol. 13, no. 3. P. 27–36. DOI: 10.1109/CC.2016.7445500.

3. Elbasheer M. O. et al. Video Streaming Adaptive QoS Routing with Resource Reservation (VQoSRR) Model for SDN Networks. *Electronics (Switzerland)*. 2022. Vol. 11, no. 8. DOI: 10.3390/electronics11081252.

4. Askar S. et al. Control Traffic in SDN Systems by using Machine Learning techniques: Review. *International Journal of Research and Applied Technology (INJURATECH)*. 2025. Vol. 5, no. 1. P. 1–24. DOI: 10.34010/INJURATECH.V5I1.15764.

5. Osman M. F. et al. A Novel Network Optimization Framework Based on Software-Defined Networking (SDN) and Deep Learning (DL) Approach. *JOIV : International Journal on Informatics Visualization*. 2024. Vol. 8, no. 4. P. 2082–2089. DOI: 10.62527/JOIV.8.4.2169.

6. Mohammed A. Q., Ghani R. F. Network Traffic Classification to Improve Quality of Service (QoS). *6th international conference for physics and advance computation sciences: ICPAS2024* : proceedings, Baghdad, Iraq, 26–27 August 2024 / AIP. 2025. Vol. 3282, no. 1. 020007. DOI: 10.1063/5.0264880/3342131.

7. Kleinrock L. Theory, Volume 1, Queueing Systems. USA : Wiley-Interscience, 1975. URL: https://ia601403.us.archive.org/13/items/in.ernet.dli.2015.134547/2015.134547.Queueing-Systems-Volume-1-Theory.pdf.

8. Ross Sh. M. Introduction to Probability Models. Elsevier, 2024. DOI: 10.1016/C2021-0-03471-4.

9. Mercado L. D. M. NBAR and SD-AVC Operations and Troubleshooting in Cisco SDWAN. URL: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2025/pdf/BRKENT-2336.pdf.

Кулаков Ю.О., Обозний Д.М.

АЛГОРИТМ ОРКЕСТРАЦІЇ ШИФРОВАНОГО ТРАФІКУ В МЕРЕЖАХ SDN

У статті розглянуто проблему перевантаження програмно визначених мереж (SDN) в умовах зростання обсягів шифрованого трафіку, що ускладнює його класифікацію та знижує ефективність традиційних методів балансування навантаження. Запропоновано алгоритм, що передбачає попередню класифікацію трафіку з використанням технологій DPI, NBAR і Cisco AVC з подальшим застосуванням політик обмеження для непріоритетних потоків. Алгоритм базується на математичній моделі типу M/M/1/K та враховує характеристики пріоритетного трафіку. Запропонований підхід дозволяє підвищити відмовостійкість мережі, покращити якість обслуговування критичних сервісів та зменшити втрати даних у перевантажених середовищах.

***Ключові слова**: програмно визначені мережі; DPI; шифрований трафік; QoS; балансування навантаження.*

Kulakov Y.O., Oboznyi D.M.

ALGORITHM FOR ORCHESTRATION OF ENCRYPTED TRAFFIC IN SDN NETWORKS

The article addresses the issue of overload in Software-Defined Networks (SDN) under increasing volumes of encrypted traffic, which complicates its classification and reduces the efficiency of traditional load balancing methods. The proposed algorithm performs preliminary traffic classification using DPI, NBAR, and Cisco AVC technologies, followed by the application of restriction policies for non-priority flows. The solution is based on the M/M/1/K queueing model and considers the characteristics of priority traffic. The proposed approach improves network fault tolerance, enhances the quality of service for critical applications, and reduces data loss in high-load environments.

***Keywords**: software-defined networks; DPI; encrypted traffic; QoS; load balancing.*