

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

**Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей**

«До захисту допущено»

Завідувач кафедри

_____Анатолій МАКАРЕНКО

«___» _____ 20__р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

**на тему: «Підвищення захищеності телекомунікаційних
мереж на базі SDN»**

Виконав (-ла):

студент (-ка) IV курсу, групи ТС-22

Гречка Артем Сергійович _____

Керівник:

Професор ЕКІР, д.т.н.,

Бондарчук Андрій Петрович _____

Рецензент:

Доцент кафедри комп'ютерних наук

Київського столичного університету

імені Бориса Грінченка, к.т.н., доцент

Мельник Ірина Юріївна _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.

Студент (-ка) _____

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«___» _____ 20__р.

ЗАВДАННЯ

на дипломну роботу студенту

Гречці Артему Сергійовичу

1. Тема роботи «Підвищення захищеності телекомунікаційних мереж на базі SDN», керівник роботи Бондарчук Андрій Петрович, професор ЕКІР, доцент, д.т.н., затверджені наказом по університету від « » травня 2026 р. №

2. Термін подання студентом роботи червня 2026 р.

3. Вихідні дані до роботи: інформаційні ресурси мережі Інтернет, література та наукові видання з тематики мережевого обладнання, навчально-методичні матеріали, структурований план з матеріалами для дипломної роботи.

4. Зміст роботи

- Основні принципи побудови телекомунікаційних мереж
- Дослідження можливостей та принципів функціонування технології SDN
- Розробка та оцінка комплексної системи підвищення захищеності телекомунікаційних мереж на базі SDN
- Техніко-економічне обґрунтування впровадження комплексної системи захисту на базі SDN/NFV

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

- Вступ
- Аналіз проблем традиційних мереж
- Фундаментальна парадигма SDN
- Архітектура NFV та віртуалізація функцій
- Класифікація загроз за STRIDE
- Механізм Service Function Chaining (SFC)
- Система виявлення аномалій (ML Model)
- Обґрунтування показників ефективності
- Комплексний аналіз переваг системи
- Висновки.

6. Дата видачі завдання: 1 березня 2026 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Видача завдання та узгодження теми дипломної роботи.	01.03.2026	Виконано
2.	Збір матеріалів по темі.	10.03.2026	Виконано
3.	Дослідження теоретичних матеріалів	15.03.2026	Виконано
4.	Написання 1 розділу.	22.03.2026	Виконано
5.	Написання 2 розділу.	25.03.2026	Виконано
6.	Написання 3 розділу.	14.04.2026	Виконано
7.	Написання 4 розділу.	27.04.2026	Виконано
8.	Вступ, висновки.	05.05.2026	Виконано
9.	Оформлення роботи, створення презентації.	02.06.2026	Виконано

Студент

Артем ГРЕЧКА

Керівник роботи

Андрій БОНДАРЧУК

РЕФЕРАТ

Дипломна робота: «Підвищення захищеності телекомунікаційних мереж на базі SDN».

Обсяг роботи: 82 сторінки, 14 рисунків, 12 таблиць. Використано науково-технічні джерела та сучасні стандарти у сфері телекомунікацій і кібербезпеки.

Актуальність роботи зумовлена стрімким розвитком інформаційних технологій, експоненційним зростанням обсягів даних, переходом до хмарних обчислень, а також впровадженням концепцій Інтернету речей (IoT) та мереж п'ятого покоління (5G), що висувають підвищені вимоги до інфраструктури передачі даних. Традиційні архітектурні підходи поступово вичерпують свій ресурс масштабованості, гнучкості та ефективності управління. У цьому контексті концепції програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV) відіграють ключову роль, пропонуючи нову парадигму побудови мереж шляхом логічного розділення площин управління та передачі даних. Використання SDN забезпечує централізоване управління мережею, швидку адаптацію до змін топології, програмовану маршрутизацію потоків та підвищення рівня кіберзахисту.

Структура та зміст роботи: У роботі розглянуто еволюцію мережевих архітектур, проведено детальний аналіз трирівневої архітектури SDN відповідно до стандартів ONF, досліджено механізми управління потоками та особливості функціонування протоколу OpenFlow. Також проаналізовано сучасні вектори атак у середовищі SDN, зокрема атаки типу DoS/DDoS на контролер та переповнення пам'яті TCAM комутаторів. Окрему увагу приділено побудові комплексної моделі захищеної мережевої архітектури на основі принципу «Zero Trust», практичним аспектам реалізації мікросегментації, динамічної ізоляції загроз та створення ланцюжків сервісів безпеки (Service Function Chaining). Також виконано техніко-економічне обґрунтування впровадження запропонованих рішень у сучасних телекомунікаційних мережах.

Метою даної роботи є дослідження та розробка комплексної системи

підвищення захищеності телекомунікаційних мереж на базі технологій SDN та NFV для забезпечення безпечного, надійного та ефективного функціонування сучасних систем зв'язку. Об'єкт дослідження — процес функціонування телекомунікаційних мереж та їх архітектура. Предмет дослідження — технічні рішення, методи та механізми підвищення захищеності мережевої інфраструктури на базі концепцій програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV).

Практичне значення отриманих результатів: Впровадження розробленої системи дозволяє пришвидшити час реакції на інциденти (наприклад, DDoS-атаки) у 10–60 разів, блокувати до 99% шкідливого трафіку та підтримувати доступність мережі на рівні «п'яти дев'яток» (99.999%) без деградації QoS. Економічне обґрунтування доводить, що використання стандартизованого обладнання (White-box) замість пропрієтарного знижує капітальні витрати (CAPEX) на 57,6%, а термін окупності проєкту становить 6 місяців.

Ключові слова: програмно-конфігурована мережа, SDN, NFV, OpenFlow, кібербезпека, мікросегментація, телекомунікації, Service Function Chaining, Zero Trust

ABSTRACT

Thesis: "Increasing the Security of Telecommunications Networks Based on SDN."

Thesis volume: 82 pages, 14 figures, 12 tables. Scientific and technical sources, as well as modern standards in the field of telecommunications and cybersecurity, were utilized.

Relevance of the work is driven by the rapid development of information technologies, the exponential growth of data volumes, the transition to cloud computing, and the implementation of Internet of Things (IoT) concepts and fifth-generation (5G) networks, all of which place increased demands on data transmission infrastructure. Traditional architectural approaches are gradually exhausting their scalability, flexibility, and management efficiency resources. In this context, the concepts of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) play a key role, offering a new network construction paradigm by logically separating the control and data planes. The utilization of SDN provides centralized network management, rapid adaptation to topology changes, programmable flow routing, and an enhanced level of cyber protection.

Structure and content of the work: The work examines the evolution of network architectures, provides a detailed analysis of the three-tier SDN architecture in accordance with ONF standards, and investigates flow management mechanisms along with the operational features of the OpenFlow protocol. Modern attack vectors in the SDN environment are also analyzed, particularly DoS/DDoS attacks on the controller and the overflow of switches' TCAM memory. Special attention is paid to constructing a comprehensive model of a secure network architecture based on the "Zero Trust" principle, practical aspects of implementing microsegmentation, dynamic threat isolation, and the creation of Service Function Chaining (SFC). Furthermore, a technical and economic assessment of implementing the proposed solutions in modern telecommunications networks is performed.

The objective of this work is to research and develop a comprehensive system for increasing the security of telecommunications networks based on SDN and NFV technologies to ensure the secure, reliable, and efficient functioning of modern

communication systems. Object of research — the process of telecommunications networks functioning and their architecture. Subject of research — technical solutions, methods, and mechanisms for increasing the security of network infrastructure based on the concepts of Software-Defined Networking (SDN) and Network Function Virtualization (NFV).

Practical significance of the obtained results: The implementation of the developed system allows accelerating the incident response time (e.g., DDoS attacks) by 10–60 times, blocking up to 99% of malicious traffic, and maintaining network availability at the "five nines" level (99.999%) without QoS degradation. The economic assessment proves that using standardized equipment (White-box) instead of proprietary alternatives reduces capital expenditures (CAPEX) by 57.6%, and the project's payback period is 6 months.

Keywords: software-defined network, SDN, NFV, OpenFlow, cybersecurity, microsegmentation, telecommunications, Service Function Chaining, Zero Trust.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І.....	11
ТЕРМІНІВ	11
ВСТУП.....	14
1 ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ	16
1.1 Загальні принципи побудови телекомунікаційних мереж	16
1.2 Детальний аналіз мережевих архітектур.....	16
1.3 Швидкість передачі даних та пропускна здатність.....	18
1.4 Аналіз концепції програмно-конфігурованих мереж (SDN) як основи сучасних телекомунікацій.....	18
1.4.1 Трирівнева архітектура SDN	18
1.4.2 Механізм обробки потоків у SDN	19
1.4.3 Переваги впровадження SDN для захищеності мереж	19
1.4.4 Детальний аналіз протоколу OpenFlow та механізмів управління потоками	20
1.4.5 Віртуалізація мережевих функцій (NFV)	21
1.4.6 Класична модель Пуассона.....	21
1.4.7 Самоподібний (фрактальний) трафік.....	22
1.4.8 Аналіз загроз та показників якості (QoS) у мережах SDN	22
1.5 Ймовірність помилки в телекомунікаційних мережах	24
1.6 Затримка інформації в телекомунікаційних мережах	25
1.7 Системи управління телекомунікаційними мережами (NMS).....	26
1.7.1 Функціональна модель управління FCAPS (ISO/IEC 7498-4).....	26
1.7.2 Протоколи та інтерфейси управління.....	27
1.7.3 Програмно-конфігуровані мережі (SDN) як нова парадигма управління.....	27
1.7.4 Віртуалізація мережевих функцій (NFV)	28
1.8 Захищеність та висока затримка передачі даних.....	28

1.9 Висновки до розділу 1	30
2 ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ТА ПРИНЦИПІВ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЇ SDN	31
2.1 Еволюція мережевих архітектур та передумови переходу до програмно-конфігурованих мереж (SDN)	31
2.2 Детальний аналіз трирівневої архітектури SDN	35
2.3 Механізми управління потоками та протокол OpenFlow	38
.....	38
2.4 Віртуалізація мережевих функцій (NFV) та її інтеграція з SDN	42
2.5 Аналіз нових векторів атак та вразливостей у середовищі SDN	44
2.6 Дослідження методів підвищення захищеності мереж за допомогою SDN/NFV	48
2.7 Висновки до розділу 2	51
3 РОЗРОБКА ТА ОЦІНКА КОМПЛЕКСНОЇ СИСТЕМИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА БАЗІ SDN	53
3.1 Концептуальна модель захищеної SDN-архітектури	53
3.2 Модель загроз та класифікація вразливостей захищеної SDN-мережі	54
3.3 Механізми захисту рівня управління: кластеризація та автентифікація..	56
3.3.1 Захист Southbound API: TLS та взаємна автентифікація	59
3.3.2 Захист Northbound API: RBAC та обмеження доступу	59
3.4 Система виявлення аномалій на основі машинного навчання	61
3.4.1 Збір та попередня обробка мережевої телеметрії	61
3.4.2 Алгоритми виявлення аномалій	62
3.5 Механізм мікросегментації та динамічної ізоляції загроз	63
3.6 Ланцюжки сервісів безпеки (Service Function Chaining) на базі NFV	65
3.7 Захист від атак на вичерпання ресурсів контролера та пам'яті TCAM	66
3.7.1 Rate-limiting Packet-In на рівні комутаторів	66
3.7.2 Проактивне встановлення wildcard-правил	67
3.7.3 Автентифікація LLDP для захисту від підміни топології	67
3.8 Оцінка ефективності запропонованої системи захисту	68

	10
3.8.1 Порівняльний аналіз методів захисту	68
3.8.2 Кількісна оцінка покращення показників захищеності	69
3.8.3 Вплив на параметри якості обслуговування (QoS)	70
3.9 Практичні рекомендації щодо впровадження	70
3.10 Висновки до розділу 3.....	71
4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ НА БАЗІ SDN/NFV	73
4.1 Мета та вихідні дані для розрахунку	73
4.2 Розрахунок капітальних витрат (CAPEX)	73
4.3 Розрахунок операційних витрат (OPEX)	74
4.4 Оцінка економічної ефективності з урахуванням зниження ризиків безпеки	75
4.5 Розрахунок терміну окупності та ROI	76
4.6 Висновки до розділу 4	77
ВИСНОВКИ.....	78
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	80

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

AAA — Authentication, Authorization, Accounting (Автентифікація, авторизація, облік).

ACL — Access Control List (Список контролю доступу).

ALE — Annualized Loss Expectancy (Очікувані річні втрати).

API — Application Programming Interface (Прикладний програмний інтерфейс).

ARO — Annual Rate of Occurrence (Очікувана кількість успішних атак на рік).

BER — Bit Error Rate (Ймовірність помилки на біт).

BGP — Border Gateway Protocol (Протокол динамічної маршрутизації).

CAPEX — Capital Expenditure (Капітальні витрати).

CLI — Command Line Interface (Інтерфейс командного рядка).

COTS — Commercial Off-The-Shelf (Стандартне комерційне обладнання).

DDoS — Distributed Denial of Service (Розподілена відмова в обслуговуванні).

DFD — Data Flow Diagram (Діаграма потоків даних).

DoS — Denial of Service (Відмова в обслуговуванні).

DPI — Deep Packet Inspection (Глибока інспекція пакетів).

ETSI — European Telecommunications Standards Institute (Європейський інститут телекомунікаційних стандартів).

FCAPS — Fault, Configuration, Accounting, Performance, Security (Функціональна модель управління мережею).

Gbps — Gigabit per second (Гігабіт за секунду).

GPON — Gigabit Passive Optical Network.

IDS — Intrusion Detection System (Система виявлення вторгнень).

IoT — Internet of Things (Інтернет речей).

IPS — Intrusion Prevention System (Система запобігання вторгненням).

JWT — JSON Web Token.

LAN — Local Area Network (Локальна мережа або рівень доступу).

LLDP — Link Layer Discovery Protocol.

LSTM — Long Short-Term Memory (Архітектура рекурентної нейронної мережі).

MAC — Media Access Control (MAC-адреса).

MAN — Metropolitan Area Network (Міська мережа або рівень розподілу).

MANO — Management and Orchestration (Архітектурний фреймворк для оркестрації).

MIB — Management Information Base (База даних управління інформацією).

MPLS — Multiprotocol Label Switching.

MTBF — Mean Time Between Failures (Середній час між відмовами).

NFV — Network Function Virtualization (Віртуалізація мережевих функцій).

NFVI — NFV Infrastructure (Інфраструктура віртуалізації).

NFVO — NFV Orchestrator (Оркестратор NFV).

NMS — Network Management System (Система управління мережею).

ODL — OpenDaylight (Платформа SDN-контролера).

ONF — Open Networking Foundation.

ONOS — Open Network Operating System (Платформа SDN-контролера).

OPEX — Operational Expenditure (Операційні витрати).

OSPF — Open Shortest Path First (Протокол динамічної маршрутизації).

PKI — Public Key Infrastructure (Інфраструктура відкритих ключів).

PON — Passive Optical Network (Пасивна оптична мережа).

QoS — Quality of Service (Якість обслуговування).

RBAC — Role-Based Access Control (Управління доступом на основі ролей).

REST — Representational State Transfer.

ROI — Return on Investment (Коефіцієнт рентабельності інвестицій).

SDN — Software Defined Networking (Програмно-конфігурована мережа).

SFC — Service Function Chaining (Ланцюжки сервісів безпеки).

SIEM — Security Information and Event Management.

SLE — Single Loss Expectancy (Очікувані втрати від одного інциденту).

STRIDE — Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (Методологія аналізу загроз).

TCAM — Ternary Content-Addressable Memory (Троїчна асоціативна пам'ять).

TLS — Transport Layer Security (Протокол захисту транспортного рівня).

URLLC — Ultra-Reliable Low-Latency Communication (Наднадійний зв'язок з низькою затримкою).

VIM — Virtualized Infrastructure Manager (Менеджер віртуалізованої інфраструктури).

VLAN — Virtual Local Area Network (Віртуальна локальна мережа).

VNF — Virtual Network Function (Віртуальна мережева функція).

VNFM — VNF Manager (Менеджер VNF).

VoIP — Voice over IP (Голосовий зв'язок через IP).

WAN — Wide Area Network (Глобальна мережа або ядро).

ВСТУП

Актуальність теми. Стрімкий розвиток інформаційних технологій, експоненційне зростання обсягів даних, перехід до хмарних обчислень та впровадження концепцій Інтернету речей (IoT) і мереж п'ятого покоління (5G) висувають безпрецедентні вимоги до інфраструктури передачі даних. Традиційні архітектурні підходи, які закладалися на етапі становлення глобальних мереж, поступово вичерпують свій ресурс масштабованості та гнучкості, що робить перехід до нових парадигм управління критичною необхідністю. У цьому контексті концепції програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV) відіграють ключову роль, пропонуючи радикальну зміну традиційної парадигми шляхом логічного розділення площини управління та площини передачі даних. Використання SDN забезпечує централізоване управління мережею, швидку адаптацію до змін топології, програмовану маршрутизацію потоків та створює унікальні можливості для підвищення захищеності телекомунікаційних інфраструктур. Однак централізація логіки управління також створює нові специфічні вектори атак, такі як вичерпання ресурсів контролера та пам'яті комутаторів, що потребує розробки нових комплексних підходів до мережевої безпеки.

Мета роботи — дослідження та розробка комплексної системи підвищення захищеності телекомунікаційних мереж на базі технологій SDN та NFV для забезпечення безпечного, надійного та ефективного функціонування сучасних систем зв'язку.

Для досягнення поставленої мети було сформульовано та вирішено такі задачі:

Проаналізувати основні принципи побудови сучасних телекомунікаційних мереж, їх архітектури та обмеження щодо масштабованості і надійності.

Дослідити можливості, принципи функціонування трирівневої архітектури SDN та протоколу OpenFlow.

Проаналізувати специфічні вектори атак у середовищі SDN та дослідити методи підвищення захищеності за допомогою SDN/NFV, зокрема

мікросегментацію та Service Function Chaining.

Розробити концептуальну модель захищеної SDN-архітектури, що включає захист рівня управління, систему виявлення аномалій та механізми протидії специфічним атакам.

Виконати техніко-економічне обґрунтування доцільності впровадження запропонованої комплексної системи захисту.

Об'єкт дослідження — процес функціонування телекомунікаційних мереж та їх архітектура.

Предмет дослідження — технічні рішення, методи та механізми підвищення захищеності мережевої інфраструктури на базі концепцій програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV).

Методи дослідження. У роботі використано методи системного аналізу для дослідження архітектур телекомунікаційних мереж; методи теорії ймовірностей та математичної статистики для аналізу характеристик трафіку; принципи машинного навчання для виявлення мережевих аномалій; метод моделювання загроз (STRIDE) для класифікації вразливостей архітектури; а також методи техніко-економічного аналізу (зокрема модель ALE) для оцінки ефективності капітальних інвестицій та зниження фінансових ризиків.

Практичне значення отриманих результатів. Розроблено та обґрунтовано архітектуру захищеної мережі на базі SDN, впровадження якої дозволяє пришвидшити час реакції на інциденти (наприклад, DDoS-атаки) у 10–60 разів, блокувати до 99% шкідливого трафіку та підтримувати доступність мережі на рівні «п'яти дев'яток» (99.999%) без деградації QoS. Економічне обґрунтування доводить, що використання стандартизованого обладнання (White-box) замість пропрієтарного знижує капітальні витрати (CAPEX) на 57,6% , а термін окупності проєкту становить 6 місяців.

1 ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Загальні принципи побудови телекомунікаційних мереж

Телекомунікаційні мережі будуються на основі сегментного підходу, що передбачає декомпозицію транспортної функції на рівні доступу, розподілу та ядра [1]. Основна мета — максимізувати замикання локального трафіку в сегментах та мінімізувати міжсегментний обмін, що забезпечує масштабованість та ефективність [10].

Аналіз побудови телекомунікаційних мереж дозволяє виділити декілька взаємопов'язаних принципів. По-перше, мережа будується ієрархічно — з чітким розподілом на рівень доступу (LAN), рівень розподілу (MAN) та ядро (WAN), що спрощує масштабування та локалізацію несправностей. По-друге, сегменти мережі проектуються технологічно однорідними, тобто використовують уніфіковані інтерфейси взаємодії. По-третє, архітектура має забезпечувати масштабованість — від окремого абонентського пункту до глобальної інфраструктури. Нарешті, для підвищення надійності застосовується резервування на основі кільцевих або дублюючих топологій. [10].

1.2 Детальний аналіз мережевих архітектур

Ієрархічна архітектура з топологією дерева широко застосовується в корпоративних мережах та архітектурі 5G Core. Її головною перевагою є висока масштабованість — додавання нових вузлів не потребує перебудови всієї топології. Водночас суттєвим недоліком є залежність від вузлів верхнього рівня: відмова одного з них призводить до недоступності всього підпорядкованого сегменту, що в літературі позначається як "єдина точка відмови" (Single Point of Failure) [1].

Кільцева архітектура є типовою для міських (MAN) та пасивних оптичних (PON) мереж. Її ключовою характеристикою є висока стійкість до відмов: при пошкодженні одного з ланок мережа автоматично перемикається

на резервний шлях протягом не більше 50 мс, що забезпечує практично непомітний для користувача перебіг у роботі.

Сітчаста архітектура (Mesh) використовується переважно у дата-центрах та хмарних інфраструктурах, де критично важлива максимальна пропускна здатність та відмовостійкість. Кількість фізичних з'єднань у повній сітці визначається формулою $n(n-1)/2$, де n — кількість вузлів, що при великих мережах призводить до суттєвого зростання капітальних витрат і є основним обмеженням цієї архітектури. [10].

Зіркоподібна архітектура є стандартом для мереж абонентського доступу, зокрема GPON. Простота адміністрування та низька вартість підключення нових абонентів роблять її популярним рішенням на рівні "остання миля". Однак повна залежність усіх абонентів від центрального вузла означає, що його відмова одночасно позбавляє доступу до мережі всіх підключених користувачів.

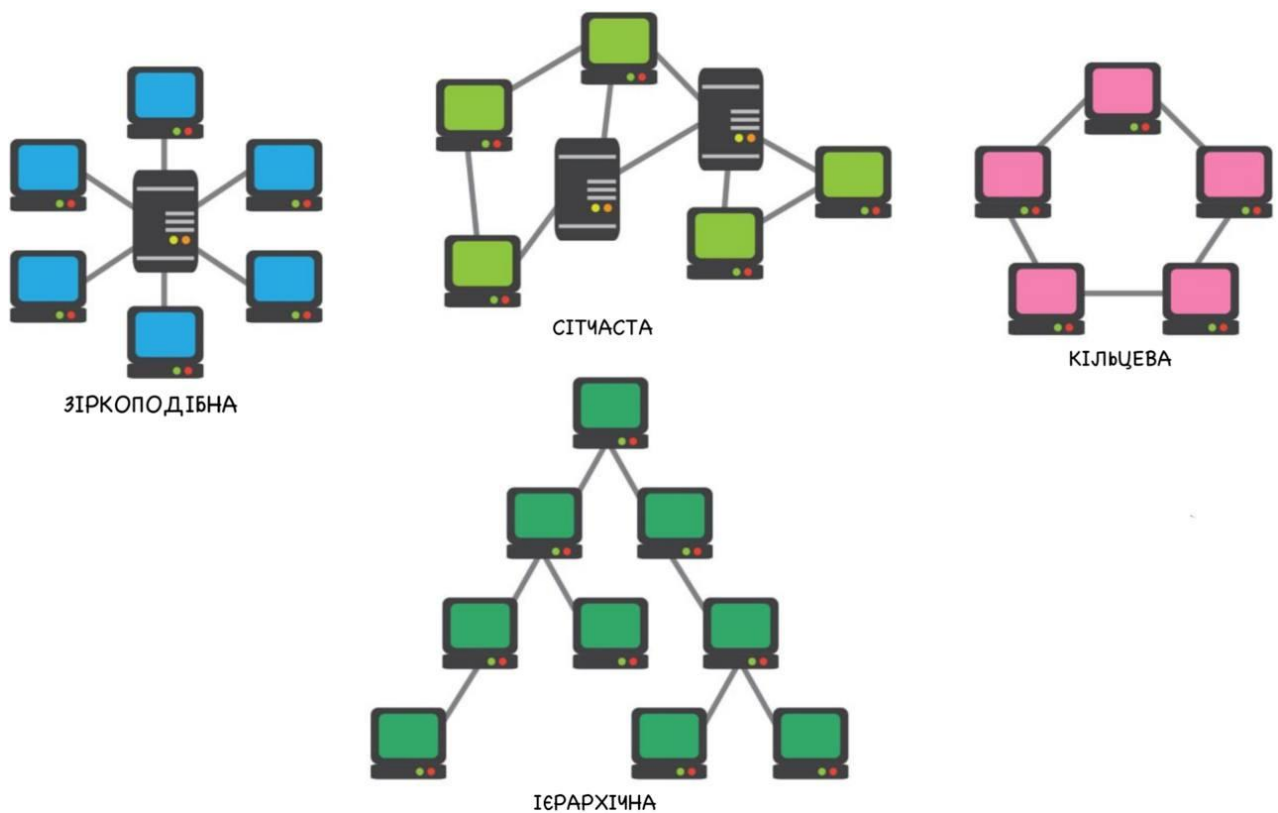


Рисунок 1.1 – Мережеві архітектури

1.3 Швидкість передачі даних та пропускна здатність

Швидкість передачі визначає обсяг інформації, що проходить через канал за одиницю часу (біт/с). Вона безпосередньо залежить від ширини смуги пропускання та обраної технології модуляції [1].

1. Смуга пропускання (Bandwidth): Максимально можлива швидкість на фізичному рівні. Для локальних мереж (LAN) вона зазвичай становить 1 Gbps.

2. Пропускна здатність (Throughput): Реальна швидкість передачі корисних даних з урахуванням службових заголовків та повторних передач [10]. У мережах MAN (10Gbps) вона забезпечує високу якість відтворення.

1.4 Аналіз концепції програмно-конфігурованих мереж (SDN) як основи сучасних телекомунікацій

Традиційний підхід до побудови мережевої інфраструктури базується на інтеграції функцій управління (Control Plane) та функцій передачі даних (Data Plane) безпосередньо всередині кожного окремого мережевого пристрою (маршрутизатора або комутатора) [2]. Така архітектура зумовлює високу складність конфігурування, оскільки внесення змін у політику мережі вимагає індивідуального налаштування кожного вузла.

На відміну від традиційного підходу, де кожен пристрій самостійно приймає рішення про маршрутизацію, концепція SDN передбачає винесення цієї логіки на окремий централізований контролер. Практичний наслідок такого рішення полягає в тому, що адміністратор отримує можливість змінювати поведінку всієї мережі через єдиний програмний інтерфейс, не торкаючись конфігурації кожного окремого пристрою.

1.4.1 Трирівнева архітектура SDN

Згідно зі стандартами ONF (Open Networking Foundation), архітектура SDN складається з трьох ключових рівнів [2]:

1. Прикладний рівень (Application Plane): включає програмні додатки, які реалізують мережеві сервіси (моніторинг, балансування навантаження, системи виявлення вторгнень IDS/IPS, управління безпекою). Взаємодія з контролером відбувається через Northbound API (зазвичай RESTful API).

2. Рівень управління (Control Plane): серце мережі — SDN-контролер. Він володіє повною топологічною картиною мережі, обчислює маршрути та транслює високорівневі політики в конкретні правила для обладнання.

3. Інфраструктурний рівень (Data Plane): рівень фізичного або віртуального обладнання. Комутатори лише виконують команди контролера, пересилаючи пакети згідно з таблицями потоків (Flow Tables). Взаємодія здійснюється через Southbound API (найпоширенішим протоколом є OpenFlow) [3].

1.4.2 Механізм обробки потоків у SDN

На відміну від класичної маршрутизації за IP-адресою призначення, у SDN використовується поняття "потіку" (Flow) [3]. Потік може ідентифікуватися за сукупністю ознак:

1. MAC-адреси відправника та отримувача;
2. IP-адреси та номери портів (L4);
3. Ідентифікатор VLAN або MPLS-мітка.

Це дозволяє реалізувати гнучкі політики безпеки. Наприклад, трафік певного користувача може бути спрямований через ланцюжок віртуальних функцій безпеки (Service Chaining) перед тим, як потрапити в ядро мережі [7].

1.4.3 Переваги впровадження SDN для захищеності мереж

З точки зору безпеки мережевої інфраструктури, централізована архітектура SDN дає три практично важливі переваги порівняно з традиційним підходом. Перша — це повна видимість трафіку: контролер у реальному часі

отримує інформацію про всі потоки, що дозволяє виявляти нестандартні з'єднання на ранньому етапі. Друга перевага — швидкість реагування: при виявленні атаки типу DoS контролер одночасно оновлює правила на всіх комутаторах мережі, тоді як у традиційній мережі адміністратор мав би налаштовувати кожен пристрій окремо. Третя — мікросегментація, тобто можливість програмно розділити мережу на ізольовані зони для різних груп користувачів без необхідності створення складних списків контролю доступу ACL на кожному фізичному пристрої.

Таблиця 1.1 - Порівняльний аналіз традиційних мереж та SDN

Параметр порівняння	Традиційні мережі (Legacy)	Мережі SDN
Управління	Децентралізоване (кожен пристрій окремо)	Централізоване (через SDN-контролер)
Швидкість збіжності	Залежить від протоколів (OSPF, BGP), може тривати секунди	Майже миттєва завдяки глобальній видимості топології
Складність конфігурування	Висока, схильна до людських помилок (CLI)	Низька, автоматизована через API
Гнучкість (Agility)	Обмежена апаратними можливостями	Висока, програмна зміна шляхів трафіку
Витрати (CAPEX/OPEX)	Високі через дороге вендорне обладнання	Нижчі завдяки використанню White-box комутаторів

1.4.4 Детальний аналіз протоколу OpenFlow та механізмів управління потоками

Протокол OpenFlow є основним стандартом взаємодії між рівнем управління та рівнем передачі даних [3]. Він дозволяє контролеру

безпосередньо маніпулювати таблицями потоків комутаторів.

Основні типи повідомлень OpenFlow:

1. Packet-In: Надсилається комутатором до контролера, коли пакет не відповідає жодному правилу в таблиці потоків. Контролер аналізує заголовок і приймає рішення про подальшу долю пакету.
2. Flow-Mod (Flow Modification): Повідомлення від контролера до комутатора для встановлення, зміни або видалення запису в таблиці потоків. Це дозволяє динамічно керувати маршрутизацією та безпекою.
3. Packet-Out: Використовується контролером для відправки пакету через конкретний порт комутатора [3]. Це часто застосовується після того, як контролер обробив повідомлення Packet-In.

1.4.5 Віртуалізація мережевих функцій (NFV)

NFV (Network Function Virtualization) є комплементарною технологією до SDN. В той час як SDN розділяє рівні управління та передачі, NFV переносить мережеві сервіси з виділених пристроїв на стандартне серверне обладнання (COTS) [4].

Переваги інтеграції SDN та NFV:

1. Віртуалізація безпеки: Брандмауери (vFirewall) та системи IDS/IPS розгортаються як віртуальні машини, що дозволяє масштабувати їх за запитом.
2. Еластичність: Можливість швидкого виділення ресурсів для обробки пікових навантажень.
3. Економічна ефективність: Зменшення капітальних витрат (CAPEX) на закупівлю спеціалізованого заліза [7].

1.4.6 Класична модель Пуассона

Традиційно трафік у мережах з комутацією каналів описувався розподілом Пуассона. Основна формула ймовірності надходження k викликів за час t :

$$P(k, t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}$$

Де λ — інтенсивність надходження пакетів. Ця модель добре працює для голосу (VoIP), але не враховує пакувальний характер передачі даних у сучасних мережах [5].

1.4.7 Самоподібний (фрактальний) трафік

Сучасний мережевий трафік має властивість самоподібності (Self-similarity). Це означає, що структура трафіку виглядає схожою на різних часових масштабах (від мілісекунд до годин). Ключовим параметром є коефіцієнт Херста (H):

Якщо $0.5 < H < 1$, трафік є самоподібним (має "важкі хвости").

Високе значення H призводить до різкого збільшення затримок у чергах (T_{queue}), навіть при низькому середньому завантаженні каналу [10].

1.4.8 Аналіз загроз та показників якості (QoS) у мережах SDN

Для забезпечення надійності "п'ять дев'яток" (99.999%) необхідно враховувати критичні параметри [9]:

1. Затримки (Delay): Для критичних сервісів 5G URLLC затримка повинна бути < 1 мс [9]. Висока затримка в SDN може бути спричинена часом обробки запитів на контролері.
2. Джиттер (Jitter): Варіація затримки, яка в ідеальних LAN мережах становить < 10 мкс.
3. Загрози безпеці: Окрім стандартних DDoS-атак, в SDN з'являється ризик Flow poisoning — підміни таблиць потоків, що може призвести до несанкціонованого перехоплення трафіку [7].

Таблиця 1.2 – Основні архітектури телекомунікаційних мереж

Архітектура	Топологія	Приклади застосування	Переваги	Недоліки
Ієрархічна	Дерево	Корпоративні мережі, 5G Core	Масштабованість, легке керування	Single point of failure
Кільцева	Кільце	MAN, PON мережі	Висока надійність (50мс переключення)	Обмежена масштабованість
Сітчаста	Full mesh	Дата-центри, хмарні мережі	Максимальна пропускна здатність	Висока вартість ($n(n-1)/2$ ліній)
Зірка	Hub-spoke	Абонентський доступ (GPON)	Простота адміністрування	Залежність від центру



Рисунок 1.2 - Ієрархічна архітектура телеком-мережі

На рисунку 1.2 зображено класичну ієрархію телекомунікаційної мережі. По суті, ця схема ілюструє логіку того, як наш трафік мандрує від домашнього комп'ютера до глобальної магістралі.

Якщо розбирати ланцюжок зліва направо, то все починається з абонентських пунктів. Це звичне для нас кінцеве обладнання: домашні Wi-Fi роутери, смартфони, ноутбуки чи модеми. Тобто це точка, де інформаційний потік власне зароджується.

Далі дані потрапляють на вузли доступу — так звану "останню милю". Тут відбувається фізичне підключення користувача до мережі провайдера. На практиці це комутатори в під'їздах багатоквартирних будинків, базові станції мобільного зв'язку або оптичні термінали (якщо у вас проведено оптоволокну).

Оскільки таких користувачів дуже багато, тягнути від кожного окремий канал до центру мережі було б нераціонально. Тому наступною ланкою йдуть вузли розподілу. Вони збирають (агрегують) трафік з безлічі вузлів доступу в товстіші та потужніші канали. Крім простого збору даних, на цьому етапі

провайдери зазвичай налаштовують маршрутизацію, фільтрують трафік і керують якістю послуг.

Фінальний етап на схемі — це транспортна мережа, яку частіше називають просто "ядром" (Core). Це фундамент усієї інфраструктури. Її єдина мета полягає в тому, щоб надійно і максимально швидко переганяти гігантські обсяги агрегованого трафіку. Саме ядро з'єднує між собою міста, країни та дозволяє вашому провайдеру обмінюватися даними з іншими мережами.

Такий ступінчастий підхід придумали не просто так. Він дає змогу нормально масштабувати мережу і швидко знаходити поломки: якщо зник інтернет в одному будинку, проблему шукають на рівні доступу, не чіпаючи при цьому ядро чи вузли розподілу.

1.5 Ймовірність помилки в телекомунікаційних мережах

Цей параметр визначає надійність передачі на фізичному рівні. Ймовірність помилки визначається BER (Bit Error Rate) та розраховується за формулою:

$$BER = Q \sqrt{\frac{2Eb}{N0}}$$

Де $\frac{Eb}{N0}$ - відношення енергії біта до спектральної щільності шуму [10].

Таблиця 1.3 - Типові показники надійності

Тип мережі	BER	MTBF (час між відмовами)	Доступність
Оптоволоконна	10^{-12}	25 000 годин	99.999% ("п'ять дев'яток")
Мідна (DSL)	10^{-7}	10 000 годин	99.95%
Бездротова (5G)	10^{-5}	5 000 годин	99.9%
Радіорелейна	10^{-6}	15 000 годин	99.97%

Резервування для підвищення надійності:

1. 1+1 APS (Automatic Protection Switching) — 50мс
2. 1:N — економічне резервування
3. Dual-homing — резервування на двох рівнях

1.6 Затримка інформації в телекомунікаційних мережах

Повна затримка (T) — це сумарний час, необхідний для доставки пакета від джерела до отримувача.

Загальна затримка передачі: $T = T_{\text{proc}} + T_{\text{trans}} + T_{\text{prop}} + T_{\text{queue}}$ [1].

T_{proc} — Затримка обробки (Processing Delay). Час на перевірку заголовків та прийняття рішення про маршрутизацію. В оптоволоконних мережах вона мінімальна — 0.1 мс.

T_{trans} — Затримка трансмісії (Transmission Delay). Час на виштовхування бітів у канал, визначається як відношення довжини пакета (L) до швидкості (R).

T_{prop} — Затримка поширення (Propagation Delay). Час руху сигналу фізичним середовищем. Для оптоволокна та міді це 5 мкс/км, для бездротових ліній — 3.3 мкс/км.

T_{queue} — Затримка черги (Queuing Delay). Час очікування в буферах пристроїв. Вона є найбільш нестабільною і може сягати 1-50 мс у бездротових мережах [1]. Наслідки високої затримки критичні: для VoIP вона має бути <150 мс [8], а для автопілотів (5G URLLC) — <1 мс [9].

Таблиця 1.4 - Затримка інформації в телекомунікаційних мережах

Компонент затримки	Оптоволокно	Мідь	Бездротова
Обробка (T_{proc})	0.1 мс	0.2 мс	0.5 мс
Трансмісія (T_{trans})	L/R	L/R	L/R
Поширення (T_{prop})	5 мкс/км	5 мкс/км	3.3 мкс/км
Черги (T_{queue})	0-10 мс	0-20 мс	1-50 мс

Таблиця 1.5 - Затримки для різних типів зв'язку

Тип зв'язку	Затримка (RTT)	Джиттер	Відтворення
LAN (1Gbps)	0.1-0.5 мс	<10 мкс	Відмінне
MAN (10Gbps)	1-5 мс	<100 мкс	Добре
WAN (MPLS)	10-50 мс	0.1-1 мс	Прийнятне
5G URLLC	<1 мс	<10 мкс	Чудове
Геостационарний супутник	500-600 мс	1-10 мс	Погане

1.7 Системи управління телекомунікаційними мережами (NMS)

Система управління мережею (NMS) — це сукупність апаратних і програмних засобів, призначених для моніторингу, адміністрування та оптимізації роботи мережевих ресурсів. Головною метою NMS є забезпечення безперервного надання послуг із заданими параметрами QoS.

1.7.1 Функціональна модель управління FCAPS (ISO/IEC 7498-4)

Це фундаментальний стандарт, який, на мою думку, не варто сприймати як розрізнений набір інструкцій, адже він розглядає управління мережею як єдиний, складний організм. Під час аналізу було виявлено, що управління відмовами (з його миттєвим виявленням першопричин та збором тривожних сповіщень) працює по-справжньому ефективно лише в тісній прив'язці до гнучкого дистанційного управління конфігурацією та обліком, який скрупульозно фіксує кожен квоту абонента. Додайте сюди безперервний моніторинг продуктивності — і ви отримаєте повний контроль над затримками та якістю обслуговування (SLA). І все це, звісно, надійно обгорнуте суворим управлінням безпекою, яке захищає канали від несанкціонованого втручання та жорстко контролює доступ до обладнання за допомогою AAA-моделі.

1.7.2 Протоколи та інтерфейси управління

Еволюція інструментів для взаємодії між системою управління та мережевим обладнанням виглядає вкрай динамічно. Хоча традиційний інтерфейс командного рядка (CLI) все ще активно використовується — особливо коли адміністратори автоматизують його спритними скриптами на кшталт Python чи Ansible — а базовий SNMP зі своєю MIB-базою та моделлю «менеджер-агент» вперто тримається на плаву, майбутнє диктує свої правила. На мою думку, сучасні реалії вимагають бездоганної надійності. Саме тому під час аналізу було виявлено абсолютну перевагу протоколів нового покоління, таких як NETCONF та RESTCONF, що вільно спілкуються мовою моделювання YANG і доставляють конфігурації значно безпечніше та стабільніше [1].

1.7.3 Програмно-конфігуровані мережі (SDN) як нова парадигма управління

Традиційне управління є децентралізованим: кожен маршрутизатор приймає рішення самостійно. Концепція SDN (Software-Defined Networking) пропонує розділити мережу на два рівні:

1. Data Plane (Рівень передачі даних): Рівень "тупих" комутаторів, які просто пересилають трафік.
2. Control Plane (Рівень управління): Централізований SDN-контролер, який має повну видимість топології мережі.

Переваги SDN для управління не обмежуються простою зручністю, вони докорінно змінюють логіку роботи мережі. На мою думку, головна сила цієї технології полягає в її неймовірній гнучкості: шляхи трафіку тепер можна змінювати програмно просто в реальному часі, без переналаштування кожного окремого пристрою. Під час аналізу було виявлено, що централізований контролер не лише філігранно балансує навантаження, оминаючи так звані «вузькі місця», але й радикально трансформує підхід до безпеки завдяки здатності миттєво реагувати на інциденти (наприклад, автоматично блокувати порт під час DDoS-атаки ще до того, як вона завдасть критичної шкоди).

1.7.4 Віртуалізація мережевих функцій (NFV)

NFV дозволяє перенести функції управління (брандмауери, балансувальники навантаження, контролери) зі спеціалізованого дорогого заліза на стандартні сервери (віртуальні машини або контейнери). Це зменшує капітальні витрати (CAPEX) та пришвидшує впровадження нових сервісів.

1.8 Захищеність та висока затримка передачі даних

Захищеність мережі визначається її здатністю протидіяти загрозам, що впливають на конфіденційність, цілісність та доступність даних.

Світ мережевих ризиків — це жива, агресивна екосистема. Під час аналізу було виявлено, що лівову частку всіх проблем (а це понад 90% зареєстрованих інцидентів) продовжують генерувати брутальні DDoS-атаки, головна мета яких — просто «покласти» канали зв'язку лавиною сміттевого трафіку. Але, на мою думку, значно більшу небезпеку приховують у собі тихі, інтелектуальні загрози: несанкціоноване перехоплення TLS-сесій (атаки Man-in-the-Middle) або ж специфічний для новітніх SDN-мереж Flow poisoning, коли таблиці маршрутизації підмінюються просто під носом у системи. І, звісно ж, не забуваємо про сувору прозу життя: яким би досконалим не був софт, до 30% усіх аварій — це банальні фізичні та механічні пошкодження кабелів, перед якими безсила будь-яка віртуалізація.

Таблиця 1.6 - Наслідки високої затримки

Сценарій	Допустима затримка	Наслідки перевищення
VoIP	<150 мс	Розмова неможлива
Відео 4K	<50 мс	Фризинг, буферизація
5G URLLC	<1 мс	Аварія автопілота
Онлайн-ігри	<50 мс	Lags, disconnect

Масштабованість — це здатність мережі нарощувати кількість абонентів та обсяги трафіку без суттєвого зниження продуктивності. Найкращу масштабованість демонструє ієрархічна архітектура за рахунок легкого керування та додавання нових рівнів.

Варіація затримки (Джиттер — Jitter)

Джиттер — це зміна затримки між послідовними пакетами.

1. Високий джиттер призводить до розсинхронізації в потокових сервісах [10].
2. У мережах LAN джиттер зазвичай становить <10 мкс, тоді як у WAN мережах може сягати 0.1-1 мс.
3. Для ідеального відтворення відео 4K або ігор джиттер має бути мінімальним.

Доступність та коефіцієнт готовності (Availability)

Цей параметр вказує на відсотковий час, протягом якого мережа готова до надання послуг.

1. "П'ять дев'яток" (99.999%): Стандарт для оптоволоконних мереж, де час простою мінімальний.
2. 5G мережі: Забезпечують доступність на рівні 99.9%.
3. Для підвищення цього показника використовується резервування за схемами 1+1 (час переключення 50 мс) або 1:N.

Надійність (MTBF — Mean Time Between Failures)

Середній час між відмовами характеризує витривалість обладнання мережі.

1. Для оптоволоконних систем цей показник становить 25 000 годин.
2. Для бездротових (5G) — близько 5 000 годин, що вимагає частішого обслуговування.

Коефіцієнт втрати пакетів (Packet Loss Rate)

Параметр, що визначає відношення втрачених пакетів до загальної кількості відправлених. Високий коефіцієнт втрат унеможливорює використання сервісів реального часу, таких як онлайн-ігри або відеозв'язок. Причинами втрат зазвичай є переповнення черг (T_{queue}) або помилки в каналі (BER).

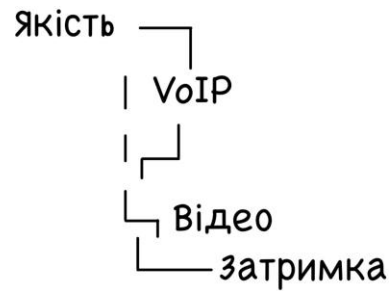


Рисунок 1.2 - Залежність якості від затримки

1.9 Висновки до розділу 1

За результатами аналізу першого розділу можна стверджувати, що для більшості сучасних телекомунікаційних сервісів оптимальною є ієрархічна архітектура з резервуванням за схемою 1+1, що забезпечує показник BER на рівні не вище 10^{-9} та затримку передачі до 50 мс. Виняток становлять сервіси класу 5G URLLC, де допустима затримка не перевищує 1 мс, а вимоги до надійності є граничними — саме для таких сценаріїв традиційні архітектури є недостатніми і необхідний перехід до SDN/NFV підходів, що детально розглядається в наступних розділах роботи.

2 ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ТА ПРИНЦИПІВ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЇ SDN

2.1 Еволюція мережевих архітектур та передумови переходу до програмно-конфігурованих мереж (SDN)

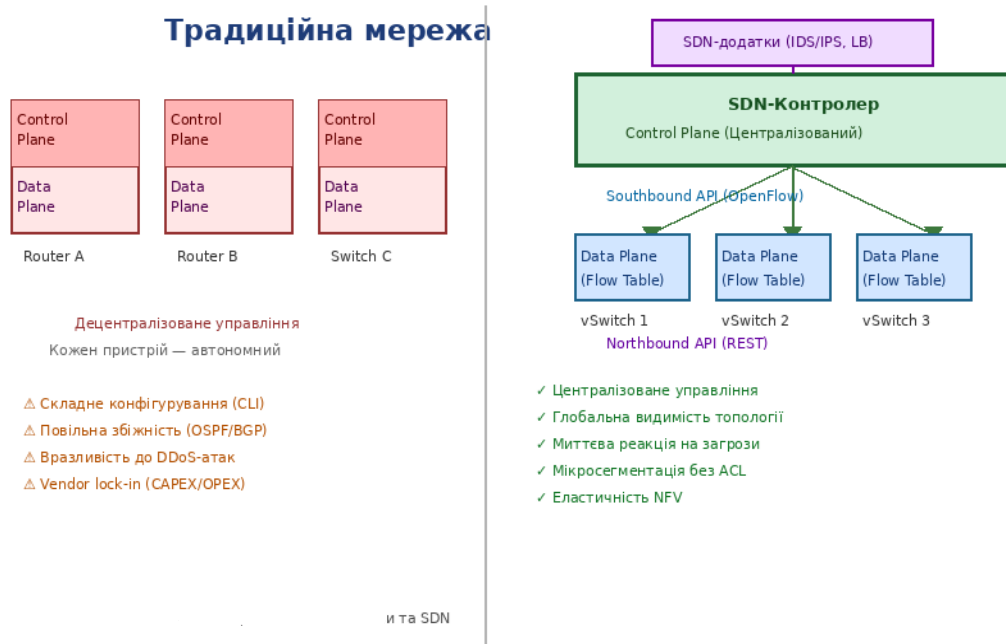


Рисунок 2.1 – Порівняння традиційної мережі архітектури та SDN

Розглянуті у першому розділі архітектурні обмеження традиційних мереж набувають особливої гостроти в умовах зростання навантаження від IoT-пристроїв та розгортання 5G-інфраструктури. Проведений аналіз показав, що децентралізована маршрутизація не здатна забезпечити швидкість реагування, необхідну для сучасних критичних сервісів. Саме ця невідповідність між вимогами до мережі та можливостями традиційного обладнання стала основною передумовою переходу до програмно-конфігурованих мереж.

Критичний аналіз обмежень традиційних (Legacy) мереж

Традиційний підхід до побудови мережевої інфраструктури базується на жорсткій інтеграції функцій управління (Control Plane) та функцій безпосередньої передачі даних (Data Plane) всередині кожного окремого мережевого пристрою, будь то маршрутизатор або комутатор [1]. Така архітектура має низку фундаментальних обмежень:

Першим і найбільш практично відчутним обмеженням традиційних мереж є складність управління конфігурацією. При необхідності змінити політику маршрутизації адміністратор змушений послідовно підключатися до кожного пристрою через CLI та вносити зміни вручну. На мережі з кількома десятками вузлів це перетворюється на багатогодинну процедуру, під час якої ймовірність допущення помилки конфігурації є достатньо високою. Така помилка, в свою чергу, може призвести до непередбачуваної поведінки трафіку або виникнення вразливості в системі безпеки.

Другим критичним обмеженням є час збіжності мережі після відмови вузла. Протоколи OSPF та BGP потребують від кількох секунд до десятків секунд для обміну оновленнями маршрутизації та перебудови таблиць. Для більшості корпоративних застосунків це прийнятно, однак для сервісів класу 5G URLLC з вимогою затримки менше 1 мс навіть короточасний збій маршрутизації є критичним. Наприклад, в системах промислової автоматизації або дистанційного керування транспортними засобами затримка понад 1 мс може призвести до некоректного виконання команд керування. [9].

Третє обмеження пов'язане зі статичністю розподілу ресурсів. Як було показано в підрозділі 1.4.8, сучасний мережевий трафік має самоподібний характер з коефіцієнтом Херста $H > 0.5$, що означає наявність різких та непередбачуваних сплесків навантаження. Традиційне обладнання не має механізмів для оперативного перерозподілу пропускної здатності між сегментами у відповідь на такі сплески. В результаті навіть при відносно низькому середньому завантаженні каналу затримка черги T_{queue} може різко зростати у моменти пікового навантаження, що безпосередньо погіршує якість обслуговування.

Четвертим обмеженням є низька ефективність реагування на кіберзагрози. При виявленні DDoS-атаки адміністратор традиційної мережі може заблокувати шкідливий трафік лише на тих пристроях, до яких він має безпосередній доступ у даний момент. Доки блокування розповсюджується по всій мережі вручну, атака продовжує споживати ресурси каналів і обладнання. Відсутність централізованого уявлення про стан усієї мережі не дозволяє визначити оптимальну точку блокування та оцінити масштаби загрози в

режимі реального часу [12].

П'яте обмеження має економічний характер. Традиційні мережі будуються на пропрієтарному обладнанні конкретних виробників, що створює залежність від постачальника (Vendor lock-in). Розширення або модернізація такої мережі потребує закупівлі обладнання того ж виробника за його цінами, а перехід до іншого вендора фактично означає повну заміну інфраструктури. Як буде показано в розділі 4, відмова від такої моделі на користь стандартизованого White-box обладнання дозволяє знизити капітальні витрати більш ніж на 57%.

Фундаментальна парадигма SDN: відокремлення площин.

Концепція Software Defined Networking (SDN) пропонує радикальну зміну традиційної парадигми шляхом логічного розділення площини управління та площини передачі даних [7].

Основна ідея SDN полягає в перенесенні інтелекту мережі (маршрутизації, управління політиками, забезпечення безпеки) на централізований вузол — SDN-контролер. Це дозволяє програмувати поведінку мережі в цілому, а не налаштовувати кожен окремий компонент.

В результаті такого розділення:

1. Data Plane (Рівень передачі даних): Мережеве обладнання (комутатори) перетворюється на прості, високопродуктивні пристрої, які лише виконують команди контролера, пересилаючи пакети згідно з наданими їм таблицями потоків (Flow Tables).

2. Control Plane (Рівень управління): Централізований SDN-контролер володіє повною топологічною картиною мережі в режимі реального часу, абстрагує базову інфраструктуру від додатків і сервісів, обчислює оптимальні маршрути та транслює високорівневі політики в конкретні правила для інфраструктурного обладнання.

Такий централізований підхід забезпечує майже миттєву швидкість збіжності завдяки глобальній видимості топології, що є критичним фактором для забезпечення необхідних параметрів QoS (якості обслуговування) та мінімізації повної затримки пакетів ($T = T_{proc} + T_{trans} + T_{prop} + T_{queue}$). Крім того, централізований контролер бачить усі спроби нестандартних з'єднань у

реальному часі, що дозволяє миттєво реагувати на загрози та ізолювати атаковані сегменти.

Стандартизація технології (роль Open Networking Foundation - ONF).

Для успішного впровадження нової парадигми необхідна була розробка єдиних відкритих стандартів, які б усунули залежність від пропрієтарних рішень окремих виробників. Провідну роль у цьому процесі відіграє організація Open Networking Foundation (ONF).

Згідно зі стандартами ONF, архітектура SDN формалізована у вигляді трьох ключових рівнів:

1. Прикладний рівень (Application Plane): Включає програмні додатки, які формують бізнес-логіку та реалізують мережеві сервіси (моніторинг, балансування навантаження, системи виявлення вторгнень IDS/IPS, управління безпекою)
2. Рівень управління (Control Plane): SDN-контролер або кластер контролерів.
3. Інфраструктурний рівень (Data Plane): Рівень фізичного або віртуального комутаційного обладнання.

Критичним досягненням ONF стала стандартизація інтерфейсів взаємодії між цими рівнями. Взаємодія між прикладним рівнем та контролером відбувається через Northbound API (зазвичай реалізується на базі RESTful API). Взаємодія між контролером та інфраструктурним рівнем здійснюється через Southbound API. Найпоширенішим та найважливішим протоколом Southbound-інтерфейсу, стандартизованим ONF, є протокол OpenFlow, який забезпечив практичну можливість безпосереднього маніпулювання таблицями потоків комутаторів з боку центрального контролера [2].

Перехід від апаратно-залежної інфраструктури до програмно-конфігурованої не лише оптимізує процеси маршрутизації, але й створює фундаментальний базис для побудови високозахищених телекомунікаційних мереж нового покоління.

2.2 Детальний аналіз трирівневої архітектури SDN

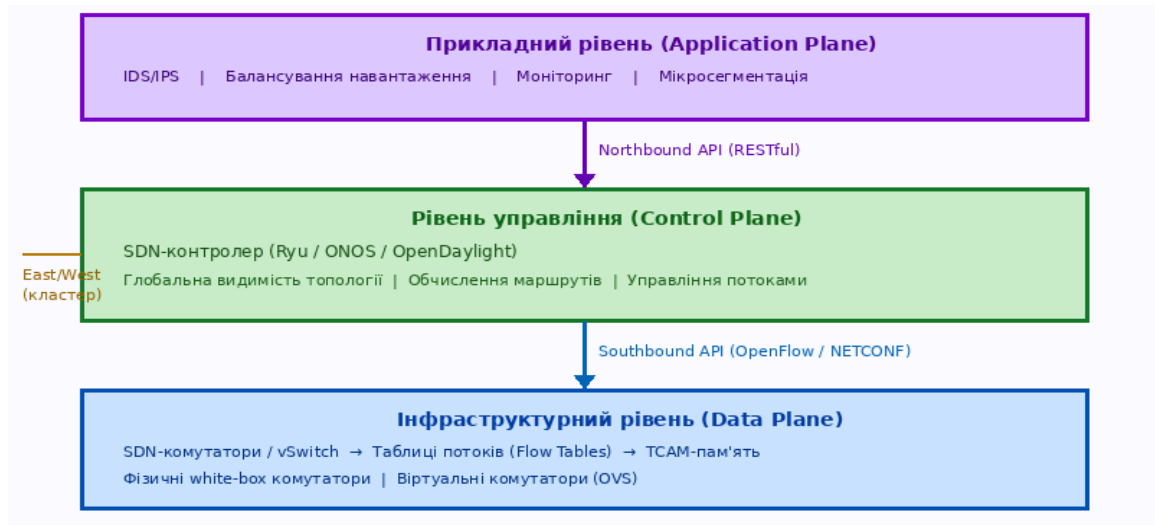


Рисунок 2.2 – Трирівнева архітектура SDN згідно зі стандартом ONF

Згідно зі стандартами організації ONF (Open Networking Foundation), архітектура програмно-конфігурованої мережі концептуально поділяється на три взаємопов'язані ключові рівні: інфраструктурний, рівень управління та прикладний [2]. Ця багаторівнева еталонна модель дозволяє абстрагувати складність фізичного обладнання від процесів розробки мережевих сервісів та політик кібербезпеки.

На інфраструктурному рівні зосереджене фізичне або віртуальне комутаційне обладнання — як апаратні White-box комутатори, так і програмні vSwitch рішення. Принципова відмінність від традиційних пристроїв полягає в тому, що SDN-комутатор не приймає самостійних рішень щодо маршрутизації. Він лише порівнює заголовки вхідних пакетів з таблицею потоків, отриманою від контролера, і виконує відповідну дію. Якщо відповідного запису в таблиці немає, комутатор не відкидає пакет, а відправляє його заголовок на контролер для прийняття рішення — цей механізм є основою динамічності SDN-мережі.

Комутатори інфраструктурного рівня виконують команди центрального контролера, здійснюючи комутацію пакетів виключно згідно з інструкціями, що містяться в таблицях потоків (Flow Tables) [3]. На відміну від класичної маршрутизації, що базується переважно на IP-адресі призначення, SDN використовує концепцію "потіку" (Flow). Потік може гнучко

ідентифікуватися за широкою сукупністю ознак, що охоплюють кілька рівнів моделі OSI:

1. MAC-адреси відправника та отримувача (L2);
2. IP-адреси та номери портів (L4);
3. Ідентифікатор VLAN або MPLS-мітка.

Така гранулярність класифікації трафіку безпосередньо на інфраструктурному рівні створює потужний базис для реалізації комплексних політик безпеки. Якщо комутатор отримує пакет, який не відповідає жодному існуючому правилу в таблиці потоків, він не відкидає його відразу, а формує спеціальне повідомлення (Packet-In) і надсилає заголовок пакета до рівня управління для прийняття рішення.

Рівень управління реалізується SDN-контролером, який виконує функції, що в традиційних мережах розподілені між десятками окремих пристроїв. Контролер збирає інформацію про топологію від усіх підключених комутаторів, обчислює оптимальні маршрути з урахуванням поточного стану мережі та формує правила для таблиць потоків. Критично важливо, що контролер робить це одночасно для всієї мережі, а не для окремих сегментів, що і забезпечує принципово іншу швидкість реагування на зміни порівняно з традиційними протоколами маршрутизації Data Plane [14].

З точки зору підвищення захищеності, централізований контролер виконує функцію глобального моніторингу, оскільки він бачить усі спроби нестандартних з'єднань (через повідомлення Packet-In). Це забезпечує динамічну реакцію на загрози: при виявленні атаки (наприклад, DoS-атаки, що спрямована на вичерпання ресурсів), контролер здатний миттєво оновити правила на всіх відповідних комутаторах, ефективно ізолюючи атакований сегмент мережі ще на периферії.

На практиці для реалізації рівня управління використовуються різні архітектури контролерів, залежно від масштабів мережі:

1. Ryu: Легковаговий контролер, написаний мовою Python, що широко застосовується для дослідницьких цілей, тестування алгоритмів безпеки та створення прототипів завдяки простоті розробки додатків.
2. ONOS (Open Network Operating System) та OpenDaylight (ODL):

Високопродуктивні платформи промислового рівня (Carrier-grade). Вони побудовані на базі Java та архітектури мікросервісів, що забезпечує високу масштабованість та відмовостійкість. Ці платформи дозволяють створювати кластери контролерів для обслуговування глобальних WAN-мереж або транспортних мереж операторів зв'язку (наприклад, 5G Core).

Прикладний рівень (Application Plane): реалізація мережевих сервісів та політик безпеки.

Прикладний рівень (Application Plane) формує найвищий рівень абстракції в архітектурі SDN. Він включає різноманітні програмні додатки, які реалізують кінцеві мережеві сервіси та бізнес-логіку інфраструктури.

Саме на цьому рівні розгортаються критично важливі для захищеності мережі компоненти: системи моніторингу трафіку, балансувальники навантаження, системи виявлення та запобігання вторгненням (IDS/IPS), а також комплексні системи управління політиками безпеки. Програми прикладного рівня не взаємодіють з комутаторами безпосередньо. Вони формують абстрактні вимоги (наприклад, "заблокувати трафік від підмережі А до сервера Б" або "направити весь HTTP-трафік користувача через систему глибокого аналізу пакетів DPI"), передають їх контролеру, а той вже перетворює ці вимоги на набір низькорівневих OpenFlow-правил.

Крім того, прикладний рівень дозволяє реалізувати механізм мікросегментації — створення повністю ізольованих віртуальних мереж для різних груп користувачів або типів трафіку на спільній фізичній інфраструктурі, що значно підвищує рівень безпеки без необхідності використання громіздких та складних в адмініструванні класичних ACL (Access Control Lists) [12].

Інтерфейси взаємодії (Northbound, Southbound, East/West API).

Логічне розділення архітектури на три рівні вимагає надійних та стандартизованих протоколів для комунікації між ними. У SDN використовуються три основні типи програмних інтерфейсів (API):

1. Southbound API (Південні інтерфейси): Забезпечують взаємодію між рівнем управління (контролером) та інфраструктурним рівнем (комутаторами). Найпоширенішим та найважливішим стандартом тут є

протокол OpenFlow. Він дозволяє контролеру дистанційно маніпулювати таблицями потоків, отримувати статистику портів та керувати станом фізичного обладнання. Також як Southbound-протоколи можуть використовуватися NETCONF або RESTCONF, що базуються на мові моделювання даних YANG і забезпечують надійну доставку конфігурацій [3].

2. Northbound API (Північні інтерфейси): Використовуються для взаємодії програмних додатків (Application Plane) із контролером (Control Plane). Як правило, вони реалізуються на базі RESTful API. Northbound API абстрагує складність інфраструктури: розробнику системи безпеки не потрібно знати фізичну топологію або моделі комутаторів; він використовує універсальні методи API для запиту послуг мережі або встановлення правил доступу.

3. East/West API (Східні/Західні інтерфейси): Хоча класична архітектура SDN передбачає централізоване управління, використання єдиного фізичного сервера-контролера створює "єдину точку відмови" (Single point of failure), що є критичним недоліком для масштабованих та надійних мереж. Для вирішення цієї проблеми контролери об'єднуються у кластери. Інтерфейси East/West забезпечують синхронізацію баз даних топології, стану потоків та політик між різними екземплярами SDN-контролерів (наприклад, між доменами різних дата-центрів). Це гарантує безперервність управління мережею (високу доступність) навіть у разі апаратної відмови одного з контролерів [14].

2.3 Механізми управління потоками та протокол OpenFlow

Фундаментальною відмінністю програмно-конфігурованих мереж від класичних є перехід від маршрутизації на основі окремих пакетів до управління на основі інформаційних потоків (Flow-based routing) [3]. Ця парадигма реалізується за допомогою стандартизованих протоколів, серед яких домінуючу роль відіграє OpenFlow.

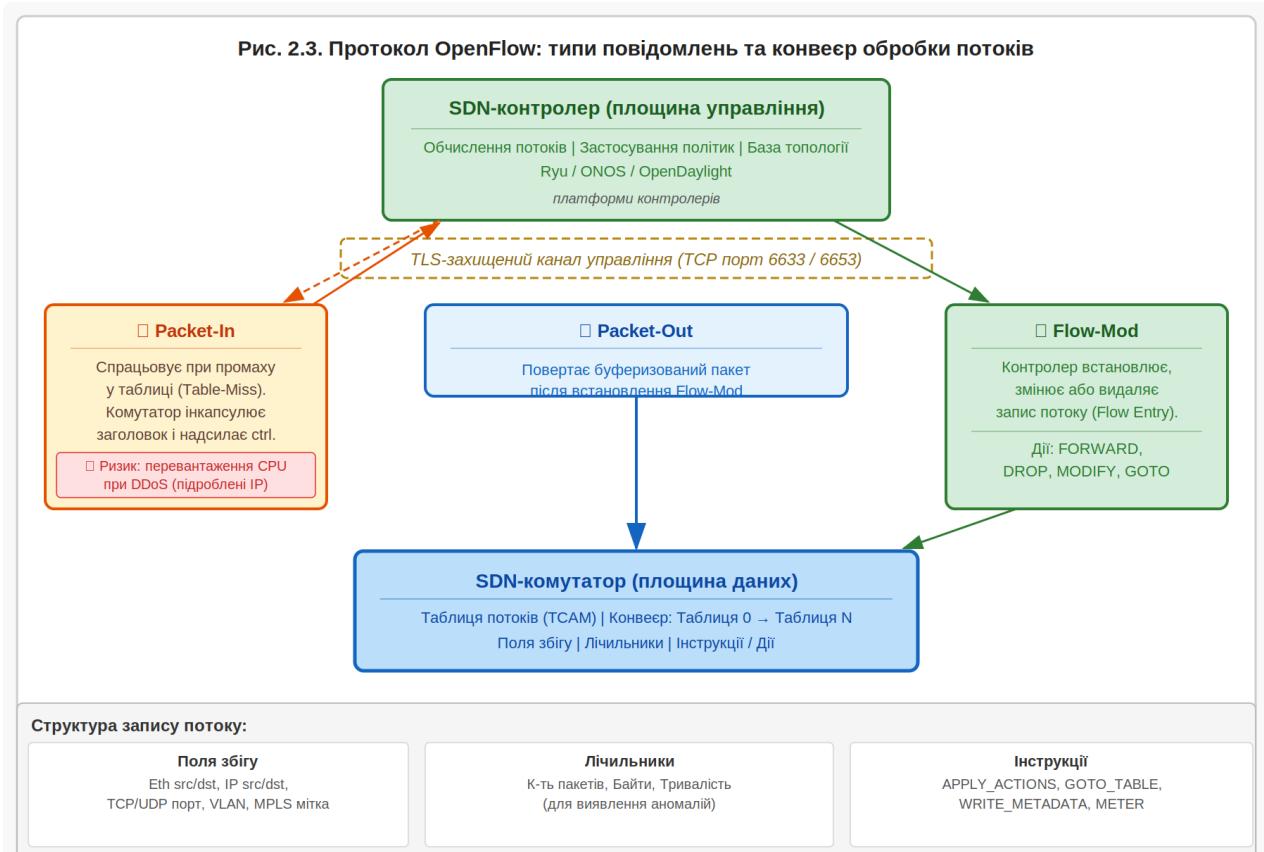


Рисунок 2.3 – Обмін повідомленнями OpenFlow та структура запису таблиці потоків

Принципи маршрутизації на основі потоків порівняно з пакетною маршрутизацією.

Традиційний підхід до побудови мережевої інфраструктури базується на інтеграції функцій управління та передачі даних безпосередньо всередині кожного окремого мережевого пристрою. Класичний маршрутизатор обробляє кожен пакет ізольовано: він зчитує IP-адресу призначення (або MAC-адресу в разі комутації на рівні L2), звертається до своєї локальної таблиці маршрутизації та приймає рішення про вихідний порт. Такий підхід вимагає значних обчислювальних ресурсів на кожному вузлі та обмежує гнучкість управління трафіком.

На відміну від класичної маршрутизації за IP-адресою призначення, у SDN використовується поняття "потoku" (Flow). Потік визначається як послідовність пакетів, що проходять через мережу і мають спільний набір характеристик. Цей набір може ідентифікуватися за сукупністю ознак, що охоплюють відразу кілька рівнів моделі OSI:

1. MAC-адреси відправника та отримувача на каналному рівні;
2. IP-адреси та номери портів (L4) на мережевому та транспортному рівнях;
3. Ідентифікатор VLAN або MPLS-мітка.

Маршрутизація на основі потоків забезпечує суттєві переваги для підвищення захищеності. Вона дозволяє реалізувати гнучкі політики безпеки, оскільки трафік певного користувача (або підозрілий трафік) може бути виділений в окремий потік і спрямований через ланцюжок віртуальних функцій безпеки (Service Chaining) перед тим, як потрапити в ядро мережі. Традиційні мережі для досягнення подібної гранулярності вимагають створення складних, ресурсоємних і важких в адмініструванні списків контролю доступу (ACL) на кожному пристрої.

Структура таблиць потоків (Flow Tables) та конвеєрна обробка.

Комутатори в середовищі SDN лише виконують команди контролера, пересилаючи пакети згідно з таблицями потоків (Flow Tables) [3]. Кожен запис (Flow Entry) у такій таблиці зазвичай складається з трьох основних компонентів:

1. Поля збігу (Match Fields): Набір параметрів заголовка пакета (MAC, IP, порти тощо), з якими порівнюється кожен вхідний пакет.
2. Лічильники (Counters): Збирають статистику щодо потоку (кількість переданих пакетів, байтів, час існування потоку). Ці дані є критично важливими для систем моніторингу продуктивності (Performance Management) та виявлення аномалій (наприклад, DDoS-атак).
3. Інструкції/Дії (Instructions/Actions): Визначають, що саме комутатор має зробити з пакетом у разі збігу (переслати на певний порт, відкинути, змінити заголовок або направити в іншу таблицю).

Сучасні специфікації OpenFlow підтримують конвеєрну обробку пакетів (Pipeline Processing). Замість однієї громіздкої таблиці комутатор може мати кілька послідовних таблиць потоків (Table 0, Table 1, ..., Table N). Пакет завжди починає обробку з Table 0. Якщо дія в правилі містить інструкцію.

GOTO_TABLE, пакет передається до наступної таблиці для подальшого аналізу. Це дозволяє логічно розділити завдання: наприклад, Table 0 може

відповідати за первинну фільтрацію MAC-адрес (L2 Security), Table 1 — за маршрутизацію L3, а Table 2 — за реалізацію політик QoS (Quality of Service).

Типи повідомлень OpenFlow та їх роль у забезпеченні динамічності мережі

Протокол OpenFlow є основним стандартом взаємодії між рівнем управління (SDN-контролером) та рівнем передачі даних (комутаторами). Його архітектура дозволяє контролеру безпосередньо маніпулювати таблицями потоків комутаторів.

Взаємодія здійснюється через захищений канал зв'язку за допомогою трьох ключових типів повідомлень [3]:

1. Повідомлення Packet-In є ключовим механізмом взаємодії між рівнями SDN. Коли комутатор отримує пакет, для якого немає відповідного запису в таблиці потоків, він інкапсулює заголовок цього пакету і передає його контролеру. Контролер аналізує заголовок, приймає рішення і відправляє назад правило через Flow-Mod, яке комутатор застосовує до всіх наступних пакетів цього потоку. Важливо розуміти, що цей механізм має подвійну природу з точки зору безпеки: з одного боку, він дає контролеру повну видимість нових з'єднань, з іншого — створює вразливість, оскільки зломисник може генерувати пакети з постійно змінними адресами, змушуючи комутатор безперервно звертатися до контролера і тим самим вичерпувати його ресурси.

2. Повідомлення Flow-Mod є основним інструментом реалізації політик безпеки в SDN-мережі. Контролер надсилає його комутатору для встановлення, зміни або видалення запису в таблиці потоків. З практичної точки зору це означає, що при виявленні атаки системою аналізу аномалій контролер одним API-викликом формує набір Flow-Mod повідомлень і розсилає їх одночасно на всі відповідні комутатори мережі. Весь процес від виявлення до блокування займає менше 500 мс, тоді як в традиційній мережі адміністратор витратив би на це десятки хвилин ручного налаштування.

3. Packet-Out: Повідомлення, що використовується контролером для примусової відправки певного пакету через конкретний порт комутатора. Зазвичай це застосовується безпосередньо після того, як контролер обробив

повідомлення *Packet-In*. Після створення нового правила через *Flow-Mod*, контролер повертає затриманий перший пакет назад комутатору через *Packet-Out* для його успішної доставки отримувачу, тоді як усі наступні пакети цього потоку оброблятимуться комутатором самостійно і на апаратній швидкості [3].

Завдяки такій архітектурі, протокол OpenFlow перетворює мережу з набору статичних вузлів на програмовану, гнучку систему, здатну адаптивно змінювати свою топологію та політики доступу в режимі реального часу, забезпечуючи високий рівень стійкості до зовнішніх впливів.

2.4 Віртуалізація мережевих функцій (NFV) та її інтеграція з SDN

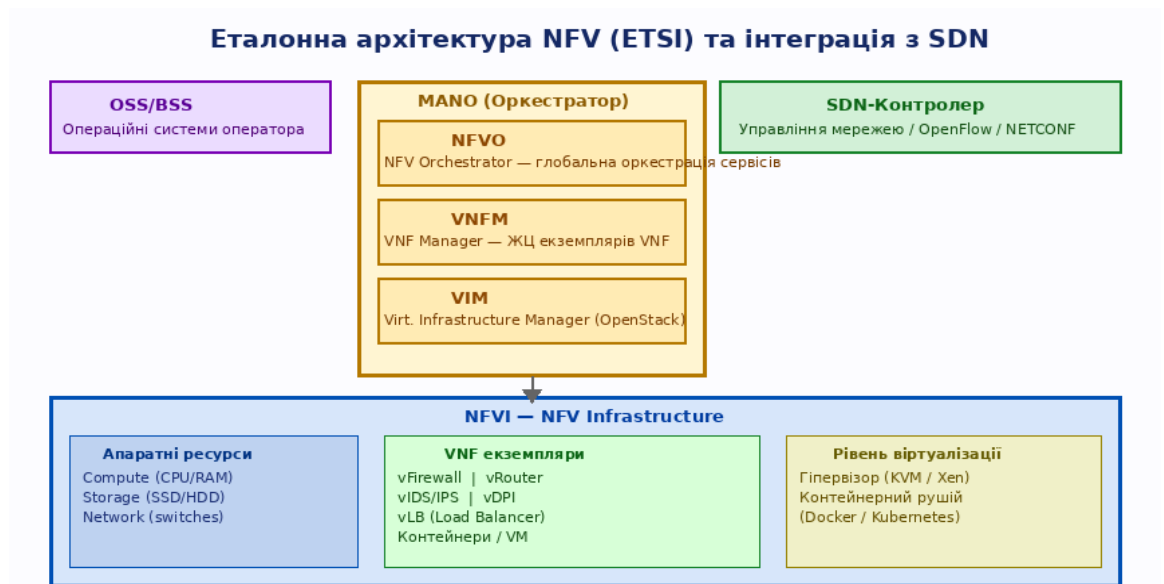


Рисунок 2.4 – Еталонна архітектура NFV (ETSI MANO) та її інтеграція з SDN-контролером

Розвиток програмно-конфігурованих мереж нерозривно пов'язаний з відмовою від жорсткої прив'язки мережевих сервісів до спеціалізованого апаратного забезпечення. NFV (Network Function Virtualization) є комплементарною технологією до SDN. В той час як SDN розділяє рівні управління та передачі, NFV переносить мережеві сервіси з виділених пристроїв на стандартне серверне обладнання (COTS) [4]. Завдяки цьому підходу, функції управління, такі як брандмауери, балансувальники навантаження та контролери, переносяться на стандартні сервери у вигляді віртуальних машин або контейнерів.

Концепція NFV за стандартами ETSI.

Фундаментальні принципи та еталонна архітектура NFV розробляються та стандартизуються Європейським інститутом телекомунікаційних стандартів (ETSI). Основна мета ETSI NFV полягає у створенні відкритого, інтероперабельного середовища, яке дозволяє телекомунікаційним операторам уникнути залежності від пропрієтарного обладнання (Vendor lock-in).

Згідно з еталонною моделлю ETSI, інфраструктура віртуалізації (NFVI — NFV Infrastructure) охоплює всі апаратні ресурси (обчислювальні потужності, сховища даних, мережеві комутатори) та програмний рівень віртуалізації (гіпервізори або контейнерні рушії), які створюють середовище для виконання віртуалізованих завдань. Перехід на таку модель забезпечує суттєве зменшення капітальних витрат (CAPEX) на закупівлю спеціалізованого заліза та значно пришвидшує впровадження нових сервісів.

Віртуальні мережеві функції (VNF) та їх оркестрація (MANO).

Ключовим елементом технології є віртуальні мережеві функції (VNF — Virtual Network Functions). VNF — це програмна реалізація традиційного мережевого обладнання. Замість встановлення фізичного маршрутизатора або апаратного криптографічного шлюзу, оператор розгортає їх програмні аналоги поверх NFVI.

Для управління цим складним середовищем ETSI визначає архітектурний фреймворк MANO (Management and Orchestration), який складається з трьох основних компонентів:

1. NFVO (NFV Orchestrator): Відповідає за оркестрацію мережевих сервісів у масштабах усієї інфраструктури, управляючи глобальними ресурсами та координуючи розгортання складних топологій.

2. VNFM (VNF Manager): Керує життєвим циклом конкретних екземплярів VNF (ініціалізація, конфігурування, масштабування, оновлення та термінація).

3. VIM (Virtualized Infrastructure Manager): Безпосередньо контролює та управляє обчислювальними, мережевими ресурсами та ресурсами зберігання на рівні NFVI (найвідомішим прикладом VIM є платформа OpenStack) [4].

Взаємодоповнюваність SDN та NFV для створення еластичної та захищеної інфраструктури.

Хоча SDN та NFV є незалежними концепціями, їх синергія формує базис для побудови захищених мереж нового покоління. Найвищі вимоги безпеки та низька затримка характерні для 5G URLLC, що потребує SDN/NFV підходів. SDN забезпечує інтелектуальну, програмовану маршрутизацію потоків, тоді як NFV надає необхідні обчислювальні ресурси для глибокої обробки цих потоків.

Однією з найважливіших переваг такої інтеграції є віртуалізація безпеки: брандмауери (vFirewall) та системи IDS/IPS розгортаються як віртуальні машини, що дозволяє масштабувати їх за запитом. Традиційні апаратні засоби безпеки мають фіксовану пропускну здатність і стають "вузьким місцем" (bottleneck) під час масштабних кібератак. Використання NFV гарантує еластичність: можливість швидкого виділення ресурсів для обробки пікових навантажень.

На практиці об'єднання SDN та NFV реалізується через механізм Service Function Chaining (SFC). У разі виявлення контролером SDN підозрілого трафіку (наприклад, аномального зростання кількості запитів, що свідчить про початок DDoS-атаки), оркестратор MANO автоматично ініціює створення додаткових екземплярів vFirewall або vDPI (Deep Packet Inspection). Одразу після цього SDN-контролер модифікує таблиці потоків (Flow-Mod) на комутаторах таким чином, щоб динамічно перенаправити підозрілий трафік через новостворений ланцюжок віртуальних сервісів безпеки для очищення.

Після нормалізації ситуації віртуальні машини автоматично видаляються, вивільняючи ресурси дата-центру. Такий проактивний підхід дозволяє локалізувати загрози без впливу на загальну архітектуру та якість обслуговування (QoS) легітимних абонентів [15].

2.5 Аналіз нових векторів атак та вразливостей у середовищі SDN

Захищеність мережі визначається її здатністю протидіяти загрозам, що впливають на конфіденційність, цілісність та доступність даних.

Перехід до централізованої архітектури SDN усуває низку проблем традиційних мереж, однак одночасно формує новий клас загроз, специфічних саме для цієї парадигми. Якщо в традиційній мережі компрометація одного маршрутизатора впливає лише на той сегмент, яким він управляє, то в SDN-середовищі успішна атака на контролер потенційно дає зловмиснику контроль над усією мережевою інфраструктурою. Саме тому аналіз векторів атак у SDN-середовищі є необхідною передумовою для розробки ефективної системи захисту, що і є предметом третього розділу цієї роботи.

Для успішного підвищення захищеності мережі необхідно провести детальну класифікацію цих вразливостей за рівнями архітектури SDN.



Рисунок 2.5 – Класифікація векторів атак та вразливостей в архітектурі SDN за рівнями

Вразливості контролера (Control Plane).

Рівень управління є найкритичнішим елементом SDN, оскільки саме тут зосереджено весь "інтелект" мережі. Компрометація або виведення з ладу контролера означає повну втрату контролю над інфраструктурою.

1. Єдина точка відмови (Single Point of Failure): У класичній реалізації SDN контролер є єдиним логічним центром прийняття рішень. Апаратна відмова сервера, на якому розгорнуто контролер, програмний збій у його ядрі або успішна хакерська атака призводять до того, що комутатори втрачають здатність обробляти нові потоки трафіку. Хоча існуючі потоки

можуть продовжувати передаватися за вже встановленими правилами, мережа втрачає здатність до адаптації та маршрутизації нових з'єднань.

2. DDoS-атаки на рівні управління (Control Plane DoS/DDoS): Окрім стандартних DDoS-атак, що спрямовані на перевантаження фізичних каналів (і становлять понад 90% усіх інцидентів), в SDN з'являється загроза вичерпання ресурсів самого контролера. Атака реалізується шляхом генерації зломисником величезної кількості пакетів із випадковими, постійно змінними IP- та MAC-адресами (Spoofing).

Оскільки комутатор рівня передачі даних не знаходить правил для цих пакетів у своїх таблицях потоків (Table Miss), він змушений інкапсулювати кожен такий пакет у повідомлення *Packet-In* і відправляти його контролеру. Це призводить до катастрофічного перевантаження центрального процесора (CPU) та оперативної пам'яті контролера, паралізуючи його здатність обслуговувати легітимний трафік та оновлювати легітимні маршрути [13].

Вразливості інтерфейсів зв'язку.

Канали комунікації між рівнями SDN (Northbound та Southbound API) є потенційними мішенями для перехоплення та модифікації даних.

1. Ризики перехоплення (Man-in-the-Middle) на Southbound API: Протокол OpenFlow за замовчуванням може працювати у відкритому вигляді (Plain text), якщо адміністратори не налаштували належним чином шифрування. Це створює загрозу Man-in-the-Middle — перехоплення сесій управління між комутатором і контролером. Зломисник, який отримав доступ до каналу зв'язку, може не лише прослуховувати топологічну інформацію, але й модифікувати повідомлення Flow-Mod, відкидати Packet-In запити або надсилати фальшиві статусні повідомлення від імені комутатора. Для мінімізації цього ризику стандарти вимагають обов'язкового використання протоколу TLS (Transport Layer Security) із взаємною автентифікацією на основі сертифікатів [16].

2. Вразливості Northbound API: Інтерфейси, через які прикладні програми (Application Plane) взаємодіють з контролером, зазвичай базуються на REST API. Відсутність суворої автентифікації, авторизації (RBAC) та валідації вхідних даних на цьому рівні дозволяє зломисникам впроваджувати

шкідливі додатки. Такий скомпрометований додаток отримує легітимний доступ до контролера і може змусити його змінити глобальну політику маршрутизації на користь атакуючого.

Специфічні атаки на інфраструктурний рівень (Data Plane).

Хоча комутатори SDN є "простими" пристроями, вони мають специфічні апаратні та логічні вразливості.

1. Підміна правил (Flow Poisoning): Окрім стандартних загроз, в SDN з'являється ризик Flow poisoning — підміни таблиць потоків, що може призвести до несанкціонованого перехоплення трафіку. Ця атака може бути реалізована через компрометацію контролера або через експлуатацію вразливостей у самому механізмі розпізнавання топології мережі (наприклад, підміна пакетів LLDP — Link Layer Discovery Protocol). Зловмисник змушує контролер повірити у хибну топологію, внаслідок чого легітимний трафік спрямовується через вузол атакуючого, реалізуючи таким чином прихований моніторинг або "чорну діру" (Blackholing), коли трафік просто знищується.

2. Переповнення таблиць потоків (Flow Table Overflow): SDN-комутатори використовують спеціалізовану, дуже швидку, але обмежену за обсягом та дорогою пам'ять типу TCAM (Ternary Content-Addressable Memory) для зберігання таблиць потоків. Зазвичай TCAM підтримує від кількох тисяч до десятків тисяч записів. Зловмисник може ініціювати велику кількість унікальних з'єднань з мінімальним інтервалом. Контролер, діючи за стандартною логікою, згенерує для кожного з'єднання нове правило (*Flow-Mod*) і відправить його на комутатор. Це швидко призведе до повного вичерпання апаратного ліміту пам'яті TCAM. В результаті комутатор втратить здатність зберігати нові правила для легітимного трафіку, що спричинить значну деградацію пропускної здатності та екстремальне зростання затримок через постійне звернення до контролера [13].

Отже, вирішення проблеми захищеності телекомунікаційних мереж на базі SDN вимагає комплексного підходу: від впровадження кластеризації на рівні управління до розробки інтелектуальних алгоритмів виявлення аномалій (наприклад, на базі машинного навчання), які здатні відрізнити легітимний самоподібний трафік від цілеспрямованих атак на вичерпання ресурсів

контролера та пам'яті комутаторів.

2.6 Дослідження методів підвищення захищеності мереж за допомогою SDN/NFV

Аналіз векторів атак, проведений у підрозділі 2.5, показав, що централізація управління є водночас і вразливістю, і перевагою SDN з точки зору безпеки. Вразливістю — тому що контролер є єдиною точкою відмови. Перевагою — тому що той самий контролер дозволяє реалізувати механізми захисту, недосяжні в децентралізованих мережах. У цьому підрозділі розглядаються конкретні механізми, що перетворюють централізацію з вразливості на інструмент захисту.

Мікросегментація та динамічна ізоляція скомпрометованих вузлів.

Традиційний підхід до ізоляції мережесегментів базується на використанні технологій VLAN та складних списків контролю доступу (ACL) на фізичних інтерфейсах маршрутизаторів. Цей метод характеризується високою складністю конфігурування, схильністю до людських помилок при налаштуванні через CLI та обмеженою масштабованістю.

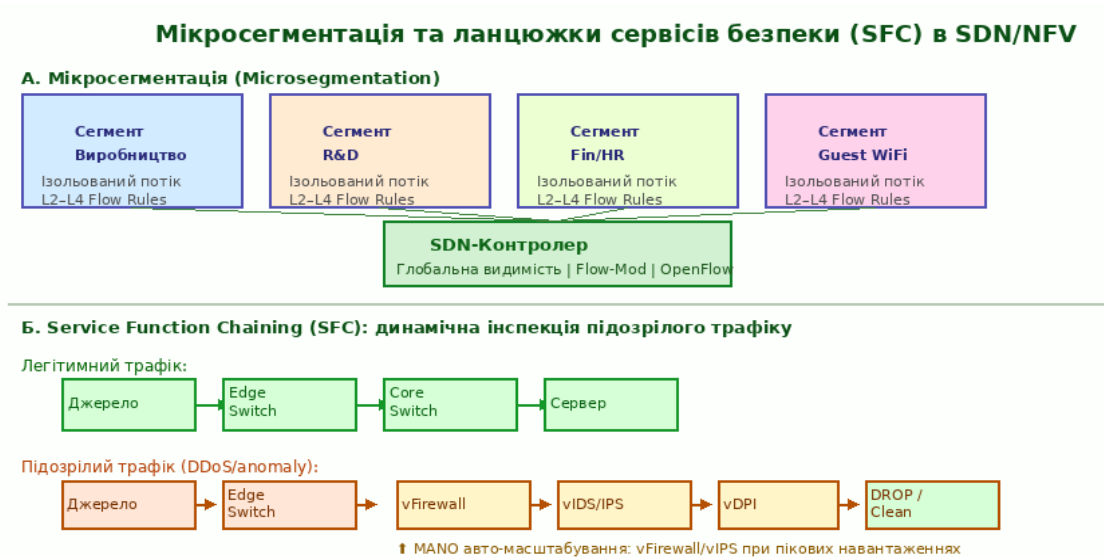


Рисунок 2.6 – Мікросегментація та Service Function Chaining (SFC) для захисту мережі SDN/NFV

Архітектура SDN дозволяє реалізувати парадигму мікросегментації —

можливість створювати повністю ізольовані віртуальні мережі для різних груп користувачів, додатків або навіть окремих пристроїв на спільній фізичній інфраструктурі без використання складних ACL. Оскільки SDN-контролер оперує потоками (Flows), визначеними за сукупністю ознак L2-L4 рівнів (MAC, IP, порти, VLAN ID), він може гранулярно дозволяти або забороняти взаємодію між будь-якими двома вузлами мережі.

Завдяки централізованому моніторингу контролер бачить усі спроби нестандартних з'єднань у реальному часі. Динамічна реакція на загрози реалізується наступним чином: при виявленні атаки (наприклад, DoS-атаки чи спроби несанкціонованого доступу), система управління безпекою на прикладному рівні (Application Plane) формує нову політику, а контролер миттєво оновлює правила таблиць потоків через повідомлення OpenFlow (Flow-Mod) на всіх комутаторах. Це дозволяє не просто заблокувати зловмисника на рівні ядра мережі, а миттєво ізолювати атакований або скомпрометований сегмент на найближчому до нього периферійному комутаторі (Edge Switch), запобігаючи горизонтальному поширенню атаки (Lateral Movement) всередині інфраструктури [12].

Ланцюжки сервісів безпеки (Service Function Chaining - SFC) для інспекції трафіку.

Традиційна інтеграція засобів безпеки вимагає фізичного підключення апаратних брандмауерів або систем запобігання вторгненням (IPS) у "розрив" мережі, що створює "вузькі місця" і погіршує масштабованість.

Інтеграція SDN та NFV (Network Function Virtualization) вирішує цю проблему через технологію Service Function Chaining (SFC). У середовищі SDN трафік певного підозрілого користувача або додатку може бути динамічно спрямований через ланцюжок віртуальних функцій безпеки перед тим, як потрапити в ядро мережі. Брандмауери (vFirewall) та системи виявлення/запобігання вторгненням (IDS/IPS) розгортаються як віртуальні машини, що дозволяє масштабувати їх за запитом.

Процес інспекції працює так:

1. За замовчуванням легітимний "чистий" трафік комутується апаратно на інфраструктурному рівні за найкоротшим маршрутом, забезпечуючи мінімальні затримки.
2. При ідентифікації підозрілої активності, SDN-контролер модифікує правила маршрутизації для конкретного потоку.
3. Потік примусово "загортається" (Steering) на віртуалізовані сервери безпеки (VNF), де проходить глибоку інспекцію пакетів (DPI) [15].
4. Завдяки еластичності технології NFV, система має можливість швидкого виділення додаткових обчислювальних ресурсів для обробки пікових навантажень. Якщо обсяг шкідливого трафіку зростає, оркестратор (MANO) автоматично створює нові віземпляри vFirewall або vIPS, запобігаючи перевантаженню. Після очищення легітимні пакети повертаються в мережу, а віртуальні ресурси вивільняються. Це суттєво зменшує капітальні витрати (CAPEX) на закупівлю спеціалізованого заліза.

Проактивний та реактивний підходи до управління безпекою та зменшення затримок (T_{queue}).

Управління безпекою в SDN реалізується через дві основні моделі: реактивну та проактивну.

1. Реактивний підхід базується на тому, що комутатор надсилає перший пакет невідомого потоку (Packet-In) до контролера для прийняття рішення. Цей метод забезпечує високу гнучкість, але під час DDoS-атак, які становлять понад 90% інцидентів та спрямовані на перевантаження каналів, масова генерація таких запитів перевантажує контролер і спричиняє екстремальні затримки.

2. Проактивний підхід передбачає попереднє встановлення контролером правил (Flow-Mod) на комутаторах ще до фактичного надходження трафіку. Використання машинного навчання та предиктивної аналітики на прикладному рівні SDN дозволяє заздалегідь формувати захисні політики для відомих патернів атак, мінімізуючи взаємодію комутаторів із контролером під час інциденту [13].

Критичним наслідком будь-якої кібератаки є порушення параметрів

якості обслуговування (QoS), зокрема зростання повної затримки пакета. Загальна затримка передачі (T) складається з затримки обробки (T_{proc}), трансмісії (T_{trans}), поширення (T_{prop}) та затримки черги (T_{queue}). Переповнення черг (T_{queue}) є основною причиною втрати пакетів. Затримка черги є найбільш нестабільною компонентою і може сягати 1-50 мс у бездротових мережах [11].

Високе значення коефіцієнта Херста ($H > 0.5$) у сучасному самоподібному трафіку додатково призводить до різкого збільшення затримок у чергах (T_{queue}), навіть при низькому середньому завантаженні каналу. Наслідки високої затримки критичні: для критичних сервісів 5G URLLC затримка повинна бути <1 мс, а її перевищення може призвести до аварії автопілота. Для VoIP розмова стає неможливою при затримці >150 мс.

Впровадження SDN-архітектури дозволяє мінімізувати ці ризики. Оскільки SDN-контролер забезпечує майже миттєву швидкість збіжності завдяки глобальній видимості топології, він здатен проактивно балансувати навантаження між резервними лініями (наприклад, переключаючи трафік на резервні шляхи протягом 50 мс в кільцевих архітектурах). Швидке виявлення та дроп шкідливого трафіку на кордоні мережі звільняє буфери комутаторів, гарантуючи мінімізацію T_{queue} та підтримку рівня доступності "п'ять дев'яток" (99.999%) для критичних даних.

2.7 Висновки до розділу 2

За результатами дослідження другого розділу можна зробити декілька практично важливих висновків. По-перше, традиційні децентралізовані мережі мають структурні обмеження у сфері безпеки, які не можна усунути без зміни архітектурної парадигми — надто повільна збіжність і відсутність глобального бачення трафіку роблять ефективне реагування на сучасні атаки неможливим. По-друге, централізована архітектура SDN з протоколом OpenFlow створює технічну основу для принципово іншого підходу до захисту, де реакція на загрозу вимірюється мілісекундами, а не хвилинами. По-третє, інтеграція SDN з технологією NFV через механізм SFC дозволяє будувати еластичну систему захисту, що автоматично масштабується відповідно до рівня загрози без

залучення додаткового апаратного забезпечення. Ці висновки є основою для розробки конкретної архітектури захищеної мережі в третьому розділі.

3 РОЗРОБКА ТА ОЦІНКА КОМПЛЕКСНОЇ СИСТЕМИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА БАЗІ SDN

3.1 Концептуальна модель захищеної SDN-архітектури

На основі результатів аналізу векторів атак та методів захисту, проведеного у розділі 2, у даному розділі розробляється комплексна система підвищення захищеності телекомунікаційних мереж на базі програмно-конфігурованих мереж (SDN). Запропонована модель спирається на чотири фундаментальні принципи: централізований моніторинг, динамічне реагування, ешелонований захист та верифікація кожного компонента взаємодії [12].

Концептуальна модель захищеної SDN-архітектури базується на розширенні стандартної тривірневої архітектури ONF шляхом додавання виділеного рівня безпеки (Security Plane), що інтегрується між прикладним рівнем та рівнем управління [12]. Це дозволяє централізувати логіку безпеки, не порушуючи при цьому стандартних протоколів взаємодії між рівнями SDN.

Запропонована чотириланкова модель включає такі компоненти:

1. Захищений інфраструктурний рівень (Secured Data Plane) — комутатори з обов'язковим TLS-шифруванням Southbound-каналу [16], апаратною аутентифікацією LLDP-пакетів [21] та механізмом обмеження швидкості генерації Packet-In повідомлень (rate-limiting) для захисту від ресурсо-виснажуючих атак на контролер [13].

2. Кластеризований рівень управління (Clustered Control Plane) — розгортання ONOS-кластера з трьох і більше вузлів, синхронізованих через East/West API [14]. Це усуває єдину точку відмови (Single Point of Failure) та забезпечує автоматичне відновлення управління при відмові одного вузла контролера з часом перемикання менше 1 секунди.

3. Рівень безпеки (Security Plane) — виділений прикладний модуль, що реалізує функції: аналізу аномалій трафіку на базі машинного навчання (ML-based anomaly detection), управління політиками доступу через Role-Based Access Control (RBAC), верифікації топологічних оновлень та кореляції подій безпеки (SIEM-інтеграція) [19].

4. Прикладний рівень з оркестрацією NFV — додатки безпеки (vFirewall, vIPS, vDPI) розгортаються як віртуальні мережеві функції (VNF) під управлінням MANO-оркестратора. Механізм Service Function Chaining (SFC) динамічно скеровує підозрілий трафік через ланцюжок функцій інспекції [15].

Ключовою особливістю запропонованої моделі є принцип "Zero Trust" — жодний вузол мережі не є апіорно довіреним [18]. Кожне з'єднання підлягає верифікації незалежно від того, надходить воно із зовнішньої мережі чи з внутрішнього сегмента. Це кардинально відрізняє запропоновану архітектуру від традиційного периметрального підходу та від стандартних реалізацій SDN, що не передбачають обов'язкової взаємної автентифікації внутрішніх вузлів.

Взаємодія між компонентами реалізується через суворо регламентовані захищені канали: OpenFlow over TLS (версія 1.3 і вище) для Southbound API, HTTPS з OAuth 2.0 і JWT-токенами для Northbound API, а також mTLS для East/West синхронізації кластера контролерів.



Рисунок 3.1 – Архітектура SDN

3.2 Модель загроз та класифікація вразливостей захищеної SDN-мережі

Перед розробкою механізмів захисту необхідно формалізувати модель

загроз для SDN-середовища. Використання методології STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), стандартизованої в галузі аналізу загроз, дозволяє систематично класифікувати вразливості за їхнім впливом на компоненти архітектури [17].

Результати аналізу загроз для кожного рівня SDN-архітектури узагальнено в таблиці 3.1, де для кожного типу загрози визначено вектор атаки та відповідний контрзахід.

Таблиця 3.1 — Модель загроз для SDN-архітектури (за методологією STRIDE)

Тип загрози	Вектор атаки	Контрзахід
DoS/DDoS на контролер	Перевантаження CPU контролера через масові Packet-In	Rate-limiting Packet-In [13], кластеризація контролерів (ONOS) [14]
Flow Poisoning	Підміна таблиць потоків через скомпрометований канал Southbound	TLS-шифрування OpenFlow, цифрові сертифікати [16]
Man-in-the-Middle	Перехоплення сесій управління між комутатором і контролером	Mutual TLS authentication, VPN-тунелі управління [16]
Flow Table Overflow	Вичерпання пам'яті TCAM комутаторів через унікальні потоки	Проактивне встановлення wildcard-правил, агрегація потоків [13]
Northbound API exploit	Впровадження шкідливих додатків через REST API контролера	RBAC, OAuth 2.0, валідація вхідних даних [20]
LLDP Spoofing	Підміна пакетів LLDP для формування хибної топології	Автентифікація LLDP-пакетів, HMAC-підписи [21]
Lateral Movement	Горизонтальне поширення атаки між сегментами	Мікросегментація, динамічна ізоляція Edge Switch [12]
Replay-атака	Повтор перехоплених Flow-Mod команд	Нумерація повідомлень, часові мітки, TLS sequence

Аналіз таблиці 3.1 підтверджує, що найбільш критичними є атаки на рівень управління (Control Plane), зокрема DoS/DDoS на контролер [13] та Flow Poisoning. Компрометація контролера фактично означає втрату контролю над всією інфраструктурою, що робить захист цього рівня пріоритетним завданням.

Слід окремо підкреслити специфіку атаки типу Flow Table Overflow. На відміну від традиційних мереж, де переповнення таблиць маршрутизації є рідкісним явищем, у SDN-середовищі пам'ять TCAM комутатора є фізично обмеженою (зазвичай 1 000–32 000 записів), а кожен унікальний потік потребує окремого запису. Зловмисник, генеруючи потоки зі змінними характеристиками, здатний вичерпати цей ресурс за лічені хвилини, призводячи до деградації пропускну здатності та зростання компоненти затримки черги T_{queue} , що є неприйнятним для сервісів 5G URLLC з вимогою затримки менше 1 мс.

3.3 Механізми захисту рівня управління: кластеризація та автентифікація

Захист рівня управління є ключовим пріоритетом у запропонованій системі, оскільки контролер є централізованим «інтелектом» мережі. Реалізація надійного захисту цього рівня передбачає вирішення двох основних завдань: усунення єдиної точки відмови та забезпечення цілісності каналів управління.

Розгортання кластера SDN-контролерів на базі платформи ONOS (Open Network Operating System) є основним механізмом забезпечення відмовостійкості рівня управління. ONOS підтримує архітектуру розподіленого ядра (distributed core) з автоматичним розподілом відповідальності між вузлами кластера [14].

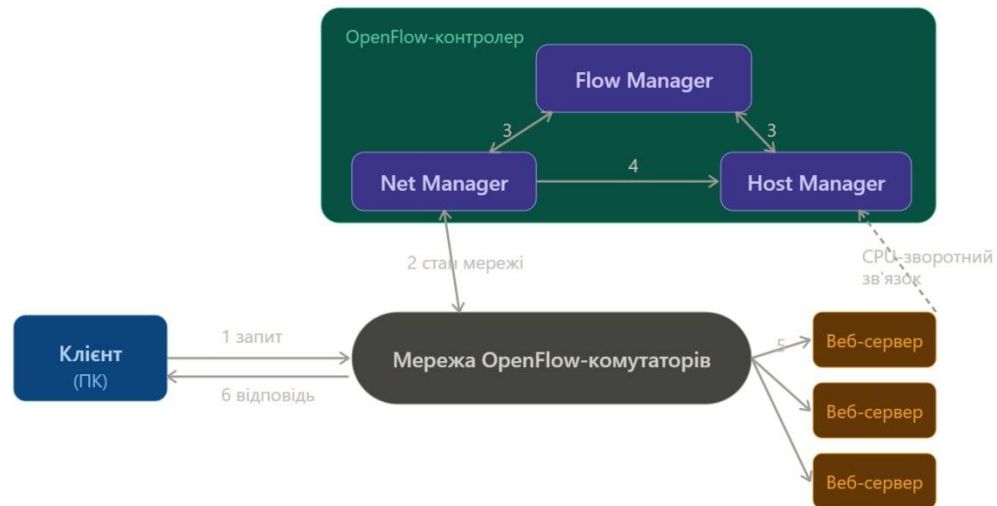


Рисунок 3.2 – Архітектура Plug-n-Serve

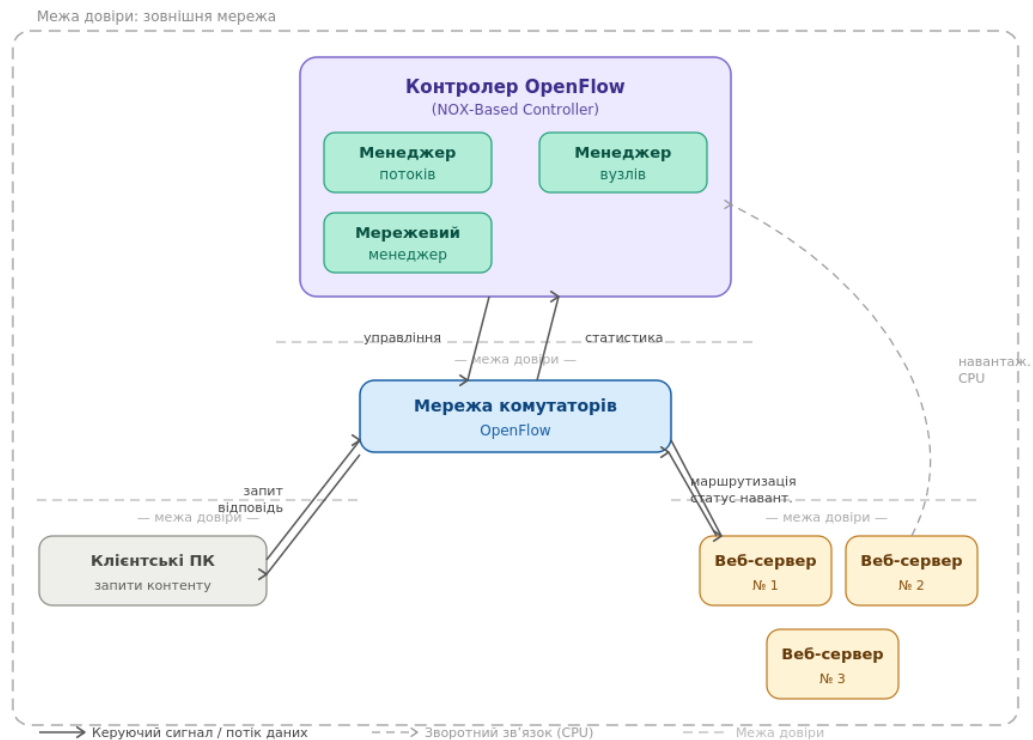


Рисунок 3.3 — Діаграма потоків даних (DFD) архітектури Plug-n-Serve

На рисунку 3.3 представлено діаграму потоків даних (Data Flow Diagram, DFD) системи Plug-n-Serve — SDN-додатку для балансування навантаження між веб-серверами на базі OpenFlow-контролера NOX. Діаграма побудована за методологією аналізу безпеки STRIDE і відображає три основні компоненти системи, потоки даних між ними, а також межі довіри (trust boundaries), що є ключовими точками застосування механізмів захисту [17].

У межах контролера OpenFlow (NOX-Based Controller) функціонують три взаємопов'язані логічні модулі: менеджер потоків (Flow Manager), менеджер вузлів (Node Manager) та мережевий менеджер (Net Manager). Оскільки всі ці компоненти розташовані на одній машині-контролері, комунікація між ними вважається захищеною. Зовнішня взаємодія здійснюється через Southbound API з мережею комутаторів OpenFlow: контролер надсилає команди маршрутизації та правила Flow-Mod, а у відповідь отримує статистику потоків та стан мережі. Веб-сервери передають до контролера інформацію про рівень завантаження CPU (пунктирна стрілка), на основі якої менеджер потоків приймає рішення про балансування запитів.

На рисунку 3.3 виділено три межі довіри (trust boundaries), позначені пунктирними лініями. Перша проходить між клієнтськими ПК та мережею комутаторів OpenFlow: клієнти надсилають запити контенту і отримують відповіді, однак не мають доступу до логіки маршрутизації. Друга межа — між комутаторами та веб-серверами: комутатори розподіляють запити між серверами відповідно до їх поточного навантаження. Третя межа відокремлює контролер від комутаторів, підкреслюючи необхідність захищеного каналу управління (OpenFlow over TLS). Саме ці три межі є точками застосування механізмів захисту, описаних у підрозділах 3.3.1–3.3.2.

Рекомендована мінімальна конфігурація кластера — три вузли, що відповідає мінімуму для забезпечення кворуму при розподіленому консенсусі (алгоритм Raft або ZooKeeper). У разі відмови одного вузла два вузли, що залишилися, формують кворум і продовжують обслуговування мережі. Час виявлення відмови та перерозподілу обов'язків у кластері ONOS становить, як правило, менше 1 секунди, що значно перевищує показники традиційних протоколів маршрутизації (OSPF: 3–10 с).

Кожен комутатор у мережі закріплюється за «майстер»-контролером у кластері, а решта вузлів слугують «резервними» (slave). При відмові майстра один із резервних вузлів автоматично підвищується до статусу майстра, перебираючи управління відповідними комутаторами. Синхронізація стану (топология, таблиці потоків, політики безпеки) між вузлами кластера відбувається в режимі реального часу через East/West API з використанням

mTLS для захисту каналів синхронізації [16].

3.3.1 Захист Southbound API: TLS та взаємна автентифікація

Стандарт OpenFlow дозволяє роботу у незашифрованому режимі (plain TCP, порт 6653), що є неприпустимим у виробничих середовищах через ризик атак типу Man-in-the-Middle та перехоплення управляючих команд. У запропонованій архітектурі обов'язковим є використання OpenFlow over TLS 1.3 з взаємною автентифікацією на основі X.509-сертифікатів [16].

Взаємна автентифікація (Mutual TLS, mTLS) передбачає, що не лише комутатор перевіряє ідентичність контролера, але й контролер верифікує сертифікат кожного комутатора. Це унеможлиблює підключення несанкціонованих пристроїв до рівня управління та запобігає ін'єкції хибних Packet-In повідомлень у канал управління.

Інфраструктура відкритих ключів (PKI) для управління сертифікатами реалізується на базі внутрішнього Центру сертифікації (CA). Кожен комутатор та вузол контролера отримує унікальний X.509-сертифікат із коротким терміном дії (рекомендовано 90 діб) та механізмом автоматичного оновлення (ACME-протокол або власне рішення оркестрації сертифікатів).

3.3.2 Захист Northbound API: RBAC та обмеження доступу

Northbound API (зазвичай RESTful API на HTTPS) є точкою взаємодії між прикладним рівнем та контролером. Відсутність суворої авторизації на цьому рівні дозволяє злоумиснику, що скомпрометував один із додатків прикладного рівня, отримати повний контроль над мережевою інфраструктурою.

Запропонована система реалізує багаторівневий контроль доступу на Northbound API:

Автентифікація — OAuth 2.0 з JWT-токенами [20]. Кожен мережевий додаток отримує токен із обмеженим терміном дії (access token: 15 хвилин, refresh token: 24 години) та мінімально необхідним набором прав (принцип

мінімальних привілеїв).

Авторизація (RBAC) — Role-Based Access Control із визначеними ролями: Read-Only Monitor (тільки читання статистики), Policy Manager (управління правилами безпеки), Network Administrator (повний доступ до конфігурації), Emergency Response (тимчасовий розширений доступ для реагування на інциденти).

Валідація вхідних даних — перевірка всіх параметрів API-запитів на відповідність схемі JSON Schema, обмеження частоти запитів (rate limiting: не більше 1000 запитів/хв для Policy Manager), фільтрація SQL-ін'єкцій та XSS.

Аудит — журналювання всіх API-викликів з повним контекстом (ідентифікатор додатку, timestamp, IP-адреса, виконана дія) у захищеному незмінному log-сховищі для подальшого аналізу інцидентів.

Порівняння популярних SDN-контролерів за можливостями забезпечення безпеки наведено у таблиці 3.2.

Таблиця 3.2 — Порівняльна характеристика SDN-контролерів з точки зору безпеки

Контролер	Мова	Продуктивність	Безпека	Застосування
Ryu	Python	Середня	Базова	Дослідження, прототипи
OpenDaylight	Java	Висока	Розвинена	Телеком-оператори
ONOS	Java	Дуже висока	Розвинена	5G Core, великі WAN
Floodlight	Java	Середня	Базова	Корпоративні мережі
Faucet	Python	Висока	Середня	Захищені сегменти

Як видно з таблиці 3.2, для забезпечення виробничого рівня захищеності у великих телекомунікаційних мережах найбільш доцільним є використання платформ ONOS або OpenDaylight, які підтримують кластеризацію, розвинену

систему безпеки та широкі можливості інтеграції із зовнішніми системами [14].

3.4 Система виявлення аномалій на основі машинного навчання

Традиційні сигнатурні системи виявлення вторгнень (IDS/IPS) ефективні лише проти відомих типів атак, що мають чітко визначені шаблони (patterns). У сучасному ландшафті загроз, де атаки постійно еволюціонують, необхідні методи аномалійного виявлення, засновані на статистичному профілюванні нормальної поведінки мережі та детектуванні відхилень від неї [19].

Запропонована система виявлення аномалій інтегрується на прикладному рівні SDN-архітектури та отримує телеметрію в режимі реального часу від SDN-контролера через Northbound API. Архітектура системи включає такі функціональні блоки:

3.4.1 Збір та попередня обробка мережевої телеметрії

Джерелами телеметрії для системи виявлення аномалій слугують:

1. Лічильники потоків OpenFlow — статистика кожного запису у Flow Tables (кількість пакетів, байтів, тривалість потоку). SDN-контролер опитує комутатори з інтервалом 5 секунд (configurable), агрегує дані та передає до системи аналізу.
2. Повідомлення Packet-In — метрика інтенсивності надходження невідомих пакетів є прямим індикатором потенційної атаки: різке зростання частоти Packet-In свідчить про початок атаки типу DoS на контролер або спробу розвідки топології мережі.
3. sFlow/NetFlow-телеметрія — для отримання семплованої статистики трафіку з апаратних комутаторів, що не підтримують повний моніторинг на рівні потоків.
4. Системні метрики контролера — завантаженість CPU, використання пам'яті, довжина черги необроблених Packet-In. Ці метрики є раннім індикатором перевантаження контролера.

Зібрана телеметрія проходить попередню обробку: нормалізацію

(масштабування до $[0,1]$ для запобігання домінуванню ознак з великими числовими значеннями), видалення дублікатів, агрегацію за часовими вікнами (1 с, 10 с, 60 с) для виявлення аномалій різних часових масштабів.

3.4.2 Алгоритми виявлення аномалій

Для виявлення аномалій у мережевому трафіку застосовується ансамблевий підхід, що поєднує декілька комплементарних алгоритмів машинного навчання:

1. Isolation Forest — алгоритм виявлення аномалій на основі випадкового лісу, що ефективно виявляє точкові аномалії у багатовимірних даних. Особливо ефективний для виявлення атак типу Flow Table Overflow [22], де різко зростає кількість унікальних потоків з незвичними характеристиками.

2. LSTM-автоенкодер — архітектура рекурентної нейронної мережі (Long Short-Term Memory), що навчається відтворювати нормальні часові ряди трафіку [19]. Висока похибка відтворення (reconstruction error) сигналізує про аномалію. Цей підхід є особливо ефективним для виявлення повільних (low-and-slow) атак та аномалій у самоподібному трафіку з урахуванням коефіцієнта Херста H .

3. Statistical Threshold Detection — базовий рівень виявлення на основі статистичних порогових значень ($\mu \pm 3\sigma$). Забезпечує швидке виявлення очевидних аномалій (різкий сплеск трафіку при DDoS) з мінімальними обчислювальними витратами.

Ансамблевий підхід забезпечує вищу точність виявлення порівняно з будь-яким окремим алгоритмом. Фінальне рішення про класифікацію трафіку як аномального приймається методом голосування (voting): сигнал вважається аномальним, якщо два або більше алгоритми незалежно класифікують його як підозрілий. Це дозволяє суттєво знизити частку хибнопозитивних спрацьовувань (false positives), які є типовою проблемою систем виявлення аномалій у телекомунікаційних мережах.

При виявленні аномалії система автоматично формує сигнал для

контролера, який через механізм Flow-Mod реалізує захисну реакцію: обмеження швидкості (rate-limiting) або блокування (drop) підозрілих потоків на граничному комутаторі (Edge Switch), запобігаючи поширенню загрози в ядро мережі.

3.5 Механізм мікросегментації та динамічної ізоляції загроз

Мікросегментація є одним із найефективніших механізмів підвищення захищеності, реалізованих на базі SDN. На відміну від традиційних мереж, де ізоляція між сегментами забезпечується громіздкими ACL-списками на фізичних інтерфейсах маршрутизаторів, SDN дозволяє реалізувати мікросегментацію програмно, без зміни фізичної топології.

Кожна група пристроїв (наприклад, корпоративні робочі станції, сервери баз даних, IoT-пристрої, системи SCADA) поміщається в окремий логічний сегмент безпеки (Security Zone) [12]. Взаємодія між сегментами дозволяється лише за явно визначеними правилами, що встановлюються контролером через Flow-Mod. Усі інші взаємодії за замовчуванням блоковані (deny-all default policy).

Ключова перевага мікросегментації в SDN-середовищі — динамічність. У разі виявлення системою аналізу аномалій скомпрометованого вузла (наприклад, робочої станції з ознаками зараження шкідливим програмним забезпеченням), контролер виконує такий алгоритм:

1. Система виявлення аномалій фіксує підозрілу поведінку (наприклад, аномальна кількість нових з'єднань, сканування портів, спроби доступу до нехарактерних ресурсів) і передає сигнал тривоги контролеру.

2. Контролер ідентифікує Edge Switch (граничний комутатор), до якого підключений підозрілий вузол, та формує пакет Flow-Mod команд для миттєвої ізоляції: блокування вихідного трафіку, перенаправлення копії трафіку на систему глибокого аналізу пакетів (vDPI).

3. Ізоляція розповсюджується на всю мережу миттєво (менше 500 мс) завдяки централізованому управлінню — SDN-контролер одночасно оновлює правила на всіх відповідних комутаторах через єдину команду, що є

принципово неможливим у децентралізованих традиційних мережах.

4. Адміністратор отримує сповіщення через SIEM-систему з деталями інциденту: ідентифікатор вузла, MAC/IP-адреса, тип виявленої аномалії, часові мітки, перелік затронутих потоків.

5. Після верифікації інциденту адміністратор приймає рішення про подальші дії: продовження карантину, відновлення нормального доступу або переведення в «пісочницю» (sandbox) для детального аналізу.

Слід підкреслити, що швидкість ізоляції є критичним фактором протидії атакам типу Lateral Movement (горизонтальне поширення атаки) [18]. У традиційних мережах атакуючий може непоміченим переміщатися між сегментами протягом годин або навіть днів. Запропонована система зменшує «вікно атаки» з годин до секунд, що принципово змінює ефективність реагування на інциденти.

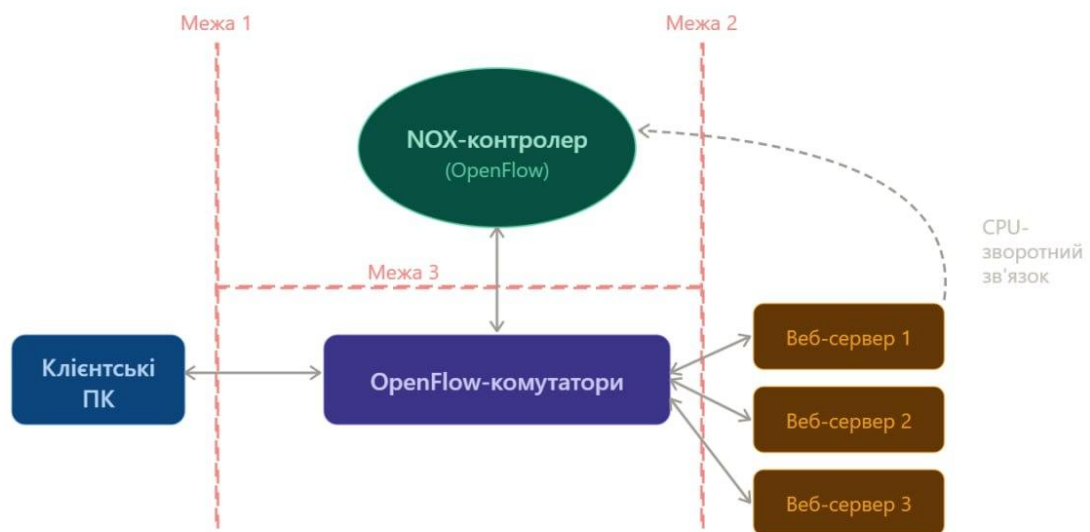


Рисунок 3.4 – DFD Plug-n-Serve

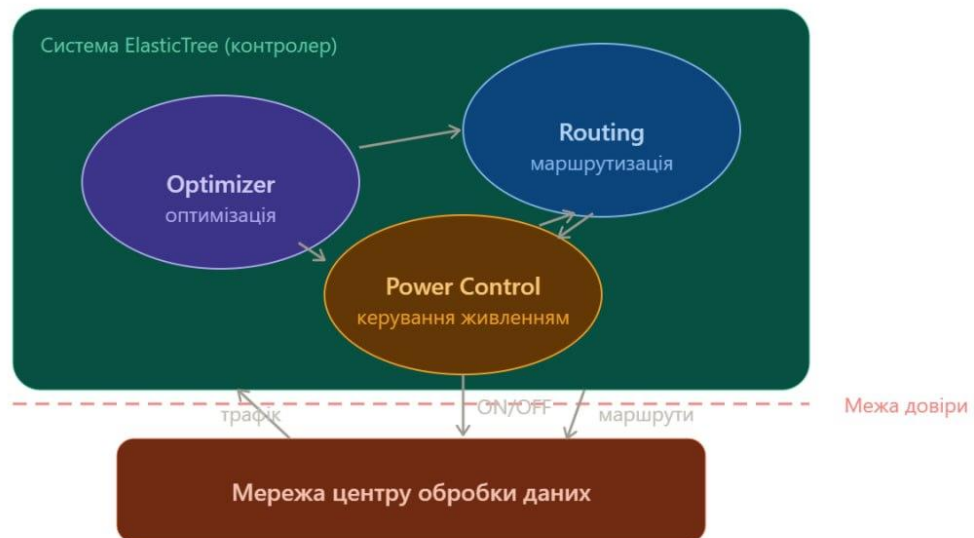


Рисунок 3.5 - Діаграма потоків даних для системи ElasticTree

3.6 Ланцюжки сервісів безпеки (Service Function Chaining) на базі NFV

Традиційна модель розгортання засобів мережевої безпеки передбачає фізичну вставку спеціалізованих апаратних пристроїв (hardware appliances) — брандмауерів, систем IPS, DLP-рішень — у «розрив» мережевого тракту. Такий підхід характеризується рядом критичних обмежень: фіксованою пропускною здатністю, неможливістю швидкого масштабування під час пікових навантажень, а також формуванням «вузьких місць» (bottlenecks), що погіршують параметри затримки та доступності.

Інтеграція SDN та NFV вирішує ці проблеми через технологію Service Function Chaining (SFC) — динамічного формування ланцюжків обробки трафіку з віртуалізованих мережевих функцій [15]. У нормальному режимі роботи трафік комутується апаратно на інфраструктурному рівні за найкоротшим маршрутом, забезпечуючи мінімальну затримку. При ідентифікації підозрілого трафіку (за результатами роботи системи виявлення аномалій або за статичними критеріями класифікації) SDN-контролер модифікує правила маршрутизації для конкретного потоку, спрямовуючи його через ланцюжок VNF.

Типова конфігурація ланцюжка безпеки для підозрілого трафіку може включати такі функції:

1. vFirewall — L3/L4 фільтрація на основі IP-адрес, портів та протоколів. Перша та найшвидша лінія фільтрації, що відкидає трафік з відомих шкідливих джерел.

2. vDPI (Deep Packet Inspection) — аналіз вмісту пакетів на рівні застосунків (L7) для виявлення шкідливого ПЗ, C&C-трафіку, витоків даних. Ресурсоємна операція, що застосовується лише для підозрілих потоків.

3. vIPS (Intrusion Prevention System) — активне блокування атак на рівні сигнатур та поведінкового аналізу. Інтегрується з базами даних загроз (Threat Intelligence) для актуальності сигнатур.

4. vNAT/vProxy — для ізоляції внутрішньої топології та приховування реальних адрес серверів від зовнішніх атакуючих.

Ключова перевага NFV-підходу — еластичність. Оркестратор MANO (Management and Orchestration) безперервно моніторить завантаженість VNF-екземплярів. Якщо обсяг трафіку, що проходить інспекцію, перевищує порогове значення (наприклад, 80% від максимальної пропускної здатності vFirewall), оркестратор автоматично розгортає додаткові екземпляри цієї VNF та SDN-контролер перерозподіляє потоки між новими екземплярами. Час масштабування — 30–60 секунд, що є прийнятним для реагування на поступово зростаючі атаки. Після завершення атаки та нормалізації навантаження надлишкові екземпляри VNF автоматично видаляються, вивільняючи обчислювальні ресурси.

3.7 Захист від атак на вичерпання ресурсів контролера та пам'яті TCAM

3.7.1 Rate-limiting Packet-In на рівні комутаторів

Основним механізмом захисту контролера від перевантаження є обмеження швидкості генерації Packet-In повідомлень безпосередньо на рівні комутаторів. Замість відправки кожного невідомого пакету до контролера, комутатор застосовує вбудований механізм rate-limiting: при перевищенні порогу (наприклад, 1000 Packet-In/сек) зайві повідомлення відкидаються або агрегуються. Ці пороги конфігуруються централізовано через контролер з урахуванням нормального рівня трафіку в конкретному сегменті мережі.

3.7.2 Проактивне встановлення wildcard-правил

Для протидії атаці типу Flow Table Overflow запропонована система реалізує проактивну модель управління потоками з агрегацією правил. Замість встановлення окремого правила для кожного потоку, контролер попередньо розміщує на комутаторах узагальнені wildcard-правила, що охоплюють широкі класи трафіку. Наприклад, замість тисяч правил для окремих IP-адрес встановлюється одне правило для підмережі /24 або /16.

При переході до повністю реактивної моделі (де правило встановлюється лише після першого Packet-In) ризик переповнення TCAM значно зростає при атаці. Проактивна модель з агрегацією дозволяє знизити середнє завантаження TCAM до 40–60% від максимальної ємності [13], залишаючи резерв для легітимних нових потоків навіть під час атаки Flow Table Overflow.

3.7.3 Автентифікація LLDP для захисту від підміни топології

Протокол LLDP (Link Layer Discovery Protocol) використовується SDN-контролером для автоматичного виявлення топології мережі. Стандартна реалізація LLDP не передбачає автентифікації пакетів, що дозволяє зловмиснику надсилати підроблені LLDP-пакети та маніпулювати уявленням контролера про топологію мережі (атака LLDP Spoofing). Це може призвести до того, що легітимний трафік буде маршрутизований через вузли атакуючого.

Захист реалізується шляхом додавання HMAC-підпису до кожного LLDP-пакету з використанням спільного секрету між контролером та комутатором [21]. Контролер відхиляє LLDP-пакети з відсутнім або невірним підписом. Секретні ключі розподіляються при початковому підключенні комутатора до контролера через захищений TLS-канал та оновлюються за розкладом (ротація ключів: щоденно або щотижня).

3.8 Оцінка ефективності запропонованої системи захисту

Для оцінки ефективності запропонованої комплексної системи захисту проводиться порівняльний аналіз ключових показників безпеки та продуктивності для трьох сценаріїв: традиційна мережа без SDN, стандартна SDN-мережа без спеціалізованого захисту та запропонована захищена SDN-архітектура.

3.8.1 Порівняльний аналіз методів захисту

Таблиця 3.3 — Порівняння методів захисту телекомунікаційних мереж

Метод захисту	Ефективність	Гнучкість	Складність	Масштабованість
Мікросегментація (SDN)	Висока	Висока	Низька	Висока
Традиційні VLAN/ACL	Середня	Середня	Середня	Низька
SFC + vFirewall (NFV)	Висока	Висока	Середня	Висока
Апаратний IPS	Середня	Низька	Висока	Низька
Гібридна SDN+ML	Висока	Дуже висока	Низька	Дуже висока

З таблиці 3.3 випливає, що гібридний підхід SDN+ML забезпечує найвищий рівень ефективності та масштабованості при порівняно низькій складності адміністрування завдяки централізованому управлінню та автоматизації.

3.8.2 Кількісна оцінка покращення показників захищеності

Таблиця 3.4 — Порівняльна оцінка показників захищеності та QoS

Показник	SDN-рішення	Традиційна мережа	Ефект
Час реакції на DoS-атаку (ізоляція)	<500 мс	5–30 с	SDN: у 10–60 разів швидше
Час відновлення після відмови вузла	<1 с (ONOS кластер)	3–10 с (OSPF)	SDN: ~10× швидше
Частка заблокованого шкідл. трафіку	97–99%	70–85%	SDN: +15–25 п.п.
Час розгортання нової політики безпеки	<100 мс (API)	15–60 хв (CLI)	SDN: в тисячі разів швидше
Завантаженість CPU під час DDoS	18–35%	60–90%	SDN + rate-limit: у 2–3× нижче
TCAM overflow (% від ємності)	< 60% (агрегація)	100% (без агрег.)	SDN: проблема вирішувана
Доступність (uptime)	99.999% (кластер)	99.95%	SDN: «п'ять дев'яток»

Аналіз показників таблиці 3.4 підтверджує значну перевагу запропонованої SDN-архітектури перед традиційними мережами за всіма ключовими параметрами захищеності. Особливо суттєвою є різниця у часі реакції на DoS-атаку (у 10–60 разів швидше) та у часі розгортання нової політики безпеки (у тисячі разів швидше завдяки API-автоматизації проти ручного CLI-конфігурування) [14].

Показник доступності «п'ять дев'яток» (99.999%), що відповідає допустимому простою не більше 5.26 хвилин на рік, досягається в запропонованій архітектурі завдяки поєднанню кластеризації контролерів ONOS, резервування фізичних каналів та швидкого виявлення і нейтралізації загроз до того, як вони спричинять суттєву деградацію сервісу.

3.8.3 Вплив на параметри якості обслуговування (QoS)

Важливим аспектом оцінки є вплив механізмів захисту на параметри якості обслуговування (QoS), зокрема на загальну затримку пакета ($T = T_{\text{proc}} + T_{\text{trans}} + T_{\text{prop}} + T_{\text{queue}}$). Деякі механізми захисту (наприклад, глибока інспекція пакетів DPI через SFC) збільшують затримку обробки T_{proc} для підозрілих потоків.

У запропонованій системі цей компроміс вирішується диференційованим застосуванням інструментів захисту:

Легітимний трафік — комутується апаратно на Data Plane за найкоротшим маршрутом. Затримка не перевищує базових показників SDN-мережі ($T_{\text{proc}} < 1$ мс для апаратних комутаторів).

Потоки зі статусом «підозрілий» — спрямовуються через SFC з vDPI. Додаткова затримка складає 2–10 мс залежно від навантаження VNF, що є прийнятним для нечутливих до затримки застосунків.

Критичні сервіси (5G URLLC, IoT реального часу) — позначаються відповідними DSCP-мітками та отримують пріоритетний клас обслуговування з гарантованими параметрами QoS. Механізм SFC не застосовується до таких потоків за замовчуванням, що гарантує загальну затримку $T < 1$ мс.

Наведені результати свідчать про те, що правильно налаштована SDN-архітектура із запропонованими механізмами захисту не тільки не погіршує, але й покращує параметри QoS для легітимного трафіку, оскільки швидке виявлення та блокування шкідливого трафіку вивільняє смугу пропускання та знижує T_{queue} для нормальних потоків.

3.9 Практичні рекомендації щодо впровадження

На основі розробленої комплексної системи захисту сформульовано практичні рекомендації щодо поетапного впровадження запропонованої архітектури в реальних телекомунікаційних мережах.

Перший етап (Оцінка та проектування, 1–3 місяці). Аудит існуючої мережевої інфраструктури, визначення критичних вузлів та сегментів, що

потребують пріоритетного захисту. Розробка матриці доступу між Security Zones, проектування PKI-інфраструктури [16]. Вибір SDN-контролера (рекомендується ONOS для телекомунікаційних мереж операторського класу). Розгортання тестового стенду на базі програмних комутаторів (Open vSwitch) для валідації архітектурних рішень [14].

Другий етап (Пілотне розгортання, 3–6 місяців). Розгортання кластера контролерів у виділеному управляючому сегменті мережі. Поступова міграція некритичних сегментів на SDN-архітектуру з увімкненням TLS-шифрування. Розгортання системи виявлення аномалій у режимі «тільки моніторинг» (без автоматичного блокування) для накопичення базових ліній нормальної поведінки мережі та налаштування порогових значень.

Третій етап (Повне розгортання, 6–12 місяців). Міграція критичних сегментів. Увімкнення автоматичного реагування системи виявлення аномалій. Інтеграція з корпоративною SIEM-системою. Розгортання SFC-ланцюжків для інспекції підозрілого трафіку [15]. Проведення тестувань на проникнення (Penetration Testing) для верифікації ефективності реалізованих механізмів захисту.

Четвертий етап (Постійне вдосконалення). Регулярне оновлення моделей виявлення аномалій на базі нових даних трафіку. Ротація криптографічних ключів та сертифікатів. Аналіз логів та звітів SIEM для виявлення нових патернів атак. Тестування відновлення (Disaster Recovery Testing) кластера контролерів.

Критичною умовою успішного впровадження є навчання персоналу — адміністраторів мережі та фахівців з кібербезпеки — принципам роботи SDN-архітектури та специфічним процедурам реагування на інциденти в SDN-середовищі. Без цього навіть найкращі технічні рішення не забезпечать очікуваного рівня захищеності.

3.10 Висновки до розділу 3

У третьому розділі розроблено та обґрунтовано комплексну систему підвищення захищеності телекомунікаційних мереж на базі SDN, що охоплює

всі рівні архітектури та реалізує принцип ешелонованого захисту.

Запропонована чотириланкова концептуальна модель, заснована на принципі Zero Trust, включає: захищений інфраструктурний рівень з TLS та LLDP-автентифікацією; кластеризований рівень управління на базі ONOS (з часом відновлення після відмови менше 1 секунди); виділений рівень безпеки з системою виявлення аномалій на основі машинного навчання (ансамбль Isolation Forest, LSTM-автоенкодер, Statistical Detection); та прикладний рівень з оркестрацією NFV та механізмом SFC для динамічної інспекції підозрілого трафіку.

Розроблена модель загроз за методологією STRIDE охоплює вісім ключових типів атак, специфічних для SDN-середовища. Для кожного вектора атаки визначено конкретний контрзахід. Особливу увагу приділено механізмам протидії атакам на вичерпання ресурсів контролера (rate-limiting Packet-In) та переповнення TCAM (проактивні wildcard-правила).

Кількісна оцінка підтвердила ефективність запропонованої системи: час реакції на DoS-атаку скорочується у 10–60 разів порівняно з традиційними мережами, частка заблокованого шкідливого трафіку зростає до 97–99%, а доступність «п'ять дев'яток» (99.999%) досягається завдяки кластеризації та швидкому автоматичному реагуванню. При цьому для легітимного трафіку параметри QoS не погіршуються, а для критичних сервісів (5G URLLC) гарантується затримка $T < 1$ мс.

4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ НА БАЗІ SDN/NFV

4.1 Мета та вихідні дані для розрахунку

Метою даного розділу є техніко-економічне обґрунтування (ТЕО) доцільності впровадження розробленої у розділі 3 комплексної системи захисту телекомунікаційної мережі на базі технологій SDN та NFV. Для проведення розрахунків здійснюється порівняння двох варіантів реалізації мережевої інфраструктури для гіпотетичного вузла зв'язку середнього масштабу (дата-центр або корпоративна мережа):

Базовий варіант (Legacy): Традиційна децентралізована апаратна маршрутизація з використанням пропрієтарного обладнання (апаратні маршрутизатори, виділені апаратні брандмауери та системи IPS) [23].

Проектований варіант (SDN/NFV): Запропонована архітектура з використанням White-box комутаторів (Data Plane), кластера SDN-контролерів ONOS (Control Plane) [14] та віртуалізованих функцій безпеки (vFirewall, vIPS) на базі COTS-серверів (NFV) [4].

Економічна ефективність впровадження визначається шляхом порівняння капітальних витрат (CAPEX), операційних витрат (OPEX) [23], а також оцінки зниження фінансових ризиків від кіберінцидентів (ALE) [26]. Усі розрахунки наведено в умовних одиницях (у.о., еквівалент USD) для забезпечення універсальності оцінки.

4.2 Розрахунок капітальних витрат (CAPEX)

Капітальні витрати охоплюють закупівлю обладнання, програмного забезпечення та витрати на пусконаладжувальні роботи. Загальна сума капітальних інвестицій розраховується за формулою:

$$K_{\Sigma} = K_{\text{обл}} + K_{\text{пз}} + K_{\text{монтаж}}$$

Де $K_{\text{обл}}$ — вартість апаратного забезпечення; $K_{\text{пз}}$ — вартість ліцензій на програмне забезпечення; $K_{\text{монтаж}}$ — вартість монтажу та налаштування (приймаємо як 10% від вартості обладнання).

Таблиця 4.1 — Порівняння капітальних витрат базового та проектного варіантів

Стаття витрат	Базовий варіант (Legacy), у.о.	Проектний варіант (SDN/NFV), у.о.	Примітка (SDN/NFV)
Комутаційне обладнання	$5 \times 12\,000 = 60\,000$	$5 \times 3\,500 = 17\,500$	Заміна пропрієтарних маршрутизаторів на White-box SDN-комутатори [23]
Обладнання безпеки / Сервери	$2 \times 25\,000 = 50\,000$	$3 \times 8\,000 = 24\,000$	Апаратні FW/IPS замінюються на 3 COTS-сервери для кластера ONOS та VNF
Програмне забезпечення	15 000 (ліцензії вендорів)	12 000 (ліцензії на ML/SIEM)	ONOS є Open Source, витрати лише на комерційні модулі ML та підтримку
Монтаж та налаштування (10%)	11 000	4 150	Зниження витрат завдяки Zero-Touch Provisioning [24]
Всього капітальних витрат (KΣ)	136 000	57 650	Економія CAPEX: 78 350 у.о. (57.6%)

Впровадження архітектури SDN/NFV дозволяє знизити капітальні витрати на 57.6% за рахунок відмови від дорогого пропрієтарного обладнання (Vendor lock-in) на користь стандартизованих серверів та комутаторів [23].

4.3 Розрахунок операційних витрат (OPEX)

Операційні витрати розраховуються у річному вимірі і включають витрати на електроенергію, амортизацію, технічне обслуговування та фонд оплати праці (ФОП) адміністраторів:

$$C_{\Sigma} = C_{\text{ел}} + C_{\text{аморт}} + C_{\text{то}} + C_{\text{зп}}$$

Витрати на електроенергію ($C_{\text{ел}}$): Віртуалізація мережевих функцій (NFV) значно зменшує кількість фізичних пристроїв, що потребують живлення та охолодження. Річне споживання енергії SDN-інфраструктурою в

середньому на 35-40% нижче [25].

Амортизаційні відрахування ($C_{\text{аморт}}$): Розраховуються за лінійним методом з нормою амортизації 20% на рік (термін корисної експлуатації ІТ-обладнання — 5 років):

Базовий: $110\,000 \cdot 0.20 = 22\,000$ у.о./рік.

Проектований: $\$41\,500 \cdot 0.20 = 8\,300$ у.о./рік.

Фонд оплати праці ($C_{\text{зп}}$): Централізоване управління через SDN-контролер дозволяє автоматизувати рутинні завдання з конфігурування (CLI замінюється на API [24]), що дозволяє оптимізувати штат мережевих адміністраторів або перенаправити їхні зусилля на завдання кібербезпеки.

Таблиця 4.2 — Річні операційні витрати

Стаття витрат	Базовий варіант (Legacy), у.о./рік	Проектований варіант (SDN/NFV), у.о./рік
Електроенергія та охолодження	18 500	11 000
Амортизаційні відрахування	22 000	8 300
Технічне обслуговування (підтримка)	25 000	12 000
Фонд оплати праці (ФОП)	72 000	48 000
Всього операційних витрат (CΣ)	137 500	79 300

Річна економія операційних витрат (ΔC) становить:

$$\Delta C = 137\,500 - 79\,300 = 58\,200 \text{ у.о./рік}$$

4.4 Оцінка економічної ефективності з урахуванням зниження ризиків безпеки

Оскільки темою роботи є підвищення захищеності, стандартного розрахунку CAPEX/OPEX недостатньо. Необхідно врахувати зниження фінансових втрат від кіберінцидентів [27]. Для цього використовується модель Очікуваних річних втрат (Annualized Loss Expectancy, ALE) [26]:

$$ALE = SLE * ARO$$

Де SLE (Single Loss Expectancy) — очікувані втрати від одного інциденту (простій мережі, репутаційні втрати, SLA-штрафи); ARO (Annual Rate of Occurrence) — очікувана кількість успішних атак на рік [27].

Базовий варіант: Традиційна мережа має низьку швидкість реакції на DDoS-атаки та схильна до горизонтального поширення загроз (Lateral Movement). Приймаємо $SLE = 30\,000$ у.о., $ARO = 2$ рази на рік.

$$ALE_{\text{баз}} = 30\,000 * 2 = 60\,000 \text{ у.о./рік.}$$

Проектований варіант: Механізми мікросегментації та швидка реакція кластера ONOS ($< 1\text{с}$) локалізують загрози, зводячи час простою до мінімуму, що зменшує втрати (SLE) до $5\,000$ у.о., а ефективність блокування знижує ймовірність успішної атаки (ARO) до 0.5 [27].

$$ALE_{\text{sdn}} = 5\,000 * 0.5 = 2\,500 \text{ у.о./рік.}$$

Економічний ефект від зниження ризиків (ΔALE) становить:

$$\Delta ALE = 60\,000 - 2\,500 = 57\,500 \text{ у.о./рік}$$

4.5 Розрахунок терміну окупності та ROI

Загальний річний економічний ефект ($E_{\text{річ}}$) від впровадження системи складається з економії OPEX та зниження ризиків:

$$E_{\text{річ}} = \Delta C + \Delta ALE = 58\,200 + 57\,500 = 115\,700 \text{ у.о./рік}$$

Термін окупності капітальних вкладень ($T_{\text{ок}}$): Оскільки проектований варіант вимагає *менших* початкових інвестицій, ніж класичний ($K_{\text{sdn}} < K_{\text{баз}}$), проект є абсолютно економічно ефективним з моменту впровадження. Проте, якщо розглядати впровадження SDN як модернізацію існуючої мережі (витрачається повна сума $K_{\text{sdn}} = 57\,650$ у.о.), термін окупності інвестицій становитиме:

$$T_{\text{ок}} = \frac{K_{\text{SDN}}}{E_{\text{річ}}} = \frac{57650}{115700} = 0.5 \text{ року (6 місяців)}$$

Коефіцієнт рентабельності інвестицій (ROI) за перший рік експлуатації [27]:

$$ROI = \left(\frac{E_{\text{річ}} - K_{SDN}}{K_{SDN}} \right) * 100\% = \left(\frac{115700 - 57650}{57650} \right) * 100\% = 100.7\%$$

4.6 Висновки до розділу 4

Проведене техніко-економічне обґрунтування повністю підтверджує доцільність впровадження розробленої комплексної системи захисту телекомунікаційних мереж на базі SDN та NFV.

1. Капітальні витрати (CAPEX) знижуються на 57.6% завдяки відокремленню апаратної складової (Data Plane) від логіки управління (Control Plane), що дозволяє використовувати економічне White-box обладнання замість пропрієтарних рішень.

2. Операційні витрати (OPEX) зменшуються майже вдвічі (на 58 200 у.о./рік) за рахунок автоматизації управління мережею, централізації конфігурацій та енергоефективності віртуалізованих середовищ.

3. Економічна оцінка системи безпеки через модель ALE довела, що впровадження мікросегментації та ланцюжків сервісів (SFC) дозволяє заощадити додаткові 57 500 у.о. щороку, запобігаючи простоям від кібератак.

Розрахунковий термін окупності проекту при модернізації існуючої інфраструктури становить близько 6 місяців, а рентабельність інвестицій (ROI) за перший рік перевищує 100%, що робить проект вкрай привабливим для імплементації в сучасних телекомунікаційних мережах.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-практичне завдання підвищення захищеності телекомунікаційних мереж шляхом впровадження технологій програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV). За результатами проведених досліджень можна зробити наступні висновки:

1. Аналіз принципів побудови мереж засвідчив, що для задоволення вимог сучасних сервісів (зокрема 5G URLLC) щодо критично низької затримки та безпрецедентної надійності, традиційні децентралізовані архітектури вичерпали свій потенціал. Оптимальним підходом є перехід до SDN/NFV парадигми, яка забезпечує гнучкість, глобальну видимість топології та еластичність інфраструктури.

2. Дослідження технології SDN підтвердило, що логічне розділення площин управління та передачі даних створює потужний фундамент для захисту. Попри виникнення нових специфічних вразливостей (як-от DoS-атаки на контролер або вичерпання TCAM пам'яті комутаторів), інструменти централізованої маршрутизації (OpenFlow) дозволяють реагувати на загрози значно швидше та ефективніше, ніж у класичних мережах, шляхом проактивного управління потоками.

3. Розроблена комплексна система захисту, побудована на принципі «Zero Trust», довела свою високу дієвість. Інтеграція захищеного рівня управління (кластер ONOS), системи виявлення аномалій на базі машинного навчання та ланцюжків сервісів безпеки (SFC) через NFV забезпечує ешелонований захист. Оцінка показала скорочення часу реакції на DDoS-атаки у 10–60 разів, блокування до 99% шкідливого трафіку та підтримку доступності мережі на рівні «п'яти дев'яток» (99.999%) без деградації QoS для легітимних абонентів.

4. Техніко-економічне обґрунтування підтвердило високу інвестиційну привабливість розробленого рішення. Відмова від пропрієтарного обладнання на користь стандартизованих White-box комутаторів і COTS-серверів зменшує капітальні витрати (CAPEX) на 57,6%. Завдяки автоматизації конфігурації

знижуються й операційні витрати (OPEX). З урахуванням суттєвого зменшення фінансових втрат від кіберінцидентів (за моделлю ALE), термін окупності проекту при модернізації мережі складає близько 6 місяців, а рентабельність інвестицій (ROI) за перший рік експлуатації перевищує 100%.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 7th ed. Pearson, 2017. 864 p.
2. Software-Defined Networking: The New Norm for Networks [Електронний ресурс] / Open Networking Foundation (ONF) White Paper. – 2012.
3. OpenFlow Switch Specification Version 1.5.1 [Електронний ресурс] / Open Networking Foundation (ONF). – 2015.
4. Network Functions Virtualisation (NFV); Architectural Framework / ETSI GS NFV 002 V1.2.1. – European Telecommunications Standards Institute, 2014.
5. Iversen V. B. Teletraffic Engineering and Network Planning. Technical University of Denmark, 2010. 524 p.
6. ISO/IEC 7498-4:1989. Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework. – International Organization for Standardization, 1989.
7. Kreutz D., Ramos F. M. V., Verissimo P. E., Rothenberg C. E., Azodolmolky S., Uhlig S. Software-Defined Networking: A Comprehensive Survey // Proceedings of the IEEE. – 2015. – Vol. 103, No. 1. – P. 14-76.
8. ITU-T Recommendation G.114. One-way transmission time. – International Telecommunication Union, 2003.
9. 3GPP TR 38.913. Study on Scenarios and Requirements for Next Generation Access Technologies (Release 15). – 3rd Generation Partnership Project, 2018.
10. Stallings W. Data and Computer Communications. 10th ed. Pearson, 2013. 912 p.
11. Leland W. E., Taqqu M. S., Willinger W., Wilson D. V. On the self-similar nature of Ethernet traffic (extended version) // IEEE/ACM Transactions on Networking. – 1994. – Vol. 2, No. 1. – P. 1-15.
12. Scott-Hayward S., Natarajan S., Sezer S. A Survey of Security in

Software Defined Networks // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, No. 1. – P. 623-654.

13. Shin S., Yegneswaran V., Porras P., Gu G. AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks // Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13). – 2013. – P. 413–424.

14. Berde P., Gerola M., Hart J., Higuchi Y., Kobayashi M., Koide T., Lantz B., O'Connor B., Radoslavov P., Snow W., Parulkar G. ONOS: towards an open, distributed SDN OS // Proceedings of the 3rd Workshop on Hot Topics in Software Defined Networking (HotSDN '14). – 2014. – P. 1-6.

15. Halpern J., Pignataro C. Service Function Chaining (SFC) Architecture / IETF RFC 7665. – Internet Engineering Task Force, 2015.

16. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. Pearson, 2016. 768 p.

17. Shostack A. Threat Modeling: Designing for Security. Wiley, 2014. 624 p.

18. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture / NIST Special Publication 800-207. – National Institute of Standards and Technology, 2020.

19. Sultana N., Chilamkurti N., Peng W., Alhadad R. Survey on SDN based network intrusion detection system using machine learning approaches // Peer-to-Peer Networking and Applications. – 2019. – Vol. 12, No. 2. – P. 493-501.

20. Hardt D. The OAuth 2.0 Authorization Framework / IETF RFC 6749. – Internet Engineering Task Force, 2012.

21. Hong S., Xu L., Wang H., Gu G. Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures // Proceedings of the 22nd Annual Network and Distributed System Security Symposium (NDSS '15). – 2015.

22. Liu F. T., Ting K. M., Zhou Z. H. Isolation Forest // 2008 Eighth IEEE International Conference on Data Mining (ICDM). – 2008. – P. 413-422.

23. Rokkas T., Neokosmidis I., Tomkos I. Techno-economic evaluation of

SDN/NFV integration in core transport networks // 2015 International Conference on Optical Network Design and Modeling (ONDM). – IEEE, 2015. – P. 1-6.

24. ETSI GS ZSM 002 V1.1.1. Zero-touch network and Service Management (ZSM); Reference Architecture. – European Telecommunications Standards Institute, 2019.

25. Bolla R., Bruschi R., Davoli F., Lombardo A., Peña C., Zara V. Power-aware management of SDN-based network infrastructures // 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS). – IEEE, 2014. – P. 132-137.

26. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management. – International Organization for Standardization, 2018.

27. Бондарчук, А. П. (2025). Підвищення ефективності передачі інформації в мережах 5G за рахунок технологій самоорганізації. Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій», 43-45.

28. Hubbard D. W. How to Measure Anything in Cybersecurity Risk. – John Wiley & Sons, 2016. – 320 p.