Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: " Архітектура безпеки 5G Core на основі віртуалізованих мережевих функцій"

Виконав: студент VI курсу, групи СБм-61
Спеціальності:
125 Кібербезпека та захист інформації
(шифр і назва напряму підготовки, спеціальності)
Марчук Дмитро Володимирович
підпис (прізвище та ініціали)

Керівник Карпінський М. П.
підпис (прізвище та ініціали)

Нормоконтроль Стадник М. А.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Марчуку Дмитру Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Архітектура безпеки 5G Core на основі віртуалізованих мережевих функцій

Керівник роботи Карпінський Микола Петрович,
доктор технічних наук, професор кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » 11 2025 року № 4/7-1024

2. Термін подання студентом завершеної роботи 12.12.2025

3. Вихідні дані до роботи Стандарти та специфікації 3GPP щодо архітектури 5G Core, сучасні підходи до NFV/SDN-оркестрації та практичні вимоги до забезпечення кібербезпеки в телекомунікаційних мережах.

4. Зміст роботи (перелік питань, які потрібно розробити)
Провести аналіз вразливостей stateful-фаєрволів і протоколів DHCP/RA у 5G Core.
Проектування політико-керованої архітектури із замкненими контурами управління.
Побудову моделі узгодження політик MANO/ZSM. Створення й експериментальне оцінювання прототипу системи безпеки на базі Open5GS, CNF та інтегрованих засобів виявлення загроз.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Актуальність дослідження. Мета, об'єкт, предмет дослідження.
Наукова новизна та практичне значення.
Завдання дослідження. Основні сценарії використання 5G.
Рівні архітектури MANO. Сегментація мережі (network slicing).
Безпека в архітектурі 5G. Огляд типових вразливостей та атак у віртуалізованих мережах.
Реалізація системи. Тестування системи.
Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Теслюк В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 19.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Підбір джерел для аналізу в галузі дослідження	25.09 – 10.10	Виконано
3.	Опрацювання джерел в галузі дослідження	11.10 – 15.10	Виконано
4.	Налаштування симуляційного середовища	16.10 – 25.10	Виконано
5.	Оформлення розділу «Архітектура та віртуалізація ядра мережі 5G»	25.10 – 05.11	Виконано
6.	Оформлення розділу «Аналіз вразливостей у середовищі 5G Core»	06.11 – 10.11	Виконано
7.	Оформлення розділу «Автономна та адаптивна архітектура безпеки для 5G Core»	11.11 – 25.11	Виконано
8.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	26.11-01.12	Виконано
9.	Оформлення кваліфікаційної роботи	02.12 – 10.12	Виконано
10.	Нормоконтроль	08.12 – 10.12	Виконано
11.	Перевірка на плагіат	12.12 – 14.12	Виконано
12.	Попередній захист кваліфікаційної роботи	15.12 – 20.12	Виконано
13.	Захист кваліфікаційної роботи	22.12.2025	

Студент _____ Марчук Д. В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Карпінський М. П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Архітектура безпеки 5G Core на основі віртуалізованих мережевих функцій // ОР «Магістр» // Марчук Дмитро Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2025 // С. 82, рис. – 14, табл. – - , кресл. – 13, додат. – 3.

Ключові слова: 5G Core, cybersecurity, NFV, SDN, network slicing, policy-based security, autonomous orchestration, Policy Conflict Detector, Open5GS, Kubernetes.

У кваліфікаційній роботі магістра розглянуто проблему забезпечення кібербезпеки у віртуалізованій архітектурі ядра мобільної мережі п'ятого покоління (5G Core). Дослідження спрямоване на розроблення автономної, політико-керованої системи безпеки, здатної забезпечувати узгоджене поширення політик, оперативне реагування на загрози та мінімізацію побічного впливу на легітимні сервіси. У роботі проведено аналіз типових вразливостей 5G Core у контексті технологій NFV, SDN, SBA та network slicing, зокрема уразливостей stateful-фаєрволів, атак на DHCP/Router Advertisement і ризиків, пов'язаних із відсутністю integrity-захисту у User Plane.

На основі проведеного аналізу запропоновано ієрархічну архітектуру безпеки з доменним (DSO) і локальним (LSO) оркестраторами, модулем прийняття та реалізації політик (PDP/PEP) і підсистемою виявлення конфліктів політик (Policy Conflict Detector, PCD). Експериментальне моделювання в середовищі Open5GS і Kubernetes підтвердило ефективність запропонованих рішень - скорочення часу реагування, зменшення кількості конфліктів між політиками та підвищення стійкості до атак типу MITM і state pollution.

ABSTRACT

Security architecture of the 5G Core based on virtualized network functions // Thesis of educational level "Master"// Dmytro Marchuk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-61 // Ternopil, 2025 // p. 82, figs. 14, tbls. -, drws. 13, apps. 3.

Keywords: 5G Core, cybersecurity, NFV, SDN, network slicing, policy-based security, autonomous orchestration, Policy Conflict Detector, Open5GS, Kubernetes.

In the master's qualification thesis, the problem of ensuring cybersecurity in the virtualized architecture of the fifth-generation mobile network core (5G Core) is examined. The research focuses on developing an autonomous, policy-driven security system capable of ensuring consistent policy distribution, rapid threat response, and minimal impact on legitimate services. The study analyzes common vulnerabilities of the 5G Core in the context of NFV, SDN, SBA, and network slicing technologies, including weaknesses of stateful firewalls, attacks on DHCP/Router Advertisement, and risks associated with the lack of integrity protection in the User Plane.

Based on the conducted analysis, a hierarchical security architecture is proposed, incorporating domain (DSO) and local (LSO) security orchestrators, a Policy Decision and Enforcement module (PDP/PEP), and a Policy Conflict Detector (PCD) subsystem. Experimental modeling in the Open5GS and Kubernetes environments confirmed the effectiveness of the proposed solutions - reducing response time, decreasing the number of policy conflicts, and increasing resistance to MITM and state-pollution attacks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SBA	—	Service-Based Architecture
MEC	—	Multi-access Edge Computing
ETSI ZSM	—	ETSI Zero-touch Service Management
MANO	—	Management and Orchestration
NFV	—	Network Functions Virtualization
SDN	—	Software-Defined Networking
DHCP	—	Dynamic Host Configuration Protocol
RA	—	Router Advertisement
DSO	—	Domain Security Orchestrator
LSO	—	Local Security Orchestrator
PDP	—	Policy Decision Point
PEP	—	Policy Enforcement Point
HSPL	—	High-level Security Policy
MSPL	—	Medium-level Security Policy
PCD	—	Policy Conflict Detector
eMBB	—	enhanced Mobile Broadband
URLLC	—	Ultra-Reliable Low-Latency Communications
mMTC	—	massive Machine-Type Communications
EPC	—	Evolved Packet Core
NRF	—	Network Repository Function
NF	—	Network Function
CU	—	Central Unit
DU	—	Distributed Unit
CNF	—	Cloud-Native Network Function
VIM	—	Virtualized Infrastructure Manager
EPC	—	Evolved Packet Core
CP	—	Control Plane

SMF	—	Session Management Function
MTD	—	Moving Target Defense
SO	—	Security Orchestrator
ME	—	Monitoring Engine
AE	—	Analysis Engine
PE	—	Policy Engine
PA	—	Policy Administrator
PCD	—	Policy Conflict Detector
MITM	—	Man-in-the-Middle
LTE	—	Long Term Evolution

ВСТУП

Актуальність теми. Віртуалізація 5G Core, поява сервісно-орієнтованої архітектури (SBA), мережевої сегментації (network slicing) та MEC радикально збільшили адаптивність телекомунікаційних систем і водночас розширили поверхню атаки. Компроміси на користь продуктивності (відмова від integrity-захисту в User Plane, кешування станів у stateful-фаєрволах, активне застосування проксі/сервісної сітки) породжують нові класи кібервразливостей, що важко виявляються традиційними засобами. На цьому тлі особливо актуальним є проєктування автономних, політико-керованих систем безпеки з замкненими контурами управління (ETSI ZSM), здатних синхронізувати політики між доменами MANO, швидко локалізувати атаки та мінімізувати побічний вплив на легітимні сервіси.

Мета і задачі дослідження. Метою роботи є створення та експериментальне обґрунтування автономної архітектури кібербезпеки для 5G Core, що забезпечує безпечне поширення політик і швидке реагування на загрози без ручного втручання адміністратора.

Для досягнення цієї мети необхідно вирішити такі задачі:

- провести аналіз типових вразливостей 5G Core у контексті NFV/SDN, SBA, slicing і MEC;
- формалізувати уразливість в станах фаєрвола та ризики модифікації DHCP/RA в User Plane за відсутності integrity-захисту;
- спроєктувати ієрархію доменного (DSO) і локального (LSO) оркестраторів безпеки з PDP/PEP та каскадним поширенням політик (від HSPL до MSPL);
- розробити модуль виявлення конфліктів політик (PCD) між правилами оператора та клієнтських сегментів;
- реалізувати прототип у середовищі Open5GS та Kubernetes/CNF та оцінити часові характеристики реагування й розповсюдження політик;
- провести тестування системи з використанням реальних сценаріїв атак.

Об’єкт дослідження. Процеси забезпечення кібербезпеки в ядрі мобільної мережі 5G (5G Core) в умовах NFV/SDN-інфраструктури.

Предмет дослідження. Механізми автономного, керованого на основі політик захисту (ZSM/MANO, PDP/PEP, HSPL/MSPL, PCD) у 5G Core, включно з алгоритмами поширення політик і оперативними контрзаходами проти атак на цілісність/доступність у User Plane та на рівні stateful-фільтрації.

Наукова новизна одержаних результатів кваліфікаційної роботи. В роботі дістало подальший розвиток політико-кероване поширення безпекових правил у 5G через ієрархію DSO/LSO з інтегрованим Policy Conflict Detector, який автоматизує валідацію клієнтських політик сегментів мережі відносно доменних політик оператора та локального контексту, зберігаючи ізоляцію сегментів і сумісність з MANO/ZSM.

Практичне значення одержаних результатів. Запропоновані механізми:

- зменшують час від виявлення до застосування (TTR) контрзаходів завдяки автоматизованому PDP/PEP і каскадному поширенню політик;
- мінімізують побічні деградації сервісу через таргетоване керування state-записами замість глобальних скидань;
- підвищують надійність конфігурацій UE (DNS/шлюз тощо) у сценаріях, де повний integrity UP недоцільний;
- сумісні з open-source стеком (Open5GS, CNF у Kubernetes) і можуть бути безпосередньо інтегровані у лабораторні стенди операторів/університетів для тестів сегментації, MEC і Zero Trust.

Апробація результатів магістерської роботи. Основні результати дослідження були представлені на XIII науково-технічній конференції «Інформаційні моделі, системи та технології» (ТНТУ, Тернопіль, Україна, 17-18 грудня 2025 р).

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 АРХІТЕКТУРА ТА ВІРТУАЛІЗАЦІЯ ЯДРА МЕРЕЖІ 5G

1.1 Архітектура мережі 5G

Архітектура п’ятого покоління мобільних мереж (5G) є результатом еволюції попередніх стандартів і водночас кардинальним переосмисленням принципів побудови телекомунікаційної інфраструктури [1]. На відміну від попередніх поколінь, де основним завданням було підвищення швидкості передавання даних і ємності радіоканалу, у 5G головним завданням є створення універсальної платформи для підтримки широкого спектра сервісів - від мобільного широкосмугового доступу до промислового Інтернету речей, автономного транспорту та систем критичного реагування. Це потребує гнучкої архітектури, здатної забезпечити масштабованість, програмну керованість, низьку затримку та високу надійність. Загальне уявлення про основні сценарії використання 5G наведено на рисунку 1.1.

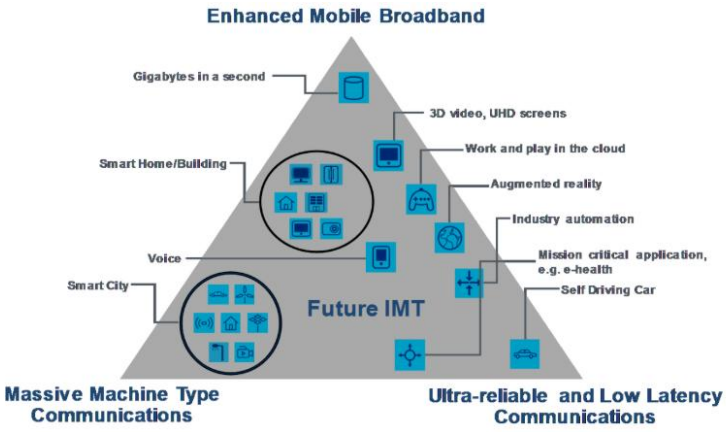


Рисунок 1.1 – Сценарії використання 5G

На рисунку показано три ключові напрями - enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC) і massive Machine-Type Communications (mMTC). Ці сценарії визначили архітектурні вимоги до ядра мережі 5G Core і спрямували розробку її функціональної структури [2].

Перехід від архітектури 4G LTE до 5G означає відмову від монолітної системи Evolved Packet Core (EPC), що складалася з окремих апаратно-

програмних блоків, таких як MME, SGW, PGW, HSS і PCRF. Ці компоненти мали статичну конфігурацію та обмежену гнучкість, що утруднювало модернізацію й масштабування. Архітектура 5G натомість заснована на концепції хмарно-нативного дизайну (cloud-native architecture), який використовує мікросервіси, контейнери й оркестрацію на базі програмно-визначуваних технологій [3]. Мережеві функції більше не прив'язані до конкретного обладнання - вони реалізуються як програмні сервіси, що виконуються у віртуалізованому середовищі на універсальних серверах. Це забезпечує динамічне масштабування, оновлення без зупинки сервісів і незалежне розгортання на різних рівнях інфраструктури - від центральних датацентрів до периферійних вузлів (edge). Таким чином, 5G фактично перетворює мережу на програмно керовану екосистему віртуальних сервісів, де гнучкість і адаптивність замінюють жорстку структуру попередніх поколінь.

Найважливішою рисою архітектури 5G Core є сервісно-орієнтована архітектура (SBA) [4]. Вона передбачає, що кожна мережева функція (NF) є набором окремих сервісів, які можуть викликатися іншими компонентами через стандартизовані програмні інтерфейси. Усі NF реєструються в центральному каталозі NRF, який дозволяє будь-якому елементу мережі динамічно виявляти інші функції та взаємодіяти з ними через HTTP/2 і REST API. Завдяки такій архітектурі 5G отримує гнучкість, адже кожну функцію можна незалежно оновлювати або масштабувати без впливу на інші компоненти. Відкриті інтерфейси забезпечують сумісність рішень різних постачальників і створюють основу для автоматизації процесів керування, коли мережа здатна самостійно реєструвати або видаляти функції відповідно до поточного стану системи. SBA стала фундаментом для реалізації принципів віртуалізації, контейнеризації та DevOps, що спрощує інтеграцію нових сервісів і скорочує час їхнього розгортання.

Архітектура ядра 5G складається з двох основних площин - площини керування (Control Plane) та площини користувацьких даних (User Plane). До першої належать функції AMF, SMF, PCF, UDM, AUSF, NSSF і NEF. Access and Mobility Management Function (AMF) відповідає за автентифікацію користувачів,

керування сесіями підключення, мобільність і сигнальний обмін із базовими станціями через інтерфейс N2. Session Management Function (SMF) створює, змінює й видаляє PDU-сесії, призначає IP адреси, визначає політики маршрутизації та взаємодіє з функцією UPF через інтерфейс N4. Policy Control Function (PCF) формує політики якості обслуговування та тарифікації, тоді як Unified Data Management (UDM) і Authentication Server Function (AUSF) забезпечують управління абонентськими даними та виконання процедур автентифікації. Network Slice Selection Function (NSSF) визначає, до якого мережевого сегмента (slice) буде підключено користувача відповідно до вимог сервісу, а Network Exposure Function (NEF) відкриває API для зовнішніх систем, полегшуючи інтеграцію з додатками та сервісами третьої сторони. Площина користувацьких даних представлена функцією User Plane Function (UPF), яка маршрутизує трафік між терміналом і зовнішніми мережами через інтерфейси N3, N9 та N6 і виконує операції QoS, облік трафіку та глибокий аналіз пакетів (DPI). Разом ці елементи формують розподілену систему мікросервісів, де кожен компонент виконує вузькоспеціалізовані функції, а узгоджена взаємодія забезпечується стандартизованими інтерфейсами N1–Nn.

Система взаємодії між компонентами 5G базується на наборі логічних інтерфейсів, які поділяються за рівнями. Інтерфейс N1 зв’язує користувацьке обладнання (UE) з функцією AMF і використовується для процедур реєстрації, автентифікації та керування з’єднанням. Інтерфейс N2 забезпечує обмін сигнальними повідомленнями між базовою станцією gNB та AMF, тоді як N3 призначений для передавання користувацького трафіку від gNB до UPF. Інтерфейс N4 дозволяє SMF керувати поведінкою UPF, а N6 з’єднує UPF із зовнішніми мережами, зокрема Інтернетом або корпоративною інфраструктурою. Крім того, існують інтерфейси N10–Nn, які забезпечують взаємодію між функціями керування, такими як AUSF–UDM, SMF–PCF або AMF–NSSF. На відміну від попередніх архітектур, де взаємодія здійснювалася через жорстко визначені протоколи, у 5G комунікація відбувається через програмні API, що надає системі більшу гнучкість, модульність і стійкість до збоїв.

Важливою складовою архітектури є концепція розподілених обчислень і (MEC). Вона передбачає переміщення частини обчислювальних процесів і мережевих функцій ближче до користувача, тобто на периферію мережі. Це дозволяє мінімізувати затримки й забезпечити локальну обробку даних без необхідності передавання їх до центрального ядра. Завдяки MEC можливо реалізовувати сервіси з наднизькою затримкою, такі як автономне керування транспортом. MEC також розвантажує магістральні канали та забезпечує кращу ефективність використання ресурсів. Тісна інтеграція MEC із NFV і MANO дає змогу автоматично розгортати необхідні функції на крайових вузлах і управляти ними централізовано, використовуючи механізми оркестрації.

На рівні радіодоступу архітектура 5G включає технологію 5G New Radio (NR), яка використовує масиви антен Massive MIMO, формування променя (beamforming), діапазони міліметрових хвиль і щільне розміщення малопотужних базових станцій (small cells). Що дає змогу досягати високої пропускної здатності в густонаселених міських районах. Базові станції нового покоління (gNB) можуть бути реалізовані як розподілена система, де центральний блок (CU) відповідає за протоколи високого рівня, а розподілений блок (DU) обробляє операції рівня MAC і PHY. Це створює передумови для розгортання хмарних радіомереж (Cloud RAN) і оптимізує використання радіоресурсів.

Попри численні переваги, впровадження 5G супроводжується низкою викликів. До них належать високі інфраструктурні витрати, пов’язані з необхідністю розгортання щільної мережі малих сот, складні процедури регулювання й розподілу спектру, проблеми сумісності між виробниками та підвищені вимоги до безпеки. Останній аспект особливо актуальний через використання віртуалізації, програмно-визначуваних компонентів і відкритих інтерфейсів, які збільшують площину потенційних атак. Вирішення цих проблем можливе завдяки узгодженню стандартів між міжнародними організаціями, такими як 3GPP, ETSI та ITU-T, а також завдяки розробці інтегрованих систем безпеки для віртуалізованих середовищ.

Ще одним важливим аспектом архітектури є енергетична ефективність. Це досягається завдяки адаптивному управлінню потужністю передавання, динамічному вимкненню неактивних базових станцій, локальній обробці даних на MEC-вузлах і оптимізації ресурсів через оркестраційні системи NFV/MANO, які балансують навантаження залежно від поточного стану мережі.

Інтеграція технологій SDN [5] і NFV [6] є наріжним каменем архітектури 5G. SDN розділяє площину керування та площину пересилання даних, забезпечуючи централізоване програмне управління маршрутами й політиками QoS, тоді як NFV переносить мережеві функції на віртуальні платформи, відокремлені від апаратного забезпечення. Разом ці технології створюють основу для динамічного оркестрування ресурсів через ETSI MANO [7], який координує використання обчислювальних, мережевих і сховищних потужностей у різних доменах. Така інтеграція дозволяє швидко розгортати нові сервіси, забезпечувати еластичність ресурсів і суттєво зменшувати експлуатаційні витрати операторів.

1.2 Віртуалізація мережевих функцій та роль MANO

Концепція NFV стала одним із ключових технологічних зрушень, що визначили архітектуру п’ятого покоління мобільних мереж. Якщо у традиційних мережах кожна функція - маршрутизатор, брандмауер, балансувальник навантаження, шлюз або DPI-система реалізувалася на спеціалізованому апаратному забезпеченні, то NFV запропонувала відокремити функціональність від фізичних ресурсів. Завдяки цьому мережеві послуги можуть бути розгорнуті у вигляді програмних компонентів на уніфікованих обчислювальних платформах, що підтримують гнучке масштабування, автоматизоване керування життєвим циклом і динамічне переміщення сервісів у межах хмарної інфраструктури.

Віртуалізація мережевих функцій тісно пов’язана з переходом до ядра 5G Core, у якому кожна мережева функція представлена як мікросервіс або контейнер, що може бути розміщений у будь-якому датацентрі чи на периферії

мережі [8]. Такий підхід радикально змінив процеси проектування, експлуатації та розвитку телекомунікаційних систем. У минулому модернізація мережі вимагала оновлення обладнання, тоді як у середовищі NFV достатньо оновити програмну складову або перезапустити контейнер з новою версією функції. Це дозволяє операторам швидше реагувати на ринкові зміни, розгортати нові сервіси за лічені години й оптимізувати використання інфраструктури.

Основна ідея NFV полягає в тому, що функції, які раніше виконувалися апаратними засобами, тепер можуть бути реалізовані у вигляді програмного забезпечення так званих VNF або CNF. Вони працюють у віртуальних машинах або контейнерах, що запускаються на серверах із гіпервізором [9-11] або оркестратором контейнерів (наприклад, OpenStack, Kubernetes). Цей підхід забезпечує можливість гнучкого розподілу обчислювальних, мережевих і дискових ресурсів між різними функціями, відповідно до поточного навантаження. Для прикладу, під час пікових годин можна автоматично збільшити кількість екземплярів AMF або UPF, тоді як у періоди низької активності зменшити їхню кількість, знижуючи енергоспоживання.

Проте реалізація NFV вимагає складного механізму координації, моніторингу та автоматизації. Саме для цього Європейський інститут телекомунікаційних стандартів (ETSI) розробив архітектуру MANO, що описує, яким чином здійснюється управління життєвим циклом VNFs і сервісів у віртуалізованому середовищі. Як показано на рисунку 2.3, MANO складається з трьох основних рівнів: NFV Orchestrator (NFVO), VNF Manager (VNFM) і Virtualized Infrastructure Manager (VIM).

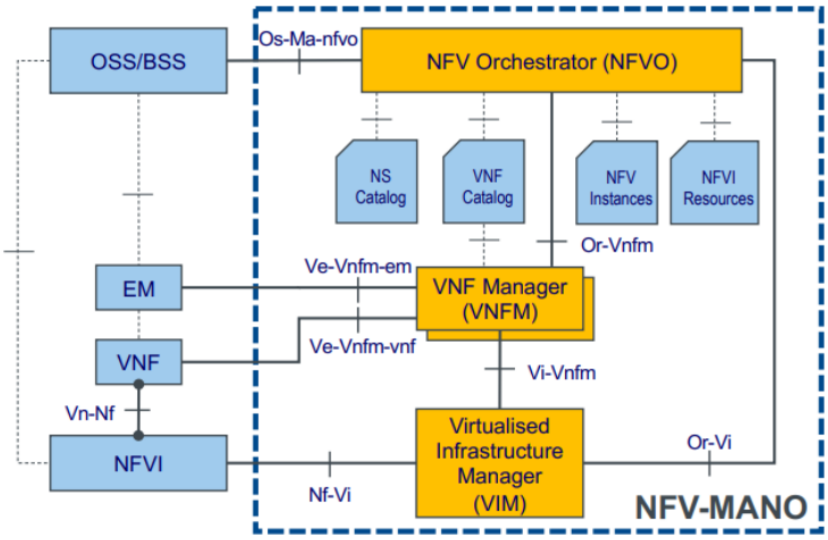


Рисунок 1.2 – Рівні архітектури MANO

Разом вони формують логічну структуру, що координує ресурси, програмні функції та політики розгортання в масштабі всієї мережі.

Роль NFV Orchestrator полягає у загальному керуванні життєвим циклом мережевих сервісів від ініціалізації до завершення. NFVO відповідає за оркестрацію всіх VNFs, їхнє розміщення в обчислювальних доменах і динамічний розподіл ресурсів між ними. У контексті 5G цей компонент є критичним, оскільки саме він забезпечує створення і керування мережевими сегментами (slices), які складаються з набору взаємопов'язаних VNFs, оптимізованих для конкретного сценарію використання - eMBB, URLLC чи mMTC. Коли оператор активує новий slice, NFVO автоматично формує логічний ланцюг функцій, резервує ресурси на відповідних вузлах і гарантує узгодженість параметрів якості обслуговування (QoS) у всіх сегментах мережі. Таким чином, NFVO виступає центральним «мозком» системи, який забезпечує синхронізацію між рівнями керування, ресурсів і сервісів.

VIM відповідає за управління фізичними й віртуальними ресурсами, які становлять основу мережі [12]. Його завдання полягає у моніторингу серверів, віртуальних машин, контейнерів, мережевих інтерфейсів і сховищ. VIM гарантує, що кожна мережева функція отримає необхідну кількість обчислювальних потужностей, пам'яті та пропускної здатності. Він також виконує функцію взаємодії між MANO і гіпервізорами або системами

контейнеризації. Типовим прикладом реалізації VIM є платформи OpenStack чи VMware vCloud, які забезпечують створення та управління віртуальними ресурсами через уніфікований API. У сучасних мережах 5G VIM може бути розподілений між кількома датацентрами, а також інтегрований з MEC-середовищем, що дозволяє розгортати частину функцій безпосередньо на периферії мережі для зменшення затримки.

Третій компонент VNF Manager здійснює управління життєвим циклом конкретних віртуалізованих функцій, включно з розгортанням, оновленням, масштабуванням, моніторингом і завершенням їхньої роботи. VNFM взаємодіє одночасно з NFVO і VIM, отримуючи команди на створення або зміну функцій і передаючи інформацію про їхній поточний стан. Наприклад, коли навантаження на певний сервіс збільшується, NFVO надсилає запит до VNFM, який ініціює створення нового екземпляра функції на вільному вузлі, визначеному VIM. Завдяки цьому мережа 5G може динамічно адаптуватися до змінних умов експлуатації без втручання оператора.

Роль MANO у 5G виходить далеко за межі традиційного управління віртуалізованими ресурсами. У нових архітектурах цей фреймворк забезпечує автоматизацію всіх процесів розгортання та обслуговування, включаючи моніторинг продуктивності, оновлення конфігурацій, балансування навантаження, відновлення після збоїв і закриття життєвого циклу сервісів. Одним із ключових напрямів розвитку MANO є інтеграція з системами штучного інтелекту та машинного навчання, що дозволяє реалізувати концепцію Self-Organizing Networks та Closed-Loop Automation. Завдяки цьому оркестратор може самостійно виявляти відхилення у роботі, прогнозувати зміни трафіку та на випередження оптимізувати ресурси. Це особливо важливо для 5G, оскільки мережа повинна одночасно підтримувати тисячі різних сервісів і пристроїв із гетерогенними вимогами до затримки, пропускної здатності та надійності.

MANO відіграє вирішальну роль у задоволенні нових вимог 5G до автоматизації, масштабованості та динамічного керування ресурсами. Зокрема, MANO не лише керує окремими VNF, але й координує всю інфраструктуру, забезпечуючи узгодженість між політиками QoS, обчислювальними ресурсами

та мережевими параметрами. Коли з’являється потреба у новому сервісі, MANO ініціює оркестрацію відповідних компонентів, виділяє ресурси через VIM, налаштовує параметри зв’язності через SDN-контролер і передає керування на рівень VNFM. Такий рівень автоматизації перетворює процес на цілком програмно-керований цикл, де більшість операцій виконується без участі людини.

У контексті поділу мережі (slicing) MANO забезпечує створення, підтримку та видалення окремих логічних сегментів, що функціонують на спільній фізичній інфраструктурі. Кожен slice може мати власні політики керування, рівень безпеки та вимоги до якості обслуговування. MANO відповідає за розподіл обчислювальних і мережевих ресурсів між цими сегментами та гарантує, що зміни в одному з них не впливають на інші. Це досягається завдяки тісній взаємодії з контролерами SDN, які керують маршрутизацією трафіку між VNFs і забезпечують логічну ізоляцію потоків. Така функціональність робить можливим надання спеціалізованих послуг різним галузям від транспортної до енергетичної чи медичної у межах єдиної фізичної інфраструктури.

MANO також відіграє ключову роль у підтримці концепції MEC. Оскільки частина функцій ядра може бути розгорнута на периферійних вузлах, система оркестрації повинна визначати оптимальне місце для розміщення кожного компонента з урахуванням затримки, навантаження та пропускної здатності каналів. Наприклад, функції UPF або частина SMF можуть бути перенесені ближче до користувача, тоді як інші, менш критичні, залишаються у центральному датацентрі. MANO координує цей розподіл і забезпечує синхронізацію між edge- і core-доменами.

Безпековий аспект також є невід’ємною частиною архітектури NFV/MANO. Перехід від фізичних до віртуальних компонентів розширює потенційну поверхню атак, тому система управління повинна реалізовувати політики безпеки на кожному рівні від гіпервізора до оркестратора. MANO інтегрується з механізмами аутентифікації, контролю доступу, моніторингу й ведення журналів, забезпечуючи відстеження дій користувачів і запобігання несанкціонованим змінам у конфігурації. Вона також може виконувати

автоматичну реакцію на інциденти, наприклад, переміщення функцій на інші вузли або ізоляцію підозрілих компонентів.

1.3 Сегментація мережі (network slicing)

Одним із найважливіших технологічних нововведень, що визначають архітектуру п’ятого покоління мобільних мереж, є концепція сегментації network slicing [13]. Цей підхід радикально змінює спосіб, у який оператори розподіляють ресурси й надають послуги, дозволяючи будувати множину віртуальних мереж поверх спільної фізичної інфраструктури. Кожна така мережа або "slice" функціонує як логічно незалежна система, адаптована під конкретний тип застосування, сервіс або групу користувачів. Як показано на рисунку 1.3 кожен slice може мати власну архітектуру, політику безпеки, якість обслуговування та набір функцій, незважаючи на те, що всі вони поділяють одні й ті самі фізичні ресурси мережі оператора.

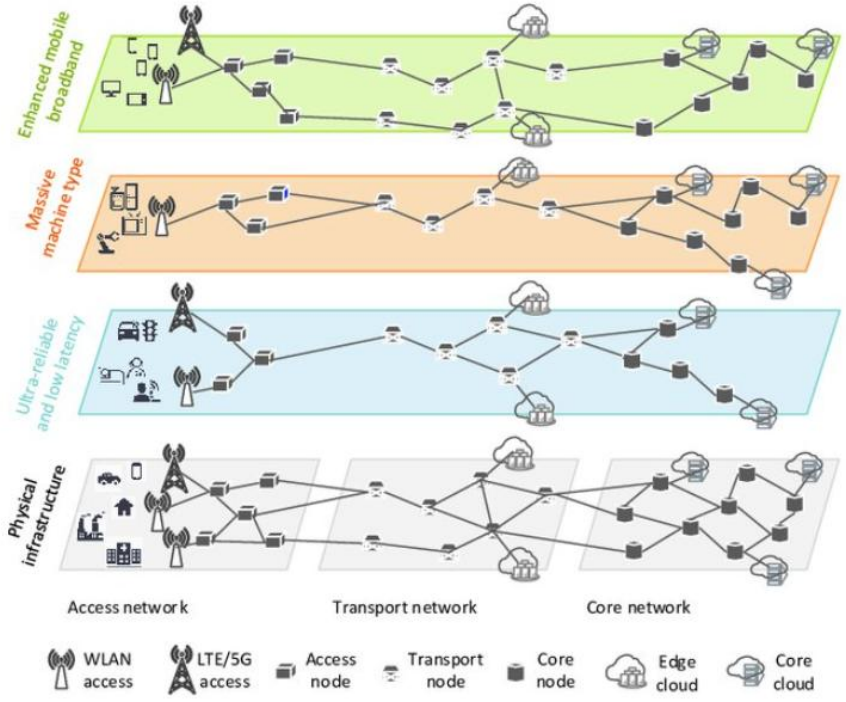


Рисунок 1.3 – Приклад концепція сегментації network slicing в 5G

Це стало можливим завдяки розвитку таких технологій, як NFV, SDN і оркестраційні фреймворки ETSI MANO, що забезпечують повну абстракцію, автоматизацію й динамічне керування ресурсами.

У традиційних мережах усі користувачі та сервіси обслуговувалися єдиною інфраструктурою з уніфікованими параметрами пропускної здатності, затримки та надійності. Такий підхід був прийнятним для попередніх поколінь мобільного зв'язку, але виявився непридатним для 5G, де одночасно співіснують сервіси з абсолютно різними вимогами від потокового відео високої роздільності до промислових систем автоматизації та масових сенсорних мереж IoT. Саме тому виникла потреба у створенні механізму, який дозволяє поділити єдину фізичну мережу на кілька логічних сегментів, кожен з яких має свої ресурси, рівень ізоляції й політику керування. У цьому контексті network slicing виступає як архітектурна парадигма, що дає змогу операторам мобільного зв'язку надавати кастомізовані послуги для різних галузей економіки, зберігаючи при цьому ефективність використання інфраструктури.

У загальному вигляді network slicing спирається на три основні принципи: ізоляцію, кастомізацію та динамічність. Ізоляція означає, що кожен slice є логічно відокремленим від інших, а його робота не впливає на продуктивність сусідніх сегментів навіть за умови спільного використання апаратних ресурсів. Це особливо важливо для критичних застосувань, таких як транспортні системи або медичні сервіси, де відмова або затримка в одному сегменті не повинна мати жодного впливу на інші. Кастомізація полягає у тому, що кожен slice може бути налаштований під конкретні технічні вимоги: у одних випадках це максимальна пропускна здатність, у інших - низька затримка чи енергоефективність. Динамічність передбачає, що ресурси можуть перерозподілятися в реальному часі залежно від зміни навантаження або появи нових сервісів, що робить slicing гнучким і саморегульованим механізмом.

Принцип network slicing у 5G реалізується шляхом поділу спільної фізичної інфраструктури на множину ізольованих віртуальних мереж, кожна з яких оптимізована для певного типу послуг. Наприклад, slice, призначений для Enhanced Mobile Broadband, зосереджується на високій пропускній здатності та масовому трафіку, slice для Ultra-Reliable Low-Latency Communications - на мінімізації затримки та максимальній надійності, тоді як slice для Massive Machine-Type Communications - на підтримці великої кількості пристроїв із

низьким енергоспоживанням. Кожен із цих сегментів може мати власну конфігурацію компонентів ядра, політики QoS, функції безпеки й навіть окремі маршрути трафіку в межах мережі. Таким чином, slicing створює середовище, у якому 5G здатна одночасно підтримувати мобільний широкосмуговий доступ, промислові додатки реального часу та глобальні IoT-системи.

Для реалізації цієї концепції використовуються технології NFV та SDN, які забезпечують віртуалізацію функцій і централізоване керування мережею. Віртуалізація дозволяє створювати окремі екземпляри мережевих функцій (AMF, SMF, UPF тощо) для кожного slice, а SDN-контролер керує маршрутизацією трафіку між ними, визначаючи, яким шляхом проходитиме потік даних. Це означає, що фізична топологія мережі стає гнучкою та програмно керованою, а новий slice може бути створений, змінений або видалений без потреби у фізичному втручанні. Оркестраційний рівень ETSI MANO відіграє центральну роль у цьому процесі, забезпечуючи автоматичне розгортання VNFs, виділення ресурсів через VIM і узгодження всіх елементів системи через NFVO. MANO працює у тісній інтеграції зі специфікацією 3GPP для Network Slice Management Function (NSMF), що відповідає за координацію створення й керування слайсами на рівні ядра мережі.

На концептуальному рівні архітектура slicing передбачає, що кожен slice складається з кількох підрівнів: Radio Access Network (RAN) Slice, Core Network Slice і Transport Slice. Це означає, що сегментація охоплює не лише ядро, але й доступову та транспортну частини мережі. У RAN slicing може здійснюватися через виділення окремих ресурсів спектру, антенних груп або черг пріоритету. У ядрі мережі slicing відображається у створенні окремих інстансів функцій AMF, SMF, UPF, які взаємодіють лише в межах одного логічного сегмента. Транспортна сегментація передбачає динамічне керування маршрутами між елементами slice за допомогою SDN, що дозволяє досягти гарантованих показників затримки та пропускної здатності.

Важливою перевагою slicing є підвищення ефективності використання ресурсів. У традиційних системах мережа резервувала ресурси під конкретний тип сервісу навіть тоді, коли вони не використовувалися. Завдяки динамічному

розподілу ресурсів між slice, 5G може балансувати навантаження, передавати невикористані ресурси іншим сегментам і тим самим зменшувати операційні витрати. Для оператора це означає можливість пропонувати мережу як послугу Network-as-a-Service (NaaS) де клієнт може замовити власний slice із заданими характеристиками. У цьому сенсі slicing стає не лише технічною, а й бізнес-моделлю, що відкриває нові джерела доходів, наприклад, для промислових підприємств, логістичних компаній або медичних закладів, які потребують гарантованого рівня сервісу.

Однією з основних проблем реалізації є складність управління великою кількістю slice, кожен з яких має свої вимоги, політики безпеки, життєвий цикл і динаміку трафіку. Для забезпечення стабільності системи потрібні потужні інструменти моніторингу, аналітики та автоматизації, що здатні в реальному часі контролювати стан кожного сегмента, передбачати потенційні конфлікти ресурсів і здійснювати випереджальну оптимізацію. Без цього slicing ризикує перетворитися на важко керовану структуру, де збільшення кількості віртуальних сегментів призводить до деградації продуктивності.

Ще одним важливим аспектом є безпека. Попри логічну ізоляцію, усі слайси функціонують на спільній фізичній інфраструктурі, що створює потенційні ризики міжсегментного впливу. Наприклад, у разі порушення ізоляції або неправильної конфігурації зловмисник може спробувати отримати доступ до ресурсів іншого slice, викликавши ланцюговий ефект у масштабах усієї мережі. Тому архітектура безпеки 5G передбачає суворе застосування політик контролю доступу, багаторівневе шифрування й постійний моніторинг активності на рівні MANO та SDN-контролерів. Кожен slice має власну політику безпеки, що включає автентифікацію користувачів, аудит дій і засоби виявлення вторгнень [14,15], інтегровані з загальною системою управління подіями безпеки (SIEM).

З точки зору продуктивності, network slicing дозволяє гнучко керувати якістю обслуговування. Кожен slice може бути оптимізований під певні метрики, такі як пропускна здатність, затримка або надійність. Наприклад, для автономних транспортних систем критичними є затримка не більше 1 мс і безперервність з’єднання, тоді як для потокового відео основним параметром є

висока пропускна здатність. Мережевий оркестратор аналізує вимоги до сервісу та розподіляє ресурси відповідно до пріоритетів, гарантуючи, що навіть при високому навантаженні критичні слайси матимуть перевагу.

У поєднанні з механізмами NFV і MANO slicing формує основу для повністю автоматизованих мереж 5G, де створення нового сегмента може здійснюватися програмно через API. Це дозволяє операторам і корпоративним клієнтам динамічно адаптувати мережу під свої потреби, наприклад, створювати тимчасові slice для спортивних подій, виставок або надзвичайних ситуацій. Згідно з принципами ETSI MANO, життєвий цикл slice включає етапи проектування, розгортання, моніторингу, масштабування та завершення, які виконуються автоматично під контролем оркестратора. Такий підхід робить slicing ключовим елементом концепції "zero-touch network", де втручання людини мінімізоване. З економічної точки зору, slicing сприяє переходу операторів від моделі універсальної мережі до моделі орієнтованих сервісів. Це означає, що мережа більше не є статичною інфраструктурою, а перетворюється на платформу, здатну підтримувати різноманітні бізнес-сценарії. Наприклад, один оператор може одночасно обслуговувати споживачів потокового відео, промислові підприємства, транспортні компанії та роздрібну торгівлю, при цьому кожен із клієнтів користується власним ізольованим slice із гарантованими характеристиками. Така модель відкриває нові можливості монетизації мережі й створює умови для тіснішої взаємодії між телекомунікаційною сферою та галузями економіки.

1.4 Безпека в архітектурі 5G

Безпека є однією з ключових проблем архітектури мереж п’ятого покоління, оскільки 5G поєднує у собі високий рівень віртуалізації, розподілену структуру, програмно-визначувані технології та масове підключення пристроїв. Архітектурні інновації, які роблять 5G гнучкою, масштабованою і продуктивною системою, водночас створюють нові поверхні для потенційних атак і загроз. Саме тому безпека у 5G не може розглядатися як окремий компонент. Вона

повинна бути інтегрована на всіх рівнях архітектури, від фізичної інфраструктури до хмарних середовищ, де виконуються віртуалізовані функції ядра.

На відміну від попередніх поколінь мобільних мереж, де основні елементи архітектури були реалізовані у вигляді апаратних пристроїв з фіксованими функціями, у 5G більшість ключових мережевих компонентів реалізується програмно, у вигляді VNFs або CNFs, які виконуються в середовищах віртуалізації чи контейнеризації. Це означає, що безпека мережі залежить не лише від фізичного захисту обладнання, а й від надійності програмного коду, гіпервізорів, контейнерних оркестраторів і механізмів керування ресурсами. У таких умовах будь-яка вразливість у програмному забезпеченні або неправильна конфігурація може стати точкою входу для атаки [16], яка потенційно здатна вплинути на кілька віртуальних функцій одночасно.

Віртуалізація, що лежить в основі архітектури 5G Core, надає значну гнучкість і економічну ефективність, проте вона розширює поверхню атаки, роблячи систему більш уразливою до загроз типу “multi-tenant” або “side-channel”, коли зловмисник може використати спільні ресурси процесора чи пам’яті для витоку даних між ізольованими середовищами. Це особливо критично в умовах NFV і MANO, де один фізичний сервер може одночасно обслуговувати десятки мережевих функцій різних операторів або різних slices. Як показано на рисунку 1.2, система MANO складається з взаємопов’язаних рівнів управління, які мають доступ до фізичних і логічних ресурсів мережі, тому компрометація оркестратора або менеджера віртуальної інфраструктури (VIM) може мати катастрофічні наслідки для всієї мережі.

Одним із найсерйозніших викликів безпеки у 5G є складність самої архітектури. У порівнянні з 4G, нове покоління включає більше рівнів, компонентів і точок взаємодії: базові станції, MEC-вузли, ядро, SDN-контролери, оркестратори MANO, численні API для зовнішніх сервісів. Кожен із цих елементів є потенційним вектором атаки. Для прикладу, функція Network Exposure Function (NEF), яка відкриває стандартизовані інтерфейси до зовнішніх систем і додатків, створює нові ризики, пов’язані з автентифікацією, контролем

доступу та перевіркою запитів. У разі некоректної реалізації API зловмисник може отримати доступ до внутрішніх сервісів ядра або зібрати конфіденційну інформацію про структуру мережі.

Іншим важливим аспектом є ланцюг постачання. Побудова мережі 5G передбачає інтеграцію великої кількості апаратних і програмних компонентів від різних виробників, що створює ризики на етапі виробництва, транспортування або оновлення. Коли неблагонадійні постачальники можуть свідомо або несвідомо інтегрувати шкідливі елементи або залишити бекдори у своєму обладнанні. У віртуалізованих середовищах цей ризик збільшується, оскільки використання відкритих бібліотек і контейнерів із публічних репозиторіїв може призвести до потрапляння в систему вразливого або зараженого коду.

Не менш небезпечним є зростання кількості пристроїв Інтернету речей (IoT), які підключаються до мережі 5G. Масове підключення мільйонів пристроїв створює нову площину ризиків, оскільки більшість IoT-компонентів мають обмежені обчислювальні ресурси і не підтримують складні механізми шифрування чи автентифікації. Що робить їх легкою мішенню для атак типу DDoS [17] або ботнетів. У таких умовах навіть один скомпрометований пристрій може стати точкою входу для масштабної атаки на мережу, використовуючи протоколи управління або сигнальні інтерфейси.

Додатковим джерелом уразливостей стає network slicing, яка, з одного боку, дозволяє ефективно ізолювати сервіси, а з іншого збільшує складність управління безпекою. Кожен slice є окремою логічною мережею з власними політиками доступу, рівнем пріоритетів і параметрами QoS. Якщо механізми ізоляції між slices не реалізовані належним чином, атака на один сегмент може поширитися на інші. Оскільки всі слайси поділяють спільну фізичну інфраструктуру та оркестраційний рівень, компрометація MANO або SDN-контролера може призвести до міжсегментного доступу, що загрожує конфіденційності та цілісності даних.

Не менш значущою проблемою є розподілений характер архітектури 5G, зокрема використання Multi-Access Edge Computing. Перенесення обчислень на периферію мережі покращує продуктивність, але створює додаткові точки

потенційного проникнення. На відміну від централізованих датацентрів, edge-вузли можуть розміщуватися у віддалених або слабо контрольованих локаціях, де складніше забезпечити фізичну безпеку, моніторинг і оперативне оновлення програмного забезпечення. Це робить MEC середовище привабливим для атак, спрямованих на модифікацію контейнерів, перехоплення трафіку або підміну службових компонентів.

Складність архітектури 5G посилюється відсутністю повністю стандартизованих протоколів безпеки для нових елементів, таких як slicing, NFV або edge computing. Хоча організації 3GPP і ETSI активно розробляють відповідні специфікації, на практиці різні вендори можуть реалізовувати власні механізми аутентифікації, шифрування й управління ключами, що призводить до фрагментації. Внаслідок цього у місцях стику різних систем можуть виникати вразливості, які складно виявити на етапі тестування. Також актуальною залишається проблема інтеграції спадкової інфраструктури. Оскільки 5G на початкових етапах розгортання співіснує з мережами 4G і навіть 3G, необхідність підтримки зворотної сумісності може призвести до появи слабких місць у захисті, особливо у разі тунелювання трафіку через застарілі протоколи або шлюзи.

Питання безпеки у 5G не обмежуються технічними аспектами, вони мають також організаційний і правовий вимір. Використання віртуалізованих сервісів означає, що дані користувачів можуть оброблятися у різних географічних зонах або навіть у хмарах сторонніх провайдерів. Це створює ризики для приватності та захисту персональної інформації, оскільки у різних юрисдикціях діють різні вимоги до зберігання та передачі даних. У контексті масового збору телеметричних даних, який притаманний 5G, забезпечення конфіденційності стає одним із центральних викликів. Для зменшення впливу зазначених ризиків у 5G поступово впроваджуються нові підходи до безпеки. Один із них - Zero Trust Security Model, який виходить із принципу, що жоден елемент мережі не може вважатися довіреним за замовчуванням. Це означає, що кожна взаємодія між компонентами повинна супроводжуватися автентифікацією, авторизацією й перевіркою цілісності незалежно від того, чи відбувається вона у межах одного

домену чи між різними slice. Модель Zero Trust вимагає наскрізного контролю на всіх рівнях від користувацького пристрою до хмарного ядра і постійного моніторингу поведінки мережі для виявлення аномалій [18].

Важливою складовою безпеки у 5G є динамічна сегментація політик і мультишарове шифрування. Оскільки трафік проходить через численні віртуалізовані середовища, використовується комбінація транспортного шифрування (TLS, IPsec) і шифрування на рівні застосунків. Для кожного slice можуть бути встановлені власні криптографічні профілі, що регулюються оркестратором MANO. Крім того, активно застосовуються системи моніторингу з машинним навчанням, які аналізують трафік у реальному часі, виявляючи ознаки компрометації чи несанкціонованого доступу.

Захист edge-середовищ і MEC є ще одним напрямом розвитку 5G-безпеки. Тут використовуються механізми довіреного завантаження (secure boot), віддаленої атестації та виявлення аномалій на периферійних вузлах. Взаємодія між edge і core здійснюється через захищені тунелі, а управління контейнерами виконується централізовано з урахуванням політик доступу.

Проблема безпеки у ланцюгу постачання вирішується шляхом впровадження процедур перевірки постачальників і сертифікації компонентів, використання підписаних артефактів програмного забезпечення та систем безперервного аудиту. Для захисту даних користувачів широко застосовується наскрізне шифрування, завдяки якому навіть у разі перехоплення трафіку зловмисник не може його дешифрувати.

Таким чином, у контексті віртуалізації безпека у 5G набуває комплексного, багаторівневого характеру. Вона більше не обмежується межами окремих пристроїв або сегментів, а охоплює весь життєвий цикл мережевих функцій від створення контейнерів до їхньої оркестрації й моніторингу. Така стратегія повинна включати постійне оновлення програмного забезпечення, моніторинг активності, сегментацію прав доступу, виявлення аномалій і автоматичне реагування на інциденти.

1.5 Використання open-source реалізацій 5G Core:

Розвиток мобільних мереж п’ятого покоління супроводжується появою відкритих, програмно реалізованих платформ, які дозволяють дослідникам і розробникам створювати, тестувати та вдосконалювати функціональні елементи ядра мережі без потреби у дорогому пропрієтарному обладнанні. Відкриті реалізації 5G Core, такі як Open5GS [19] та Free5GC, стали ключовими інструментами для академічних і лабораторних досліджень, а також для побудови прототипів майбутніх телекомунікаційних систем. Вони відповідають специфікаціям 3GPP, реалізують основні NF і підтримують архітектуру SBA, що лежить в основі ядра 5G. Використання таких рішень сприяє демократизації технологій, відкриває доступ до глибшого розуміння внутрішніх механізмів 5G і дозволяє експериментувати з новими підходами до віртуалізації, оркестрації та безпеки.

Як показано на рисунку 1.1, архітектура 5G складається з розподіленої мережі функцій, серед яких AMF, SMF, UPF, PCF, UDM, AUSF, NSSF, NRF і NEF. Кожна з цих функцій у відкритих реалізаціях представлена окремим програмним модулем або мікросервісом, який взаємодіє з іншими компонентами через стандартизовані інтерфейси Nn, визначені у специфікаціях 3GPP. На відміну від апаратних рішень, open-source платформи реалізують ці функції як контейнери або демон-процеси, що дозволяє розгортати їх на звичайних серверах під управлінням Linux, у хмарних середовищах або навіть на персональних комп’ютерах для навчальних цілей.

Open5GS - це одна з найпоширеніших відкритих реалізацій ядра 5G, орієнтована на модульність і простоту розгортання [19]. Проєкт розробляється спільнотою ентузіастів і підтримує як автономний режим (SA), так і неавтономний (NSA), що дозволяє інтегрувати 5G Core із мережею EPC 4G. Завдяки цьому Open5GS є гнучким інструментом для побудови гібридних архітектур і дослідження процесів міграції від LTE до 5G. Система реалізує основні компоненти ядра - AMF, SMF, UPF, PCF, UDM, AUSF і NRF, які взаємодіють через SBA інтерфейси з використанням HTTP/2 і JSON. Така

структура відображає принципи архітектури 5GC, де кожна функція виступає як незалежний сервіс, що реєструється у NRF і може масштабуватися або оновлюватися автономно. Особливістю Open5GS є його прозорість і сумісність із віртуалізаційними платформами. Система може бути розгорнута як у вигляді локальних процесів, так і в контейнерному середовищі Docker або Kubernetes, що полегшує інтеграцію з оркестраторами NFV/MANO. Це дозволяє дослідникам моделювати повноцінну інфраструктуру оператора зв'язку в лабораторних умовах, експериментувати з різними топологіями, механізмами розподілу трафіку, алгоритмами балансування навантаження або політиками якості обслуговування (QoS). Завдяки відкритому коду можна безпосередньо аналізувати внутрішню логіку сигнальних процедур, таких як реєстрація користувача, встановлення PDU-сесії, маршрутизація трафіку чи управління мобільністю. Це робить Open5GS цінним навчальним ресурсом для університетів і дослідницьких центрів, які займаються питаннями віртуалізації, кібербезпеки та мережевої оркестрації.

Інша популярна платформа, Free5GC, є відкритим проєктом, що спочатку був започаткований дослідниками Національного Тайванського університету. Free5GC зосереджується на реалізації ядра 5G з використанням контейнеризації, мікросервісної архітектури та автоматизованого масштабування. На відміну від Open5GS, який має монолітніші процеси, Free5GC побудований повністю за принципами cloud-native і підтримує динамічне керування життєвим циклом функцій через Kubernetes. Це робить його зручним для досліджень у сфері оркестрації, network slicing і інтеграції з Multi-Access Edge Computing. Free5GC також повністю відповідає специфікаціям 3GPP Release 15 і частково підтримує Release 16, включаючи реалізацію NSSF для управління слайсами, що дозволяє моделювати створення ізольованих віртуальних мереж поверх спільної інфраструктури. Підтримка SDN у платформі реалізована через інтеграцію з контролерами, такими як ONOS або OpenDaylight, що дозволяє будувати динамічні маршрути трафіку та керувати політиками QoS у реальному часі.

Важливою перевагою обох платформ є можливість взаємодії з відкритими інструментами віртуалізації радіодоступу. Найчастіше вони використовуються

разом із UERANSIM, який емулює gNB (базову станцію) та UE (користувацьке обладнання), забезпечуючи повноцінну сигнальну взаємодію через інтерфейси N1, N2 і N3. Така комбінація дозволяє дослідникам створювати повноцінні експериментальні мережі 5G, де Open5GS або Free5GC виконують роль ядра, а UERANSIM – радіодоступу [20]. Цей підхід дає змогу відтворити типові сценарії реєстрації користувача, встановлення PDU-сесій, маршрутизації трафіку та перевірки QoS без використання реального обладнання, що особливо цінно для навчальних і дослідницьких цілей.

Використання відкритих реалізацій також полегшує тестування рішень у сфері кібербезпеки. В умовах, коли 5G активно впроваджує віртуалізацію, сегментацію мережі та розподілені обчислення, виникає потреба у перевірці механізмів захисту, виявлення аномалій і протидії кібератакам. Open5GS і Free5GC дозволяють впроваджувати засоби безпеки на різних рівнях архітектури, експериментувати з Zero Trust моделлю, механізмами контролю доступу або інтеграцією систем виявлення вторгнень (IDS/IPS) у контексті NFV. Наприклад, дослідник може модифікувати код функції AMF, щоб додати логіку поведінкового аналізу користувачів або впровадити новий алгоритм шифрування на рівні SMF чи UPF. Така відкритість і гнучкість відсутня у комерційних продуктах, де код є закритим і недоступним для змін.

З технічного погляду, Open5GS частіше використовується для навчальних демонстрацій і тестування базових функцій 5G Core, тоді як Free5GC орієнтований на складніші експерименти з контейнеризацією, масштабуванням і оркестрацією. Обидві платформи сумісні з віртуальними середовищами OpenStack і Kubernetes, що дозволяє інтегрувати їх у системи керування ETSI MANO або аналогічні оркестратори. Таким чином, вони можуть бути частиною більших лабораторних середовищ, де досліджується взаємодія між NFV, SDN, MEC і network slicing.

Попри значні переваги, open-source реалізації мають і свої обмеження. Їхня продуктивність і стабільність зазвичай поступаються промисловим рішенням, особливо під час оброблення великих обсягів трафіку або підтримки тисяч одночасних з’єднань. Крім того, через відкритий характер кодової бази питання

безпеки потребує додаткової уваги, адже недосвідчений користувач може розгорнути систему з некоректними налаштуваннями, що відкриє доступ до критичних елементів мережі. Тим не менше, для цілей дослідження й тестування такі рішення залишаються безцінними, оскільки дозволяють експериментувати з реальними протоколами, аналізувати поведінку трафіку та виявляти потенційні проблеми ще до впровадження у промислових масштабах. У контексті глобальної стандартизації відкриті 5G Core-платформи мають ще одну перевагу - вони сприяють узгодженню реалізацій і перевірці сумісності між різними виробниками. Завдяки публічному доступу до коду та інтерфейсів розробники з усього світу можуть перевіряти коректність реалізації специфікацій 3GPP, експериментувати з новими версіями протоколів або створювати доповнення для майбутніх релізів. У результаті такі платформи не лише відображають поточний стан технології, але й формують підґрунтя для її подальшої еволюції.

1.6 Висновки до розділу 1

У першому розділі було розглянуто архітектуру мережі 5G, принципи віртуалізації мережевих функцій та роль системи MANO у керуванні життєвим циклом віртуальних сервісів. Детально проаналізовано концепцію сегментації мережі (network slicing), що забезпечує гнучке розподілення ресурсів і створення ізольованих логічних мереж для різних типів сервісів. Окрему увагу приділено питанням безпеки у віртуалізованому середовищі 5G та викликам, пов’язаним із розподіленою архітектурою, MEC і IoT. Також описано практичне значення open-source реалізацій Open5GS та Free5GC, які забезпечують експериментальну платформу для дослідження й тестування ядра 5G.

РОЗДІЛ 2 АНАЛІЗ ВРАЗЛИВОСТЕЙ У СЕРЕДОВИЩІ 5G CORE

2.1 Огляд типових вразливостей та атак у віртуалізованих мережах

Перехід телекомунікаційних архітектур до технологій NFV та SDN у поєднанні з розгортанням 5G Core радикально змінив природу загроз. Тепер атаки рідше виглядають як одноточкові експлойти проти апаратного вузла й частіше набувають системного характеру, виростаючи з логічних невідповідностей між шарами інфраструктури, відсутністю чітких границь довіри й компромісу між продуктивністю та безпекою. У таких середовищах типові вектори загроз зберігають свою класичну сутність, але набувають нових ефектів і масштабів через властивості віртуалізації: мультиорендування ресурсів, динамічність життєвих циклів VNFs, інтенсивне використання проксі та сервісної сітки (service mesh) і поширення east–west трафіку між мікросервісами. Загалом загрози можна розглянути через три взаємопов’язані параметри доступність, цілісність і конфіденційність (див. рисунок 2.1) [21].

Рисунок 2.1 – CIA-тріада

Проте в віртуалізованому контексті ці виміри взаємно підсилюються й породжують проміжні класи атак, характерні саме для розподілених 5G-систем.

У площині доступності основну роль продовжують відігравати DoS- та DDoS-атаки, однак механіка їхньої реалізації у віртуальних мережах відрізняється. Масштабовані NFV-інстанси й програмні комутатори часто поділяють апаратні пулі CPU, I/O та кешів, тому цільова навантажувальна атака може використовувати як мережеві, так і «сусідські» вектори, спрямовані на загальні ресурси. Крім того, поширений у мережевих сервісах connection-less протоколи створюють сприятливе середовище для віддзеркалених атак із високим коефіцієнтом підсилення. З невеликого обсягу запитів атакуючий може індукувати великий обсяг відгуків до жертви, що посилює ефект DDoS без пропорційного зростання власних ресурсів зловмисника [22]. У віртуалізованому середовищі це підсилюється поведінкою масштабованих компонентів і динамічним відкриттям і закриттям сесій, коли черги обробки, правила QoS і спільні черги kernel-space/user-space стають «вузькими місцями» для оператора.

Атаки на цілісність у 5G особливо небезпечні тією обставиною, що частина службового трафіку можуть обходити захищені канали або бути переданими через елементи інфраструктури, де цілісність не гарантується обов’язково. Прикладом є сценарії, коли посередник змінює поля протоколів прикладного рівня або конфігураційні параметри, не долаючи при цьому криптографічного бар’єра для читання вмісту.. Типова реалізація такого підходу полягає у вставленні шкідливої адреси або маршруту в потік ініціалізації сервісу, що може перенаправити користувача на злочинний ресурс або змінити критичні параметри конфігурації. Робочий сценарій подібного втручання з детальним call-flow ілюструє, як зміна адреси резолвера може поступово призвести до підміни кінцевого сервера (див. рисунок 2.2).

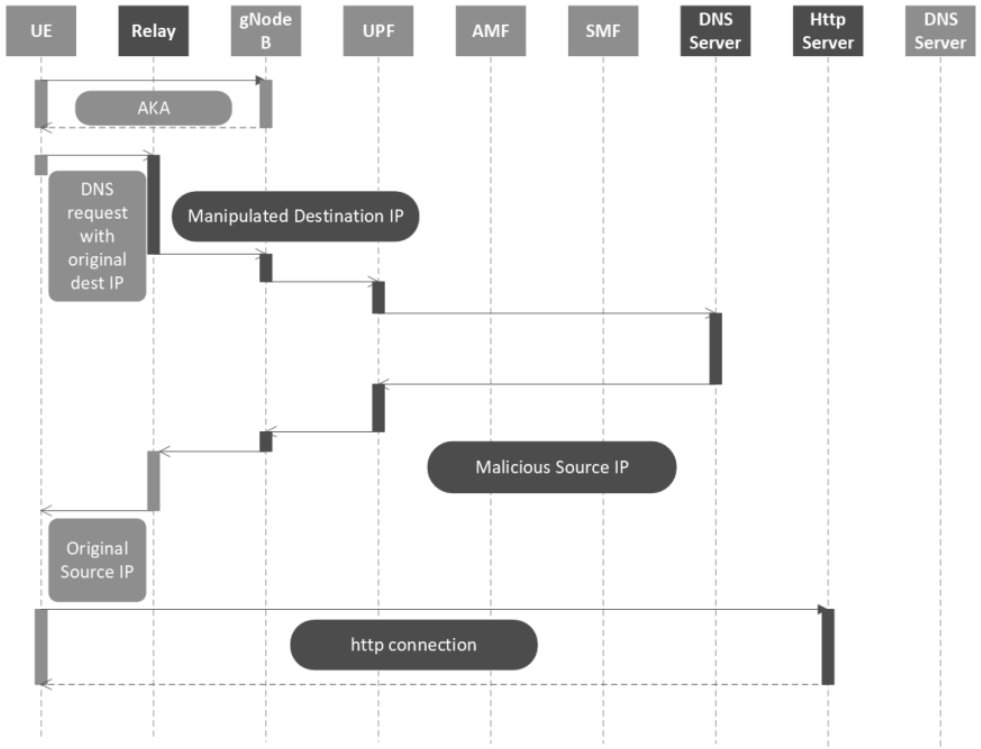


Рисунок 2.2 – Послідовність атаки

Такий клас атак показує, що наявність або відсутність захисту цілісності для окремих ділянок мережі має критичне значення. Навіть часткове відключення integrity-механізмів в ім’я продуктивності здатне створити «точки входу» для маніпуляцій.

Проблеми конфіденційності у віртуалізованих системах теж набувають нових форм. Поширені техніки ексфільтрації даних через дозволені служби, наприклад, DNS-тунелювання, стають менш помітними у середовищах, де велика частина внутрішнього трафіку розглядається як довірена або коли використовується спільний резолвер для багатьох орендарів. В поєднанні з недосконалою сегрегацією ресурсів та механізмами логування це призводить до хибного відчуття безпеки. Зловмисник може періодично передавати невеликі фрагменти інформації, які у підсумку дозволяють зібрати конфіденційні дані, тоді як традиційні індикатори аномалій залишаються у межах очікувань.

Окремим і важливим класом загроз є складні, багатоетапні атаки. У віртуалізованому середовищі їхня послідовність стає більш витонченою. Початкове проникнення може бути досягнуте через уразливість конкретної VNF або через помилкові налаштування оркестратора, далі відбувається інсталяція

бекдору та переміщення всередині доменів, використовуючи внутрішні служби як платформи розповсюдження. Ключова небезпека такого сценарію - це поєднання слабких місць різних рівнів: вразливого API оркестратора, недостатньої ізоляції контейнерів, відсутності жорсткої політики ротації примітивів шифрування і обмежених інструментів телеметрії, що ускладнює кореляцію подій у масштабі всього кластера.

Технологічні аспекти віртуалізації також породжують специфічні атаки, не завжди асоційовані з класичними мережевими векторами. Спільне використання апаратних ресурсів породжує загрози типу «noisy neighbor» та side-channel, коли поведінка одного орендаря по кешам, тактам CPU або пам’яті може бути використана для витоку або деградації сервісу іншого. У мережевому контексті сучасні стеки прискорення пакетів у user-space і DPDK-based рішення підвищують пропускну здатність, але водночас переміщують обробку в контекст, де доступ контролю більш обмежений і де легше виникають тимчасові канали чи конкурентні вузькі місця.

Іншою системною проблемою є невідповідність політик і життєвих циклів між компонентами. У динамічному середовищі правила фільтрації, таблиці станів, політики QoS і механізми маршрутизації можуть змінюватися незалежно одне від одного. Така асинхронність призводить до ситуацій, коли ті чи інші рішення безпеки перестають застосовуватися послідовно. Саме ця операційна складність пояснює, чому атаки, що раніше вважалися малоефективними, у віртуалізованому 5G-ядрі часто виявляються надзвичайно витривалими й важкими для локалізації.

Нарешті, важливо зазначити прикладну взаємодію між вектором загрози та потребами експлуатації: оператори часто змушені балансувати між рівнем захисту та показниками QoS. Вимкнення деяких механізмів захисту чи їхнє застосування в економному режимі може тимчасово покращити затримки або пропускну здатність, але робить мережу вразливішою до цілеспрямованих маніпуляцій. Тому аналіз типових уразливостей у віртуалізованих мережах повинен враховувати не лише наявні технічні вектори атак, але й системні

компроміси та операційні практики, які трансформують класичні загрози в нові, притаманні саме 5G-середовищу.

2.2 Вразливість в станах фаєрвола

Вразливість в станах фаєрвола (vulnerability on firewall states) виникає на перетині двох архітектурних рішень, притаманних сучасним stateful-фаєрволам: прагнення до високої продуктивності через кешування інформації про активні потоки та прагнення застосовувати контекстні правила фільтрації для підвищення точності політик. У stateful-моделі, яка традиційно розроблялася для протоколів із встановленим з'єднанням, таких як TCP, механізм таблиці станів дозволяє уникати повторної перевірки кожного пакета проти повного набору правил, що істотно зменшує обчислювальні витрати при обробці трафіку. Однак при поширенні цієї ідеї на протоколи без з'єднання фаєрволи породжують так звані «фіктивні» з'єднання: два пакети UDP між тими самими кінцевими точками трактуються як частина одного логічного сеансу і внаслідок цього з'являється запис у таблиці станів з відповідним тайм-аутом. Саме такий механізм і створює передумови для виникнення вразливості, що добре ілюструється прикладом структури state table у FreeBSD (див. рисунок 2.3)

```
root@freebsd:/etc # pfctl -vs state
No ALTQ support in kernel
ALTQ related functions disabled
all tcp 10.51.105.105:22 <- 10.51.104.100:34412       ESTABLISHED:ESTABLISHED
   [23984528 + 2151744512] wscale 6  [592934639 + 3221225728] wscale 7
   age 00:12:25, expires in 24:00:00, 818:759 pkts, 61133:446922 bytes, rule 26
all udp 10.0.2.4:123 -> 151.80.211.8:123       SINGLE:NO_TRAFFIC
   age 00:00:57, expires in 00:00:03, 1:0 pkts, 76:0 bytes, rule 20
all udp 8.8.8.8:53 <- 10.102.11.42:53       SINGLE:MULTIPLE
   age 00:00:02, expires in 00:00:28, 2:1 pkts, 164:76 bytes, anchor 33, rule 1
all udp 10.0.2.4:58680 (10.102.11.42:53) -> 8.8.8.8:53       MULTIPLE:SINGLE
   age 00:00:02, expires in 00:00:28, 2:1 pkts, 164:76 bytes, rule 13
```

Рисунок 2.3 – Таблиця станів в операційній системі FreeBSD

При створенні стану на момент проходження першого пакета подальші пакети зі співпадаючими заголовковими полями пропускаються на підставі стану, а не перевіряються повторно за правилами. Для протоколів без з'єднання

тайм-аути станів регулярно оновлюються при надходженні кожного пакета, що дозволяє зловмиснику утримувати стан нескінченно довго, посилаючи контрольовані пакети у проміжках, менших за тайм-аут. Схематичне представлення експлуатації цієї властивості наведено на рисунку 2.4, де показано, як початковий прохід створює стан, а подальші модифіковані пакети продовжують проходити крізь фаєрвол поза межами логіки правил.

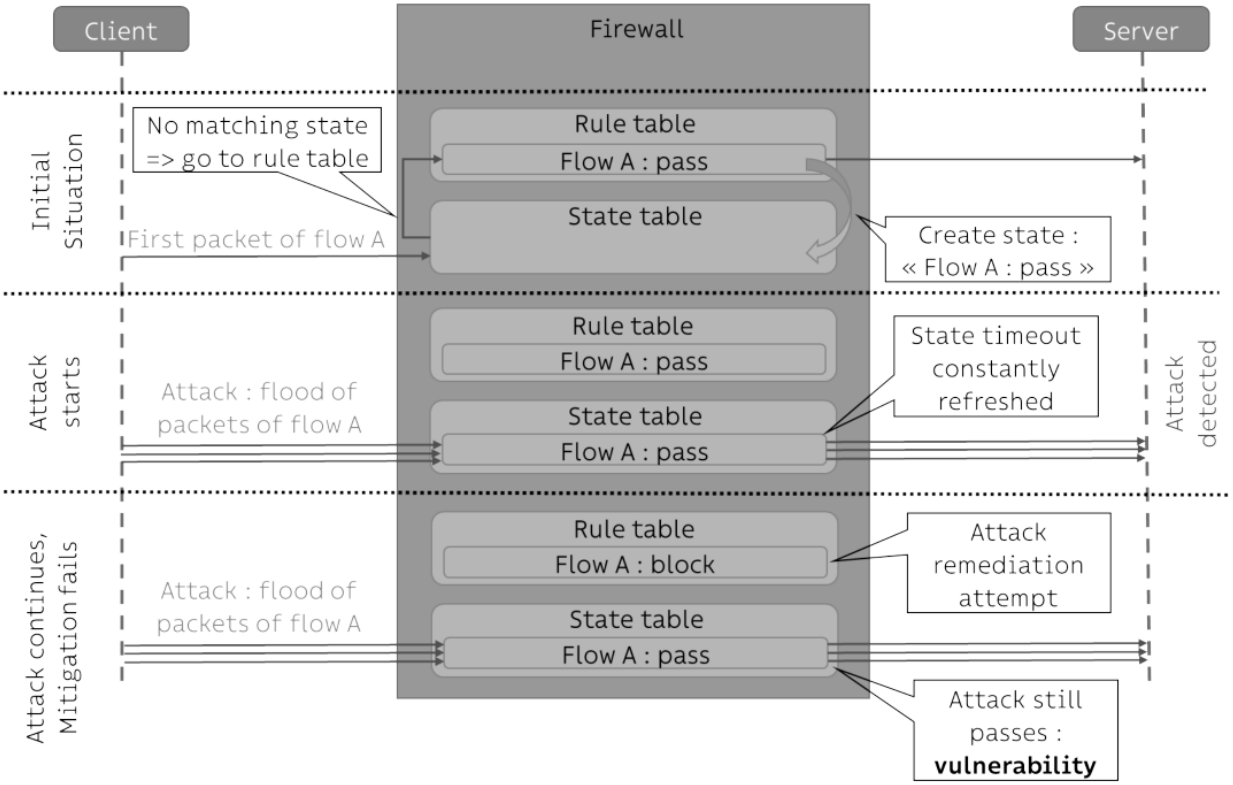


Рисунок 2.4 – Схематичне представлення експлуатації

Експлуатація цієї вразливості може набувати декількох форм. По-перше, атакувальник може сфальсифікувати або підлаштувати заголовок пакетів так, щоб вони відповідали наявному, легітимно створеному стану, і тим самим транспортувати змінений вміст, не проходячи повну логіку перевірки в політиках. У випадку протоколів, у яких частина корисних полів є передбачуваною або стандартизованою (DNS, DHCP, NTP тощо), це дозволяє проводити цілісні модифікації, наприклад підміни резолверів або параметрів конфігурації, без негайного виявлення. По-друге, можливість утримувати обраний стан відкритим шляхом періодичних пакетів робить вразливість

ідеальним інструментом для забезпечення постійного каналу доступу через фаєрвол у межах тривалих атак. На відміну від швидкоплинних DDoS-навантажень, тут атака працює приховано і може слугувати каналом для переміщення або ексфільтрації даних. По-третє, даний тип атак за допомогою стану фаєрвола підсилює клас атак, що націлені саме на ресурси фаєрволу. Створення та підтримка великої кількості станів для вимушеної обробки або контролю своїх відповідей може призвести до деградації продуктивності та навіть до відмови у наданні сервісу, оскільки фаєрвол довше тримає записи про стани, які потрібно обслуговувати. Така здатність застосовувати стан як прикриття для обхідних дій робить традиційні реактивні заходи, що базуються на додаванні drop-правил, малоефективними без одночасного механізму кореляції станів з правилами.

У відповідь на виявлену проблему концептуальне усунення вразливості зводиться до забезпечення коректності відношення між таблицею станів та таблицею правил у будь-який момент часу. Іншими словами, необхідно гарантувати, що жоден активний стан не існує в суперечності до поточного набору політик. Така формалізація є технічною основою ремедіаційної стратегії і вказує на два напрями дій: недопущення утворення станів, які не відповідають політиці, або, якщо такі стани вже існують і політика змінюється, їх селективне видалення без глобального скидання всієї таблиці станів.

Реалістичний сценарій використання цієї логіки потребує гармонізації життєвих циклів станів з процесом управління політиками. При додаванні або оновленні блокуючих правил система повинна мати змогу виявити і видалити ті стани, що суперечать новим обмеженням, але при цьому звести до мінімуму негативний вплив на легітимні з’єднання. Саме поняття селективного видалення state-записів являє собою прагматичну альтернативу повному flush таблиці станів, оскільки глобальне видалення шкодить користувачам і сервісам, які тимчасово залежать від активних станів. Також потрібно враховати потребу у достовірності джерел інформації про те, які стани слід вважати компрометованими: автоматичне видалення має базуватися або на надійних індикаторах аномальної активності конкретних state-записів, або на кореляції з

детекції атак вищого рівня, щоб уникнути фальш-позитивів і непотрібних втрат сервісу.

У науково-практичному сенсі атака за допомогою стану фаєрвола підкреслює фундаментальну дилему між продуктивністю і безпекою. Економія обчислювальних ресурсів через кешування станів створює вузьке місце, яке може бути використано для обходу політик чи для маскування тривалих атак. Вирішення проблеми вимагає як формального переосмислення правил узгодженості між таблицями, так і впровадження механізмів контролю життєвого циклу станів на рівні інфраструктури. Проте будь-яке таке рішення має базуватись на принципі мінімального втручання. Воно повинно забезпечувати селективне відключення лише тих станів, що реально суперечать новим правилам або демонструють корельовану зловмисну поведінку, залишаючи решту станів для збереження звичної якості сервісу.

2.3 Проблематика захисту служби DHCP

Протокол DHCP є базовим механізмом для автоматичного надання параметрів мережевого підключення користувацькому обладнанню (UE) у мобільних системах. Його завдання полягає у динамічному розподілі IP-адрес, шлюзів, DNS-серверів та інших параметрів, необхідних для доступу до мережі оператора. У традиційній архітектурі четвертого покоління (4G), побудованій навколо концепції EPC, усі повідомлення DHCP проходили через захищену площину керування (CP), де забезпечувались криптографічні механізми цілісності та автентифікації. Проте в архітектурі п’ятого покоління (5G Core) із впровадженням NFV та SDN частина процедур була перенесена у площину користувача (UP). Це рішення мало на меті підвищення ефективності, зменшення затримок та розвантаження елементів керування, але водночас створило нову поверхню атаки через те, що в UP захист цілісності є як опція і у більшості випадків вимикається для економії ресурсів.

У результаті DHCP-повідомлення, які містять критично важливу конфігураційну інформацію для пристрою користувача, можуть передаватися

сегментами мережі без жодного криптографічного контролю їхньої незмінності. Типовий процес отримання параметрів адресації у 5G наведено на рисунку 2.5.

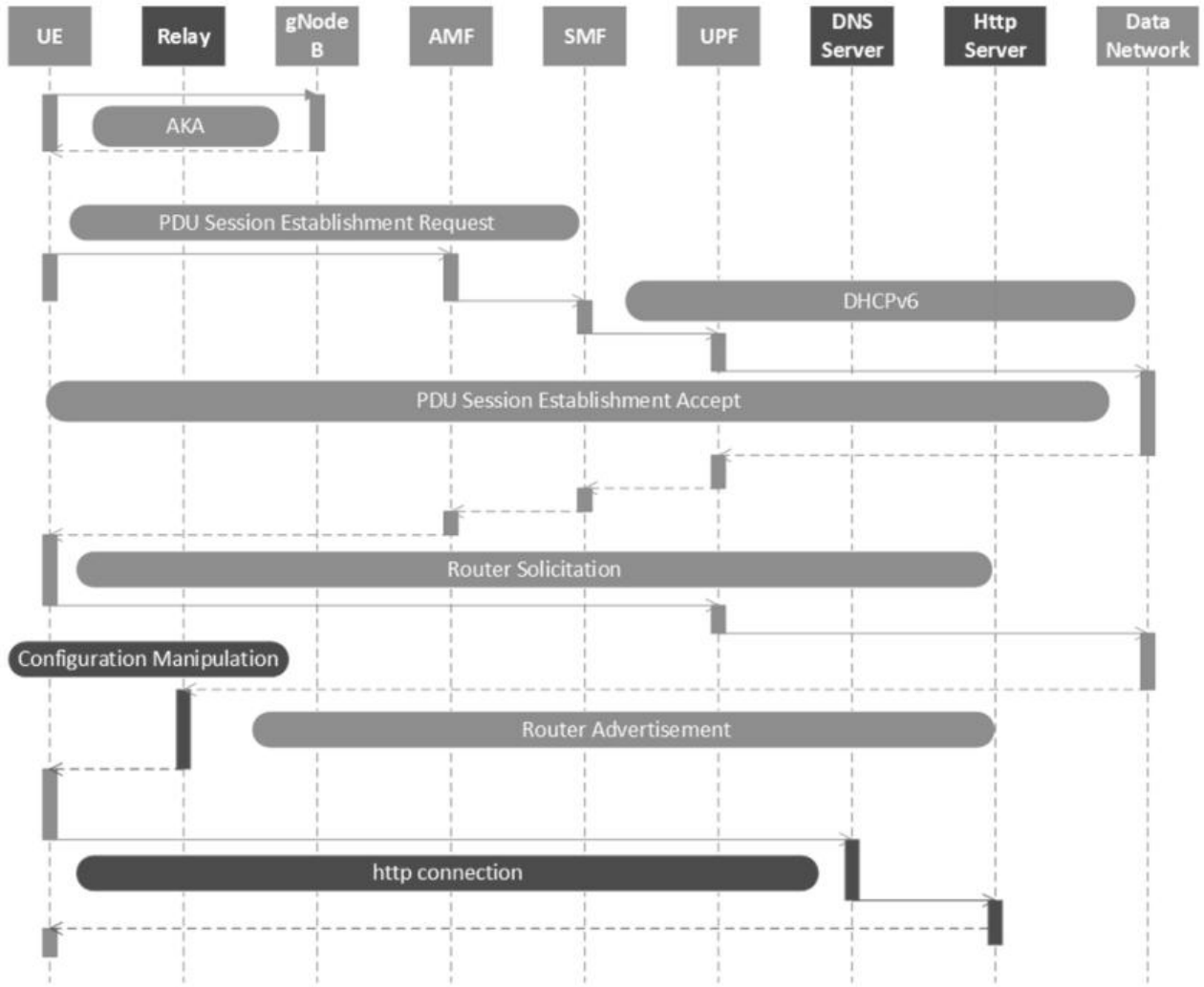


Рисунок 2.5 – Процес отримання параметрів адресації

На схемі показано, що для IPv6 ініціалізація адреси відбувається у два етапи: спочатку Session Management Function (SMF) ініціює запит у площині CP, а фактичне отримання префікса адреси та додаткових параметрів через UP Function (UPF). Оскільки на цьому етапі захист цілісності трафіку часто відключено, DHCP-повідомлення перетинає межу між площинами керування і користувача, що створює умови для потенційного втручання зловмисника.

На рисунку 2.6 показано детальніше взаємодію між SMF, UPF та Data Network (DN), де DHCP-пакети проходять через проміжні маршрутизатори та проксі-вузли.

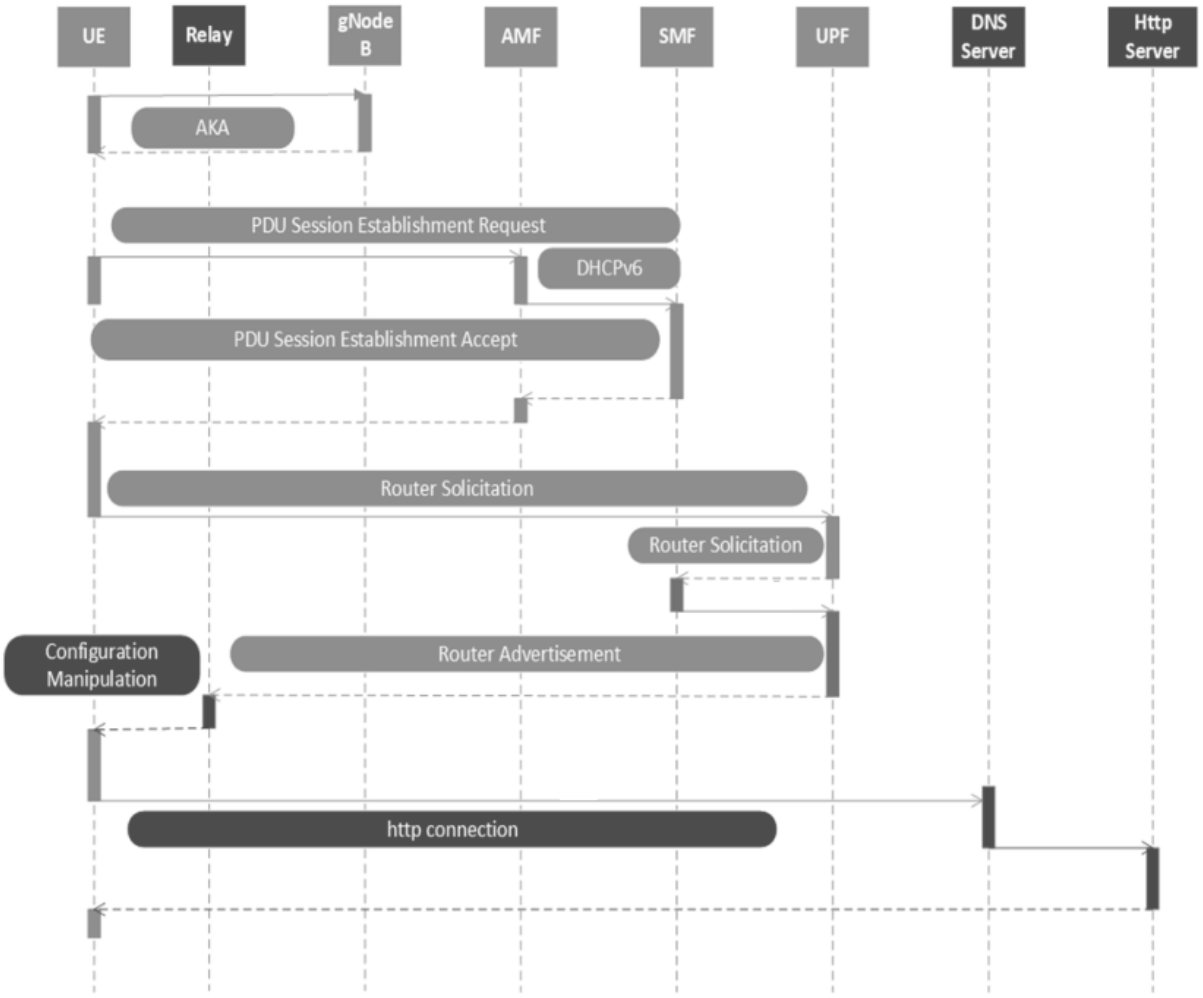


Рисунок 2.6 – Процес взаємодії між SMF, UPF та DN

Ці елементи інфраструктури можуть бути скомпрометовані або недостатньо захищені, і саме тут можлива класична атака типу Man-in-the-Middle [23]. Зловмисник, який має доступ до каналу між SMF і UPF, може перехопити або змінити пакети DHCP Reply перед тим, як вони дійдуть до користувача. Під час такої атаки структура пакета залишається коректною, але його зміст наприклад, IP-адреси DNS-резолверів або шлюзу за замовчуванням модифікується.

Механіка цієї вразливості проілюстрована на рисунку 2.7, де зображено подвійний маршрут передачі DHCP-пакетів.

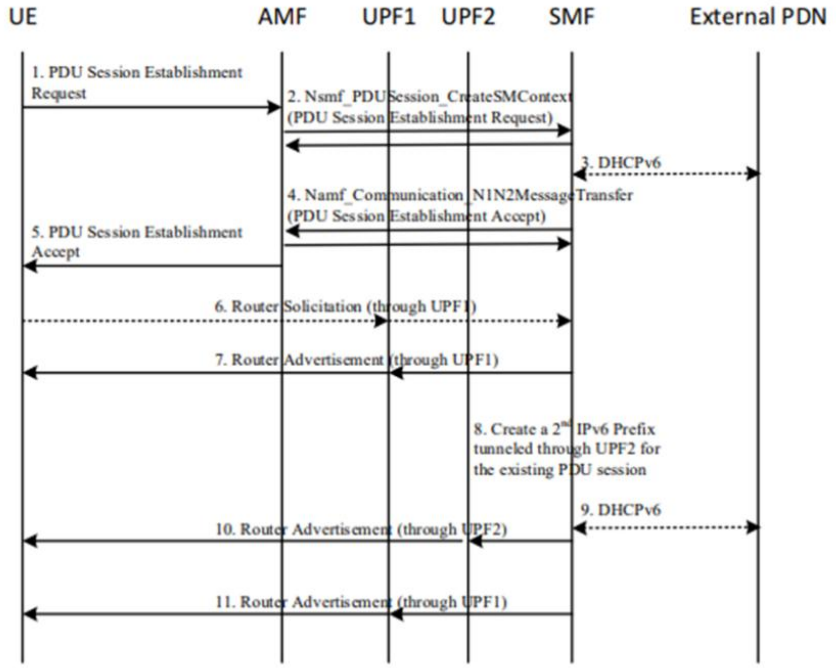


Рисунок 2.7 – Маршрут передачі DHCP-пакетів

Навіть якщо справжній сервер DHCP надсилає коректну відповідь, зловмисник може підмінити її раніше, ніж справжній пакет дійде до SMF. Через відсутність перевірки автентичності DHCP-повідомлень у площині користувача модифікований пакет сприймається як легітимний. На рисунку 2.8 показано спрощену топологію, у якій уразливий елемент UPF виступає посередником між SMF і зовнішньою мережею DN.

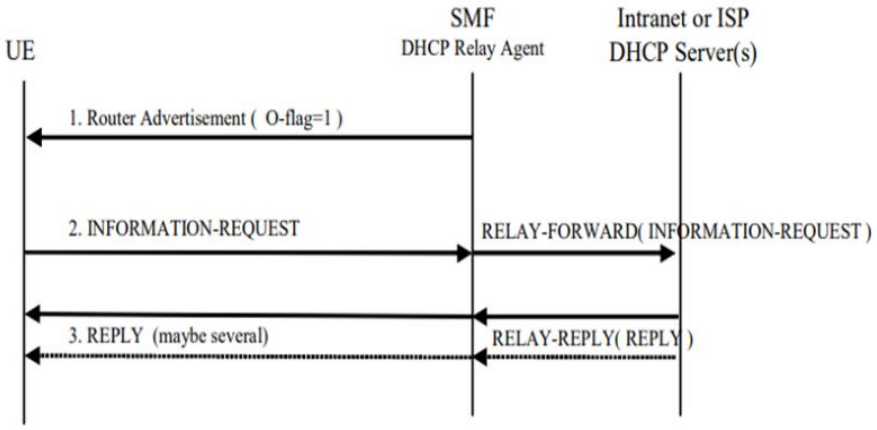


Рисунок 2.8 – Маршрут передачі DHCP-пакетів (продовження)

У такому сценарії будь-яка маніпуляція у проміжному вузлі може залишитися непоміченою, а користувач не має жодних механізмів перевірки достовірності отриманих параметрів.

Проблема посилюється через фрагментацію функціональності між різними компонентами 5G-ядра. Session Management Function (SMF) ініціює DHCP-запит, але не контролює цілісність пакета після виходу у UP. UE у свою чергу, довіряє отриманим даним і не має можливості перевірити, чи дійсно вони походять від авторитетного сервера DHCP. Так формується розрив довіри між площинами керування і користувача, який дозволяє зловмиснику змінити службову інформацію без жодних видимих ознак компрометації.

У класичних провідних або корпоративних мережах ця проблема частково вирішувалась за допомогою DHCP Authentication Option або захищених тунелів IPsec між довіреними вузлами. У мобільних мережах 5G такі рішення виявилися малопридатними через надмірні накладні витрати: використання IPsec підвищує затримку та споживання ресурсів, а реалізація повної аутентифікації DHCP-повідомлень за стандартом RFC 3118 обмежена розміром повідомлень і не підтримує динамічну зміну ключів для великої кількості одночасних сесій. Використання сертифікатів X.509 або криптографії з відкритим ключем також є неефективним через короткочасний характер сесій і високе навантаження на процесор користувача. Унаслідок цього більшість операторів обирають компромісне рішення передавати DHCP-повідомлення без перевірки цілісності, спираючись лише на правильність структури пакета.

Особливу небезпеку становлять так звані relay-агенти. Проміжні вузли, які пересилають DHCP-пакети між різними сегментами мережі. Більшість реалізацій relay-агентів не перевіряють, чи дійсно отримана відповідь походить із дозволеного джерела. Унаслідок цього перше повідомлення, яке відповідає формату DHCP-Reply, приймається як достовірне. Якщо зловмисник розміщений у тому ж віртуальному сегменті, що й UPF або relay-агент, він може надіслати підроблену відповідь швидше, ніж справжній сервер, і тим самим змінити всі параметри конфігурації, які отримує користувач.

Поширеною практикою у сучасних 5G-мережах є вимкнення перевірки цілісності для площини користувача, що частково пояснюється необхідністю зменшити затримки та навантаження на обчислювальні ресурси пристроїв. Проте така оптимізація фактично позбавляє мережу можливості контролювати, чи залишився вміст DHCP-повідомлення незмінним під час передачі. Криптографічний захист активується переважно для каналів CP, тоді як UP часто працює лише у режимі шифрування без перевірки цілісності (ciphering-only mode). У цьому режимі зловмисник може змінювати окремі біти у відомих позиціях пакета, наприклад у полі DNS-сервера або маршрутизатора, не порушуючи загальної структури DHCP-повідомлення. Наслідки таких втручань значно ширші, ніж проста конфігураційна помилка. Підміна DNS-резолвера може спрямувати трафік користувача до фішингового ресурсу, створити умови для атак типу DNS-spoofing або для прихованого тунелювання даних. Аналогічно, змінений шлюз за замовчуванням може перенаправити весь вихідний трафік через вузол зловмисника. Оскільки DHCP-параметри залишаються чинними до завершення сесії, навіть короткочасне втручання на етапі ініціалізації має довготривалий ефект.

У контексті віртуалізованих середовищ ситуація ще складніша. Сервер DHCP може працювати як окрема VNF у Data Network, SMF у контейнері в кластері, а UPF на іншій фізичній платформі. Через це шлях між ними проходить через кілька рівнів віртуалізації, де політики безпеки можуть відрізнятися. Якщо один із цих рівнів не забезпечує контроль цілісності, то весь ланцюг довіри втрачає захищеність.

Вразливість DHCP у 5G також проявляється внаслідок зростання кількості коротких сесій. Кожна зміна підмережі або оновлення контексту викликає нову DHCP-процедуру, збільшуючи кількість можливих точок втручання. У таких умовах навіть одиничний скомпрометований вузол або контейнер може бути використаний для масштабних атак. При інтеграції з сервісами обчислень на краю мережі (MEC) DHCP-трафік може виходити за межі приватного домену оператора, потрапляючи у публічні сегменти, де контроль безпеки менш суворий.

Основною причиною уразливості є не недосконаліть конкретного DHCP-сервера, а відсутність наскрізного захисту між його кінцевими точками. Коли ланцюг довіри між SMF і DHCP-сервером розірвано, навіть мінімальні модифікації у трафіку залишаються непоміченими. Системи IDS не завжди виявляють ці інциденти, оскільки структура пакета не порушується, а зміст виглядає правдоподібним. Проблематика захисту DHCP у 4G/5G показує, що під час переходу до більш масштабованих і динамічних архітектур компроміс між продуктивністю і безпекою часто вирішується на користь першої. Оптимізація шляхом відключення Integrity Protection підвищує швидкодію, але залишає критичні службові протоколи без захисту. Це створює передумови для нових класів атак, у яких зловмиснику достатньо експлуатувати передбачуваність структури DHCP-повідомлень, не вдаючись до складного злому шифрування.

2.4 Контрзаходи проти атак

З огляду на описані загрози, ефективна протидія повинна поєднувати три логічно взаємопов’язані шари заходів: підходи, що гарантують цілісність та автентичність службових повідомлень на рівні протоколів; механізми, які знижують імовірність успішної підміни або підробки маршруту доставки; а також оперативні засоби, що дозволяють миттєво ліквідувати наслідки виявлених атак без завдання непропорційної шкоди легітимним сеансам. На архітектурному рівні це співпадає з ідеями Zero Trust моделі, що апелює до постійного підтвердження довіри до кожного елементу комунікації (див. рисунок 2.9)[24].

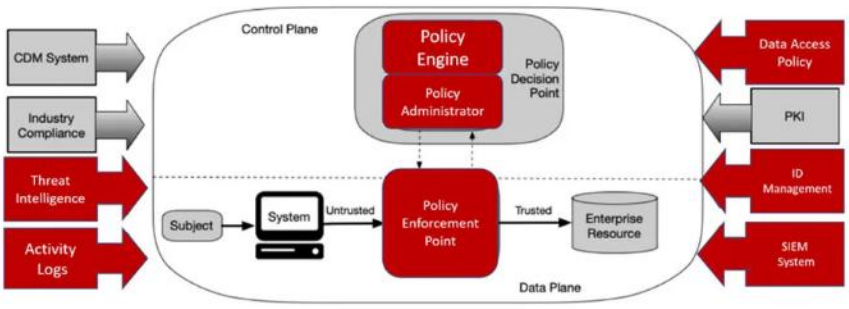


Рисунок 2.9 – Zero Trust модель

Ідея полягає в тому, що замість єдиної глобальної довіри до внутрішніх каналів слідує вимога локальних доказів автентичності та цілісності для критичних обмінів, таких як передача DHCP-параметрів або прийняття рішень на рівні політик фаєрвола.

На рівні протоколу робоча пропозиція містить дві взаємодоповнювальні прикладки. Перша - «контентна» техніка, що не вимагає кардинальних змін формату повідомлень і полягає в упаковці корисних параметрів у опції DHCP разом із двома випадковими блоками та псевдовипадковим перемішуванням порядку блоків (block + shuffle). Така маніпуляція не змінює семантику протоколу, але ускладнює точкову модифікацію полів з боку MitM-перехоплювача, бо положення важливих фрагментів перестає бути сталим між різними транзакціями. Технічно рішення використовує наявні опційні поля (vendor options) і задовільняє обмеження довжини, при цьому UE читає опції, ігноруючи довільні вставки, а зловмисникові стає вкрай важко спрогнозувати позицію потрібного поля. Друга група заходів - це криптографічні що спираються на дві моделі: симетричну Message Authentication Code (MAC) та асиметричну (підпис хешу повідомлення). Для захисту ланцюга між сервером DHCP і SMF пропонується або використовувати MAC із попередньо поділеним ключем між довіреними елементами мережі, або підписувати хеш приватним ключем сервера при наявності інфраструктури відкритих ключів. Ключова перевага другого підходу у тому, що він дозволяє SMF і UE верифікувати джерело та незмінність отриманих конфігураційних блоків, не вимагаючи при цьому повного вмикання integrity для всього UP.

Захист потоку даних між SMF та UE вимагає іншого механізму. Напириклад, коли довірений елемент ядра підписує або генерує MAC від вибраних полів DHCP/RA і передає цей маркер у Router Advertisement; UE, маючи відповідний публічний ключ або спільний секрет у SIM-карті, перевіряє підпис або MAC і приймає конфігурацію лише у випадку успішної перевірки. Такий підхід використовує наявні можливості 5G щодо зберігання ключів у SIM і не вимагає відключення або радикальної модифікації існуючих протоколів

передачі даних. Він переводить проблему з «невідомої» на «перевірену»: тепер помилка в доставці або модифікація вмісту матиме формальний криптографічний індикатор, який UE здатен розпізнати.

Окрім контентних та криптографічних інструментів, важливим елементом є інтеграція з системою раннього виявлення та автоматизованої відповіді. Інтеграція IDS-типу сенсорів із системою правил дозволяє виявити підозрілу поведінку (наприклад, аномальні патерни DNS-відповідей) і в автоматичному режимі ініціювати селективні ремедіаційні дії в брандмауері, включаючи таргетоване видалення state-записів замість глобального flush. Це поєднання підвищує оперативність реакції і зберігає доступність для легітимних користувачів, бо накладає мінімальний collateral damage.

2.5 Висновки до розділу 2

В другому розділі було показано, як віртуалізація мережевих функцій і програмно визначені мережі у складі 5G Core змінюють профіль ризиків і ускладнюють традиційну модель загроз. Показано, що класичні цілі безпеки доступність, цілісність і конфіденційність у віртуалізованому середовищі взаємопідсилюються та відкривають нові траєкторії атаки, а операційні компроміси між продуктивністю та контролем безпеки створюють «вікна можливостей» для зловмисника. На тлі цього контексту було деталізовано специфіку атак на доступність через протоколи без стану з’єднання та черги оброблення, на цілісність - через можливість точкової модифікації службових полів без порушення структури пакетів, і на конфіденційність - через використання дозволених служб як каналів фільтрації. Окремо висвітлено вразливість у станах брандмауера як наслідок розсинхронізації між таблицею правил і таблицею станів у stateful-фільтрації для протоколів без стану з’єднання. Показано, що підтримувані стани дозволяють пакетам оминути нові правила заборони, що підсилює як приховані довготривалі атаки, так і швидкі сценарії атак та робить реактивне додавання drop-правил недостатнім без узгодженого керування життєвим циклом станів. Така уразливість демонструє

фундаментальну дилему продуктивність/безпека і вимагає підходів, здатних забезпечити селективне усунення без глобального впливу на легітимні сесії.

У проблематиці DHCP для 5G підкреслено, що зміщення частини процедури адресації й конфігурації до площини користувача за відсутності обов'язкової перевірки цілісності породжує структурний розрив довіри між контрольним і користувацьким сегментами. Саме на перетині SMF, UPF і DN виникають ключові точки втручання для підміни критичних параметрів, зокрема DNS і шлюзу, з довготривалими наслідками для маршрутизації трафіку користувача. Віртуалізаційна багатошаровість, робота relay-агентів і часті короткі сесії в 5G додатково збільшують частоту й площу таких вікон атаки.

Запропоновані контрзаходи вибудувано навколо трьох механізмів: протокольні механізми забезпечення цілісності й автентичності службових повідомлень, зниження передбачуваності вмісту там, де повна криптографічна перевірка недоцільна, та оперативна, селективна реакція на рівні брандмауера. Модель Zero Trust підсилює цей дизайн, переводячи довіру з «глобальної» у «локальну», коли кожен критичний обмін підтверджується окремо. Контентна рандомізація службових полів зменшує шанси на успішну точкову підміну без змін стандартів, а криптографічні маркери (MAC або підпис) на ключових ділянках ланцюга постачання конфігурації створюють верифікований слід походження.

Узагальнюючи, розділ доводить, що ефективна безпека 5G Core у віртуалізованому виконанні неможлива без синхронізації політик, станів і протокольних гарантій, а також без готовності приймати інженерні компроміси, які віддають пріоритет відтворюваності захисту, а не лише піковій продуктивності. Найкращі результати досягаються комбінацією локальних криптографічних перевірок, зменшенням передбачуваності службових полів там, де це допустимо стандартами, та автоматизованим усуненням на межі фільтрації трафіку. Це формує практичний каркас для подальшої системної реалізації рішень та їхнього масштабування у виробничих мережах.

РОЗДІЛ 3 АВТОНОМНА ТА АДАПТИВНА АРХІТЕКТУРА БЕЗПЕКИ ДЛЯ 5G CORE

3.1 Сучасні підходи до безпеки в 5G

П’яте покоління мобільного зв’язку поєднало мережеву віртуалізацію, програмно-визначені функції та сервісно-орієнтовану архітектуру, відкривши шлях до радикально вищої ефективності керування ресурсами. Водночас така гнучкість обертається новою поверхнею атаки: у 5G слабкі місця рідко зосереджені в одному апаратному вузлі, натомість вони народжуються на стиках шарів і доменів - між ядром NFV-інфраструктури, площинами керування та даних, між оркестраторами й мережевими функціями, між політиками безпеки. У цій екосистемі класичні загрози набувають нових масштабів завдяки мультиорендності, динамічному ланцюжку довіри та широкому застосуванню контейнеризованих функцій. Саме тому сучасні підходи до безпеки 5G дедалі частіше ґрунтуються не лише на периметрі й сигнатурах, а на оркестрації захисних дій, конфлікт-менеджменті політик і принципах автономного керування в замкнених контурах.

Базовою передумовою для інтеграції безпеки у 5G є перехід від статичних конфігурацій до моделі, де політики виступають першокласними артефактами керування послугами. У яких безпека охоплює життєвий цикл сервісів від моніторингу і виявлення до реакції та відновлення. Політики описуються на різних рівнях абстракції, що дозволяє відділити намір від реалізації. Відповідно запроваджено два рівні: HSPL для декларативного формулювання вимог недоменною мовою, зрозумілою не технічним користувачам, і MSPL для уніфікованого, незалежного від конкретного пристрою опису конфігураційних дій. Перехід між ними забезпечує інтерпретатор політик; така стратифікація зменшує число помилок і полегшує масштабоване застосування політик у гетерогенних середовищах, що особливо важливо для slicing-архітектури, де кожен сегмент має ізолюватися та еволюціонувати незалежно.

На практиці, однак, складність не обмежується трансляцією намірів у дії. Політики створюють, змінюють і поширюють різні суб'єкти: оператор мережі, доменні адміністратори, постачальники сервісів, а в умовах приватних або гібридних мереж ще й клієнти, які володіють власними сегментами. Це породжує проблему конфліктів політик, логічних суперечностей між правилами різного походження або пріоритету. Література демонструє спектр підходів до їх виявлення та пом'якшення: від формальних мов специфікацій і офлайнових верифікаторів до онлайнових рушіїв, вбудованих у контури оркестрації. Наприклад, розширення FortNOX для SDN-контролера NOX запровадило механізм пріоритизації правил, що блокує встановлення flow-правил з нижчим рівнем довіри, якщо вони суперечать правилам з вищими повноваженнями. Водночас подальші аналізи показали, що крос-шарові суперечності й сценарії з кількома контролерами залишаються викликом, оскільки конфлікт може виникати не лише в межах одного домену політик, а й між доменами керування, сервісів і мережевих функцій.

Паралельно еволюціонує ідея Zero Trust як організаційного стандарту. У термінах NIST ZTA контур прийняття рішень (PDP) відокремлюється від точки застосування (PEP), а рішення уніфікуються політичним рушієм, який корелює результати аналітики, телеметрії та декларативних вимог. В межах 5G це зручно накладається на сервісно-орієнтовані оркестратори та менеджери життєвого циклу VNFs/CNFs. Концептуально така побудова відповідає зображенню багатошарового керування безпекою, де на кожному рівні діє власний оркестратор з автономним замкненим контуром, а між рівнями реалізовано кероване поширення рішень і політик (див. Додаток Б).

Стандартизаційна основа для таких рішень формується двома ключовими рамками ETSI. По-перше, NFV/MANO унормовує життєвий цикл мережевих функцій і сервісів, роблячи безпекові механізми частиною опису сервісів та їхніх вимог до інфраструктури. По-друге, Zero-touch network and service management (ZSM) пропонує референтну модель «нульового дотику», де доменні менеджери обмінюються телеметрією, а автоматизація спирається на аналітику, політики та замкнені контури. У контексті безпеки поєднання MANO і ZSM дозволяє

розміщувати детектори, корелятори, брокери подій і PEP у тих сегментах, де вони найефективніші, а також будувати канали довіри та передачі рішень між рівнями, зберігаючи сегментацію сигментів.

Окремою лінією розвиваються методи динамічної оборони, насамперед Moving Target Defense. Їхня логіка проста. Замість статичного укріплення одного периметра система постійно змінює конфігурації, маршрути, порти, ідентифікатори або розміщення ресурсів, ускладнюючи розвідку та експлуатацію вразливостей. MTD систематизуються за об’єктом зміни, способом та ритмом трансформацій, доменом застосування і вартісними характеристиками. Консенсус полягає в тому, що не існує «універсального» MTD. Ефективність тактики залежить від профілю атак і сервісного контексту, а отже вибір має бути ситуаційно обумовленим. Саме тут на перший план виходить питання керування вартостями та ризиком. MTD можуть бути енерго- та часовитратними, а надмірна частота змін здатна знизити продуктивність. Таким чином, потрібні підходи, що співвідносять очікуваний виграш у зменшенні ймовірності успішного вторгнення з експлуатаційною ціною контрзаходів, не входячи у специфіку конкретних механізмів, яка розглядатиметься далі.

Водночас 5G вводить slicing як механізм логічної ізоляції сервісів і клієнтів. Ізоляція сигментів потребує не лише технічних бар’єрів, а й керованого простору політик. За замовчуванням оператор формулює загальносистемні політики для досягнення своїх цілей. Для ізоляції, відповідності регуляціям, продуктивності. Однак клієнти сигментів часто мають додаткові вимоги, які не покриваються політиками за замовчуванням. Сучасні підходи поступово рухаються до моделі, де клієнт отримує контрольовану можливість вносити власні політики у межах свого сегменту без порушення обмежень оператора. Це неминуче ставить питання пріоритетів, перевірки сумісності та автоматизованого вирішення конфліктів. У дослідженнях, присвячених керуванню конфліктами, простежується розмаїття трактувань самого поняття «конфлікт»: від прямого заперечення дії «дозволити/заборонити» до колізій за умовами застосування, часових залежностей, перетину адресних просторів і транзитивних ефектів у

міждоменно узгоджених політиках. Відповідно, й алгоритмічні засоби виявлення коливаються між перевіркою обмежень на графах, символічним виконанням, логічним виведенням та потоковою кореляцією подій у реальному часі.

Ще одна провідна тенденція це перенесення акценту з реактивної на проактивну оборону за рахунок аналітики імовірнісних сценаріїв порушень. У підходах, де моделі нападу/захисту розглядаються як взаємодія гравців, корисність кроків атакувальника і витрати захисника формалізуються так, щоб допомогти обрати стратегію мінімізації ризику. Такі підходи цінні як рамки для прийняття рішень. Вони дозволяють системно пов’язати витрати на захист, очікувані втрати від простоїв чи компрометацій і ефективність контрзаходів. Однак практичний ефект залежить від якості вихідних оцінок. Імовірностей атак і часткової ефективності захистів, що, у свою чергу, вимагає постійного підживлення реальними спостереженнями, а не разовими експертними гіпотезами. З огляду на це сучасні підходи потребують замкнених контурів, де аналітика подій і ефективності автоматично уточнює політики і пріоритети, зберігаючи сегментацію та узгодженість між доменами.

Повертаючись до системного виміру безпеки 5G, доцільно розмежувати три рівні зрілості підходів. На першому рівні домінують класичні засоби, такі як міжмережеві екрани, IDS/IPS, списки контролю доступу, які інтегровані в контейнери й віртуальні мережеві функції, з орієнтацією на сигнатурне та евристичне виявлення. На другому рівні з’являється політико-керована автоматизація: правила описуються як наміри, узгоджуються між доменами, транслюються в конфігурації, а їх сумісність перевіряється конфлікт-менеджерами ще до розгортання. На третьому рівні вибір і ритм застосування захисних тактик залежить від ризику, що оцінюється за поточним профілем подій, і від оціненої ефективності наявних засобів. Саме цей перехід від статичної конвеєрної безпеки до політико-ймовірнісної, замкненої на аналітику позначає траєкторію новітніх рішень у 5G і пояснює, чому у принципах з еталонними архітектурами безпеки, що узгоджуються з ZSM/MANO, особливе місце відведено контурам моніторинг-аналіз-рішення-застосування та абстракціям HSPL/MSPL як мостам між наміром та виконанням.

Нарешті, у політико-керованому світі slicing постає не тільки як технологічний механізм, а як контракт довіри між оператором і власником сигметну. Сучасні підходи до безпеки прагнуть зробити цей контракт формальним можливістю автоматичної перевірки, забезпечивши, з одного боку, свободу клієнта встановлювати політики у межах свого домену, а з іншого гарантії для оператора, що жодна локальна зміна не порушить глобальних правил безпеки та ізоляції. У цьому сенсі конфлікт-менеджери політик і багаторівневі інтерпретатори не допоміжні модулі, а центральні компоненти архітектур, які дозволяють 5G-мережам залишатися гнучкими без втрати керованості.

3.2 Проєктування автономної архітектури з поширенням політик безпеки

Розвиток 5G-мереж супроводжується не лише еволюцією технологій передачі даних, а й зростанням складності системного управління безпекою. Мережеві функції, які раніше були апаратними і ізольованими, тепер реалізуються як програмні компоненти. Віртуальні (VNF) або контейнеризовані (CNF) і керуються через механізми оркестрації в межах розподілених доменів. У таких середовищах класичні підходи до безпеки, що базуються на централізованому адмініструванні, вже не гарантують оперативності реагування й не забезпечують узгодженості політик між рівнями управління. Тому сучасна концепція автономної архітектури безпеки передбачає поєднання модульності, ієрархічного керування та здатності до самостійного поширення і узгодження політик без залучення адміністратора.

В основі проєктованої системи лежить принцип замкненого контуру управління (closed loop), який є центральним елементом стандарту ETSI ZSM. У межах цього контуру всі операції від моніторингу трафіку до прийняття та застосування рішень виконуються автоматично за допомогою взаємодіючих сервісів. Такий підхід дозволяє досягти zero-touch управління. Тобто автономності реагування без ручного втручання. Система аналізує стан мережі, визначає появу аномалій, перевіряє сумісність змін політик, приймає рішення про захисні дії та негайно поширює їх на відповідні компоненти. Саме така

послідовність, інтегрована в 5G-середовище, відображена в Додатку Б, де наведено багаторівневу ієрархію взаємодії доменних і локальних оркестраторів безпеки.

Проєктована архітектура має дворівневу структуру, що може масштабуватися до кількох рівнів залежно від складності мережі. На верхньому рівні розташовується DSO, який забезпечує управління міжсигментовими (inter-slice) політиками, ізоляцію трафіку та узгодження дій між різними сервісними доменами. Нижчий рівень представлений LSO, що відповідає за безпеку всередині конкретного сигменту (slice) або підмережі. DSO та LSO взаємодіють у вертикальному напрямку, утворюючи каскад керування, у якому рішення, прийняті на рівні домену, поширюються до локальних оркестраторів, а зворотній зв’язок у вигляді подій або аналітичних звітів надходить угору. Завдяки такій архітектурі система зберігає гнучкість і масштабованість, адже кожен рівень може реалізовувати власні контури моніторингу та реагування.

Усі компоненти архітектури функціонують на базі двох стандартних політик ETSI: NFV MANO та ZSM. MANO забезпечує життєвий цикл віртуальних або контейнеризованих функцій безпеки, зокрема їх розгортання, масштабування та видалення. ZSM використовується для створення сервісно-орієнтованих потоків управління між оркестраторами, надаючи можливість координації дій різних функціональних блоків через стандартизовані API. Це дозволяє об’єднати моніторинг, аналіз, прийняття рішень і застосування політик у єдину автономну екосистему, де інформаційні потоки циркулюють без людського втручання.

Ключовим елементом у цій ієрархії є Security Orchestrator, що реалізує повний цикл спостереження → аналіз → рішення → застосування. У структурі SO функціонують кілька логічних модулів, кожен з яких відповідає за певну фазу циклу. Моніторинговий модуль (ME) виконує збір телеметрії та потоку даних із користувацької площини, агрегує їх і передає у аналітичний модуль (AE). Аналізатор використовує правила або моделі машинного навчання для виявлення відхилень, які можуть свідчити про атаку чи порушення політик. Коли аномалія підтверджується, формується тригер для PDP, який виступає ядром

механізму прийняття рішень. PDP складається з трьох компонентів, узгоджених із принципами Zero Trust Architecture: PE, що обирає рішення на основі поточних даних; PA, який транслює це рішення у конкретні дії; та PEP, що безпосередньо реалізує політику у мережевих вузлах. Такий поділ відповідальності дозволяє відокремити інтелектуальну логіку аналізу від виконання, запобігаючи несанкціонованим змінам у системі.

Важливим завданням при проєктуванні є створення механізму поширення політик, здатного об’єднати політики адміністратора мережі та користувачів окремих сегментів без порушення ізоляції. У типовій мережі 5G оператор установлює базові політики безпеки, які гарантують дотримання нормативних вимог, контроль доступу та сегментацію трафіку. Проте клієнти, що орендують окремі сегменти, можуть мати специфічні потреби. Наприклад, власні правила міжмережевого екранування чи обмеження доступу до сервісів. Тому архітектура повинна дозволяти клієнтові додавати свої політики, але водночас не порушувати вже діючих правил оператора. Для цього було розроблено PCD, який перевіряє будь-які нові політики перед їхнім впровадженням у мережу.

Концепція PCD базується на розширенні у напрямку підтримки клієнтських ініціатив. Коли користувач надсилає власну політику до системи, вона проходить двоетапну перевірку. Спершу аналізується на рівні домену, де зіставляється з політиками оператора, а потім на рівні сегменту, де перевіряється на сумісність із уже наявними політиками самого клієнта. Якщо виявлено суперечність, наприклад, спробу дозволити трафік, який оператор заборонив, PCD формує звіт і відхиляє зміну, залишаючи поточний стан безпеки незмінним. Такий підхід знімає навантаження з адміністратора, який у традиційних системах мав вручну перевіряти кожен запит користувача, і мінімізує ризик виникнення конфліктів у режимі реального часу.

Щоб забезпечити єдиний формат опису політик, система використовує двоступеневу модель HSPL/MSPL. Користувацькі політики задаються у вигляді декларативних висловлювань високого рівня, після чого Policy Interpreter автоматично транслює їх у середній рівень MSPL, придатний для безпосереднього виконання у SO. Усі перевірені й підтверджені політики

зберігаються у двох репозиторіях: Domain Repository, що містить політики адміністратора, та Local Repository, де зберігаються політики клієнта. Поділ репозиторіїв є принциповим, адже дозволяє ізолювати доменні правила від користувацьких і спростити перевірку конфліктів.

Взаємодія між DSO і LSO забезпечує каскадне поширення рішень. Коли локальний оркестратор отримує нову політику від клієнта, він спершу надсилає запит до доменного оркестратора для валідації на рівні адміністратора. Якщо конфлікту не виявлено, політика проходить локальну перевірку сумісності й після цього застосовується у відповідному сегменті. У разі, якщо клієнт володіє кількома сегментами, DSO може поширити цю політику на всі його підмережі, але кожен LSO має право відмовити у прийнятті змін, якщо вони несумісні з контекстом конкретного сегменту. Така логіка гарантує дотримання принципу slice isolation і водночас забезпечує гнучкість, дозволяючи швидко адаптувати політики без централізованого втручання.

В архітектурі всі елементи SO, включно з PCD, PE, PA, PEP, ME та AE, можуть бути реалізовані як окремі віртуальні або контейнеризовані функції. Це означає, що вони підтримують життєвий цикл, визначений MANO, і можуть масштабуватися, мігрувати або оновлюватися незалежно. Таке мікросервісне розділення не лише підвищує стійкість системи, а й дозволяє розгортати її частинами у різних фізичних або віртуальних доменах, наприклад у приватному дата-центрі оператора та в edge-інфраструктурі клієнта.

Автономність запропонованої архітектури проявляється у здатності самостійно ініціювати дії на основі аналітичних подій. Якщо AE фіксує відхилення у поведінці трафіку, PDP активує відповідну політику, що може передбачати, наприклад, блокування певного типу запитів або перезапуск функцій безпеки. Рішення про реакцію не потребує участі оператора. Усі дії виконуються через PEP автоматично, а результати записуються у лог системи для подальшого аналізу. Цей процес формує замкнену петлю зворотного зв’язку, яка постійно оновлює дані в репозиторіях політик і коригує майбутні дії. Завдяки такій побудові архітектура підтримує самонавчання, накопичуючи історію інцидентів і реакцій, вона може вдосконалювати стратегію управління безпекою.

Важливим аспектом проєктування стало також урахування часових вимог до поширення політик. Концептуально запропонована архітектура створює середовище, у якому безпека стає інтегрованою частиною сервісного життєвого циклу, а не зовнішнім додатком. Політики безпеки описуються як сервіси, оркестровані тими самими засобами, що й функціональні компоненти 5G Core. У результаті отримується система, здатна одночасно забезпечувати централізовану узгодженість дій і локальну автономію клієнтів. Вона поєднує стратегічний контроль на рівні домену з тактичним реагуванням у сегментах, а її архітектурна побудова забезпечує узгодженість політик навіть за високої динаміки мережевого середовища.

Таким чином, проєктування автономної архітектури з поширенням політик безпеки у 5G Core спирається на стандартизовані принципи MANO та ZSM, використовує ієрархію доменних і локальних оркестраторів, розмежовує рівні відповідальності та вводить механізми автоматизованої перевірки політик на конфлікти. Вона формує основу для подальшої реалізації повністю самокерованої системи безпеки, здатної підтримувати політико-керований захист у режимі реального часу.

3.3 Реалізація та оцінювання системи

Розроблена автономна архітектура безпеки була реалізована у вигляді повнофункціонального експериментального стенду, який відтворює ключові елементи середовища 5G Core. Основна мета цього етапу полягала у перевірці працездатності запропонованого механізму поширення політик та оцінюванні його часових характеристик під час реальних сценаріїв кіберзагроз. Особливу увагу було приділено вимірюванню швидкості реакції системи на атаки та часу, необхідного для розповсюдження нових правил безпеки, ініційованих користувачем. На відміну від попередніх рішень, що залишали автономність на концептуальному рівні, ця реалізація доводить можливість практичного втілення моделі повністю автоматизованого управління безпекою в контексті 5G, що функціонує без ручного втручання адміністратора.

У додатку В подано схему побудованого прототипу, який відображає логічну організацію компонентів системи та їх взаємодію у процесі реагування на атаку. Архітектура реалізована з використанням сучасних контейнерних технологій. Усі основні елементи: моніторинг, аналітика, модулі політик та оркестратори розгорнуті як CNF у кластері Kubernetes [25]. Таке рішення забезпечило гнучкість масштабування, автономне керування життєвим циклом компонентів та високий рівень ізоляції між сервісами. Використання Kubernetes також дозволило інтегрувати механізми розподілу навантаження, автоматичного перезапуску та безперервного моніторингу стану кожної функції без потреби у додатковій інфраструктурі.

Для моделювання ядра мобільної мережі використано відкриту реалізацію Open5GS, яка підтримує повну архітектуру 5G Core відповідно до специфікацій 3GPP та забезпечує чітке розділення Control Plane і User Plane [26]. Це рішення відзначається стабільністю, активною спільнотою розробників та широкою сумісністю з емуляторами радіодоступу, що робить його оптимальним вибором для побудови тестового середовища автономної архітектури безпеки. Система безпеки інтегрувалася безпосередньо у ядро, тобто в область, де здійснюється обробка трафіку, що проходить між абонентським обладнанням та мережею передачі даних. Для емуляції трафіку застосовувалися програмні генератори UE та RAN, які відтворюють поведінку користувацьких терміналів та базових станцій [27]. Це дало можливість відтворити типовий сценарій атаки без підключення реального обладнання [28].

Тестове середовище було розгорнуто на сучасній апаратній платформі, оснащеній процесором Intel Xeon Silver 4314 із 16 фізичними ядрами та тактовою частотою 3,0 ГГц, а також 64 ГБ оперативної пам’яті DDR4. Обчислювальні ресурси були розподілені між чотирма віртуальними машинами, конфігурації яких наведено у таблиці 3.1. Віртуальні машини створено з використанням гіпервізора KVM в Oracle Linux.

Таблиця 3.1 – Конфігурація віртуальних машин

Роль віртуальної машини	**Кількість віртуальних процесорів (vCPU)**	**Обсяг оперативної пам'яті (RAM) GB**	**Операційна система (OS)**
Контрольна площина Kubernetes (Control Plane Node (Open5GS))	8	16	Ubuntu 22.04 LTS
Емулятор користувацького обладнання та радіомережі UERANSIM (UE + RAN Node (gNB))	4	8	Ubuntu 22.04 LTS
Площина користувацьких даних ядра мережі (User Plane Node (UPF))	8	16	Ubuntu 22.04 LTS
Модуль міжмережевого екрану та контролю трафіку (Firewall Node)	4	4	FreeBSD 14.0 Release

Вузол контрольної площини Kubernetes отримав вісім віртуальних процесорів (vCPU) та 16 ГБ оперативної пам'яті, підсистема емуляції користувацького обладнання та радіомережі (UE + RAN) - чотири ядра та 8 ГБ, вузол користувацької площини ядра мережі - вісім ядер і 16 ГБ, а модуль міжмережевого екрану та контролю трафіку - чотири ядра та 4 ГБ оперативної пам'яті під керуванням FreeBSD 14.0 Release. Такий розподіл ресурсів забезпечив баланс між обчислювальною потужністю та ефективністю використання пам'яті, що дозволило реалістично відтворити інфраструктуру 5G Core із сегментованими обчислювальними профілями для кожної функціональної підсистеми.

Після розгортання архітектури було реалізовано два основні експерименти: перший для оцінювання автономного реагування системи на атаку, другий для вимірювання ефективності процесу поширення політик безпеки, які ініціює користувач. Для першого сценарію було обрано атаку типу aLTEr, схему якої подано в розділі 2.1. Атака aLTEr - це активний тип MITM-атаки проти мобільної мережі LTE, яка ґрунтується на слабкості в обробці трафіку користувацької площини (user plane). Центральною передумовою її здійснення є те, що хоча LTE забезпечує шифрування даних, вона використовує режим AES-CTR (Counter mode) без обов'язкового захисту цілісності (integrity) даних в user plane. Внаслідок цього шифротекст може бути змінений таким чином, щоб після

дешифрування одержати керований атакою відкритий текст. Зловмисник, який має можливість перехоплювати канал між користувацьким обладнанням (UE) і мережею, може таким чином змінити, наприклад, IP-адресу DNS-резолвера, і скерувати трафік жертви на контрольований сервер. Процес атаки можна описати так: атакуючий розгортає обладнання, яке імітує базову станцію (eNodeB) мережі LTE або діє як ретранслятор між UE і справжньою мережею, таким чином створюючи видимість нормального з'єднання, але контролюючи чи модифікуючи трафік. UE думає, що підключено до легітимної мережі, а сам атакуючий прикидається користувачем для справжньої мережі. Далі, коли через цю ланку проходять DNS-запити або інші служби, які очікують визначеного формату і результату, атакуючий змінює заголовки чи поля, керуючи шляхом трафіку.

Зловмисник при використанні DNS-запиту може модифікувати IP-адресу DNS-сервера у відповідь, перенаправивши UE на зловмисний резолвер, а згодом на фішинговий сайт. При цьому структура пакета і сам шифрування зберігаються, тому стандартні засоби виявлення часто не фіксують зміну. Оскільки захист integrity не використовується, модифікація не виявляється зміною MAC чи перевірочним кодом. У контексті переходу до 5G атака aLTEr набуває ще більшої значущості. В специфікації 5G захист цілісності User Plane первинно зроблено як опція, тобто оператор може його не активувати заради продуктивності. Це означає, що умови для подібної атаки зберігаються або навіть посилюються. Таким чином, атака aLTEr у межах LTE/5G - це не просто перехоплення трафіку, а цілеспрямована модифікація захищеного (шифрованого) каналу, яка ґрунтується на тому, що шифрування без цілісності дозволяє змінити шифротекст так, щоб після дешифрування отримати бажаний відкритий текст, і таким чином перенаправити мережеві запити жертви. Це вимагає спеціального обладнання (наприклад, програмно-визначених радіо-реле (SDR), кастомізованого стеку LTE) і близької фізичної присутності, але показує, що навіть сучасні мобільні стандарти можуть мати фундаментально слабкі місця.

У тестовому середовищі трафік, що проходив між емулятором користувацького обладнання та мережею даних, включав як легітимні запити,

так і шкідливі пакети, що імітували атаку. Моніторинговий модуль Suricata, розташований у площині користувацьких даних, аналізував кожен пакет і передавав результати до Kafka, яка виконувала роль системи обміну повідомленнями між компонентами. Далі Decision Engine (реалізований у середовищі Drools) обробляв дані та приймав рішення щодо дій, необхідних для ліквідації загрози. Після цього відповідна команда надходила до Policy Enforcement Point, який змінював правила доступу або блокував підозрілий трафік. У деяких випадках рішенням системи було внесення змін до міжмережевого екрану через SSH-з'єднання, де нові правила активувалися в реальному часі.

На рисунку 3.1 подано результати вимірювання середнього часу виявлення атаки та часу реакції системи.

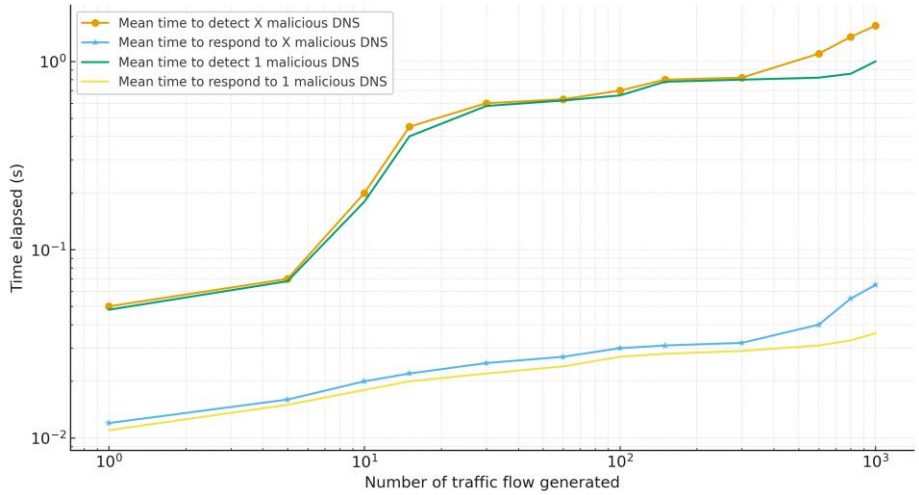


Рисунок 3.1 – Середній час виявлення та реагування на атаки

Для кожного експерименту моделювалися два варіанти навантаження: коли лише один пакет у потоці був шкідливим, і коли всі запити мали ознаки атаки. Незалежно від інтенсивності трафіку система демонструвала практично миттєву реакцію. Середній час виявлення становив менше однієї секунди від моменту потрапляння шкідливого пакета на інтерфейс до формування звіту Suricata. Середній час реакції тобто відправлення відповідного рішення від DSO до LSO також не перевищував однієї секунди. Зі збільшенням кількості запитів до 1200

в одному потоці трафіку спостерігалося лише незначне зростання часу реакції, що свідчить про лінійну залежність продуктивності від навантаження.

Отримані результати засвідчили, що запропонована архітектура не лише забезпечує швидке реагування на інциденти, а й зберігає масштабованість навіть у разі зростання обсягу даних. Це критично важливо для 5G Core, де обсяги можуть досягати гігабайтів за секунду, а затримка у виявленні загрози на кілька секунд може призвести до компрометації цілих сегментів мережі. Автоматизація взаємодії між компонентами через Kafka, а також чітке розділення функцій аналізу, прийняття рішення та застосування політик дозволили досягти стабільної продуктивності навіть при високих навантаженнях.

Другий експеримент був спрямований на дослідження ефективності поширення користувацьких політик у системі. Цей процес відтворює реальну ситуацію, коли власник сегменту бажає додати власне правило безпеки, наприклад, дозволити або заборонити певну пару IP-адреса клієнта (домен) - IP-адреса DNS. У даному сценарії користувач надсилає запит на білий список для певного домену, що вимагає додавання правила до конфігураційного файлу міжмережевого екрану та до бази правил IDS Suricata. Перед виконанням команда проходить перевірку у PCD, який порівнює нову політику з тими, що вже зберігаються у базі адміністратора. Якщо конфліктів не виявлено, система автоматично поширює правило через PDP до відповідних компонентів.

Перед початком експерименту система була попередньо заповнена 2000 правилами у міжмережевому екрані та 16 000 правилами в Suricata, щоб відтворити умови реального середовища. У цих умовах система мала не лише перевірити нові правила на конфлікти, але й ефективно оновити велику кількість конфігурацій без втрати працездатності. На рисунку 3.2 наведено залежність часу застосування політик від кількості одночасно доданих правил.

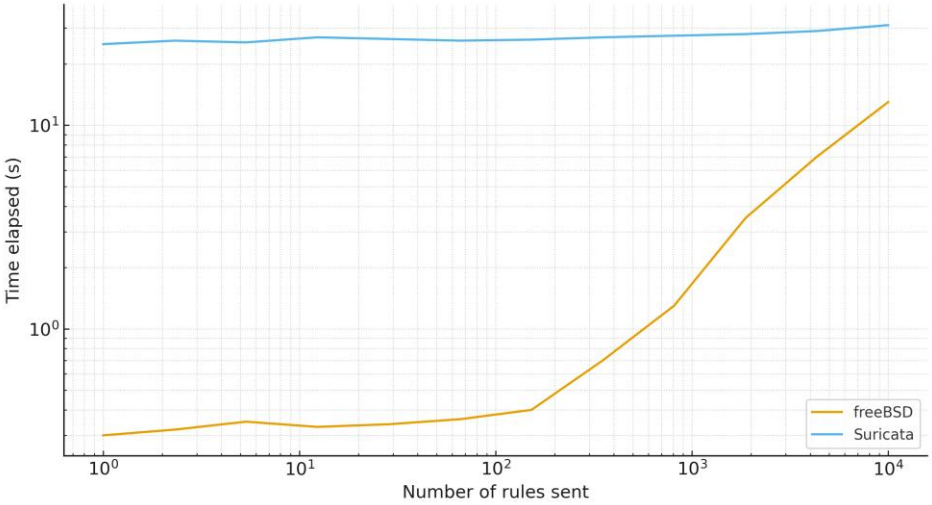


Рисунок 3.2 – Залежність часу застосування політик від кількості одночасно доданих правил

Результати показали, що навіть у разі оновлення 1000 правил тривалість процесу не перевищувала секунди. Лише при масовому оновленні від 1000 до 10000 записів час збільшувався до 10 секунд через необхідність перезавантаження PF FreeBSD. Водночас усі етапи передачі даних і аналізу політик у PCD виконувалися менш ніж за пів секунди, тобто затримка виникала виключно на рівні читання конфігураційних файлів.

Для системи виявлення вторгнень Suricata час оновлення був трохи довший у межах двох-трьох секунд, що зумовлено значним обсягом попередньо встановлених правил. Проте архітектура передбачає використання неблокувальної функції перезавантаження, яка дозволяє підтримувати фоновий режим оновлення без зупинки основного процесу аналізу трафіку. Це усуває ризик потенційної атаки типу DoS, коли зловмисник міг би надіслати надмірну кількість запитів на зміну політик, намагаючись тримати систему в постійному стані перезавантаження.

Порівняно з традиційними підходами, де клієнт змушений звертатися до адміністратора мережі для внесення змін, автономна архітектура скорочує час поширення політик із годин або навіть діб до кількох секунд. Раніше будь-яка зміна вимагала узгодження, перевірки сумісності, внесення вручну у системи управління політиками та подальшої перевірки коректності. Запропонована система усуває ці проміжні кроки завдяки автоматичній перевірці конфліктів і

каскадному оновленню оркестраторів. Результати експериментів підтвердили, що повний цикл від ініціації політики користувачем до її застосування в мережі займає мінімальний час і не порушує роботи інших сегментів мережі.

Отримані дані також демонструють ефективну взаємодію між рівнями оркестраторів. Після надходження політики локальний LSO виконує первинну перевірку на рівні клієнта, після чого передає запит до доменного DSO, який зіставляє його з політиками адміністратора. Після позитивного підтвердження політика повертається до LSO для поширення на відповідні функції безпеки. Якщо клієнт володіє кількома зрізами, DSO може автоматично передати політику на інші підмережі. Водночас локальні оркестратори можуть відмовити у застосуванні, якщо виявлять контекстні обмеження або відмінності в сервісних налаштуваннях. Такий підхід гарантує одночасно гнучкість і контрольованість процесу, що є ключовими вимогами для ізольованих сервісних середовищ 5G.

Загалом реалізація довела здатність системи до самостійного функціонування без участі людини на всіх етапах циклу: від виявлення інциденту до поширення оновлених політик. Висока швидкість реакції, лінійна масштабованість при зростанні навантаження та стабільна продуктивність компонентів засвідчують, що побудована архітектура є придатною для використання у промислових середовищах 5G Core. Вона здатна одночасно підтримувати тисячі правил безпеки, синхронізувати політики між зрізами та забезпечувати їхню узгодженість без зниження продуктивності мережі. Таким чином, проведене оцінювання підтвердило практичну ефективність проєктованої автономної архітектури. Вона забезпечує швидке виявлення атак, мінімальний час реакції та можливість оперативного оновлення політик без залучення адміністратора, що робить її перспективною основою для побудови інтелектуальних систем безпеки у 5G Core.

3.4 Висновки до розділу 3

В третьому розділі було реалізовано й експериментально підтверджено концепцію автономної та адаптивної архітектури безпеки для 5G Core, що

поєднує політико-кероване управління й замкнені контури автоматизації. Спроєктовано ієрархію оркестраторів безпеки з вертикальною координацією між Domain Security Orchestrator і Local Security Orchestrator, у складі яких працюють Monitoring/Analysis Engine, PDP з розмежованими PE/PA/PEP і Policy Conflict Detector. Архітектура забезпечує кероване внесення та поширення клієнтських політик без порушення глобальних обмежень оператора, опираючись на окремі репозиторії доменних і локальних правил та автоматичне узгодження в замкненому циклі спостереження → аналіз → рішення → застосування.

Практичну спроможність показано на повнофункціональному стенді 5G Core з використанням Open5GS, контейнеризації CNF у Kubernetes та інтеграцією Suricata, Kafka й Drools. Експерименти з імітацією атаки aLTEr засвідчили середній час виявлення й реакції менше секунди навіть за зростання трафіку, що підтверджує придатність підходу до високонавантажених сценаріїв ядра мережі. Другий експеримент довів ефективність каскадного поширення користувацьких політик. За умов попередньо насичених наборами правил оновлення фаєрвола та IDS виконувалося за секунди, а неблокувальні механізми перезавантаження виключили деградацію захисту. У сукупності це демонструє лінійну масштабованість, дотримання slice-ізоляції й керованість життєвого циклу політик без участі адміністратора.

Таким чином, запропонована архітектура перетворює безпеку з зовнішнього сервісу на невід’ємну частину керування 5G-послугами. Політики описуються декларативно, автоматично верифікуються конфлікти, узгоджуються між рівнями та оперативно застосовуються. Отримані результати підтверджують, що поєднання MANO/ZSM, HSPL/MSPL і дворівневої оркестрації створює надійний фундамент для подальшого розгортання адаптивних захисних тактик і розширення автономних можливостей системи безпеки в 5G Core.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою роботи є створення та експериментальне обґрунтування автономної архітектури кібербезпеки для 5G Core, що забезпечує безпечне поширення політик і швидке реагування на загрози без ручного втручання адміністратора. Дані системи встановлюються на серверному обладнанні, яке розміщене в приміщення спеціального типу. Пожежна безпека в серверних кімнатах є важливим завдання збереження матеріальних цінностей та життя людей.

Небезпечними чинниками, які впливають на людей під час пожежі, може бути відкритий вогонь чи іскри, підвищена температура повітря, предметів, токсичні продукти горіння, дим, знижена концентрація кисню. Тому пожежну безпеку вважають за невід'ємну частину охорони праці.

Пожежна безпека – це стан об'єкта, за якого із встановленою ймовірністю виключається можливість виникнення та розвитку пожежі, а також забезпечується захист матеріальних цінностей. У сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються різні елементи, дроти, комутаційні кабелі. При протіканні електричного струму відходить значна кількість теплоти, що може призвести до підвищення температури окремих вузлів до 80-100°С. З іншого боку, робоча температура силових транзисторів сягає 120°С. Все це може викликати оплавлення ізоляції з'єднувальних дротів, їх оголення і, як наслідок, коротке замикання, що супроводжується іскрінням, веде до неприпустимих температурних навантажень елементів схем, їх згоряння з виділенням диму [29].

Будівлі і ті їх частини, в яких розташовуються ЕОМ, повинні мати не нижче II ступень вогнестійкості. Приміщення для обслуговування, ремонту та налагодження ЕОМ повинні належати до категорії В за безпекою що до пожеж та вибухів, а за класом приміщення - до П за ПБЕ.

Неприпустимим є розташування приміщень категорій А і Б, а також виробництв з мокрими технологічними процесами поряд з приміщеннями, де розташовуються ЕОМ, виконується їх обслуговування, налагодження і ремонт, а також над такими приміщеннями або під ними.

Стіни кабін мають бути виготовлені з негорючих матеріалів. Дозволяється виготовляти їх зі скла та металевих конструкцій. У кабіні мусить бути оглядове вікно (вікна). Висота оглядового вікна має бути не менше 1,5 м, а відстань від підлоги не більше 0,8 м.

Приміщення з ЕОМ повинні бути оснащені системою автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог правил пожежної безпеки в Україні. В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, в яких розміщуються великі ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до правил пожежної безпеки в Україні та вимог нормативно-технічної та експлуатаційної документації заводу-виробника [29].

Підходи до засобів пожежогасіння повинні бути вільними. Будівлі та приміщення, в яких експлуатуються ПК та виконується їх обслуговування, налагодження і ремонт, повинні відповідати вимогам пожежної безпеки об'єктів будівництва, експлуатаційної документації заводу-виробника ПК, чинним санітарним нормам у сфері охорони праці.

Не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог, в інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення, мають бути оснащені вогнегасниками.

Приміщення, в яких розміщуються робочі місця операторів великих ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння

Система вентиляції обчислювальних центрів та приміщень з ЕОМ повинна бути обладнана блокувальним пристроєм, який забезпечує її відключення на випадок пожежі.

Пожежна безпека приміщень забезпечується такими засобами:

– справність електропроводки;

– наявність засобів пожежогасіння;

– наявність пожежної сигналізації.

До первинних засобів пожежогасіння у приміщеннях з ЕОМ відносяться різні вуглекислотні, аерозольні, порошкові вогнегасники, призначені для гасіння загорянь та пожеж у початковій стадії їх розвитку.

Вуглекислотні вогнегасники (ВВ-2, ВВ-5, ВВ-8) призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники містять вуглекислоту, яка при відкритті крана розширюється та викидається через розтруб у вигляді вуглекислого снігу температурою -55°С. Тривалість роботи вогнегасників 25-40 секунд, довжина струменя, що викидається, 1,5-2 м (ВВ-2, ВВ-5).

Аерозольні вогнегасники закачувального типу містять або тільки вогнегасний засіб, або ще й додатковий (робочий) газ (наприклад, азот, хладон). Вони призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники малогабаритні, спрощені (з об'ємом заряду від 0,25 до 1,0 літра).

Порошкові вогнегасники (ВП-1, Момент, ВП-2А, ВП-10А) застосовуються для гасіння лужних металів, що горять, горючих рідин, а також обладнання з напругою до 5000 В. Дані вогнегасники містять вогнегасний порошок і балон з

газом. Порошок з корпусу вогнегасника виштовхується стисненим газом (азот, повітря) приблизно за 30 секунд.

Автоматичні засоби пожежогасіння розраховані на подачу вогнегасної речовини у разі виникнення пожежі незалежно від того, перебувають у приміщенні люди або відсутні. Останнім часом знаходять широке застосування автономних автоматичних установок порошкового пожежогасіння.

Проведені дослідження в кваліфікаційній роботі вимагали взаємодії людини з серверним обладнанням. Тому важливим є забезпечити безпечні умови праці інженерів комп’ютерних систем при встановленні, налаштуванні та подальшому обслуговуванні систем захисту сервісів.

4.2 Оцінка стійкості роботи промислового підприємства до дії світлового випромінювання ядерного вибуху

Основну небезпеку для наземних об'єктів, зокрема і телекомунікаційних, становлять ударна хвиля, світлове (теплове) випромінювання, вторинні вражаючі фактори і радіоактивне зараження місцевості. Проте іноді доводиться враховувати і вплив проникаючої радіації та електромагнітного імпульсу.

Критеріями оцінки фізичної стійкості об'єкта прийняті: при впливі ударної хвилі - надлишкові тиски, при яких елементи виробничого комплексу не руйнуються або одержують такі ушкодження чи руйнування (слабкі і середні), при яких вони можуть бути відновлені в короткі терміни; при впливі світлового випромінювання - максимальні значення світлових імпульсів, при яких не відбувається загоряння матеріалів, сировини, устаткування, будинків і споруд; при впливі вторинних факторів - надлишкові тиски, при яких руйнування і пошкодження не призводять до аварій, пожеж, вибухів, затоплень, небезпечного зараження місцевості й атмосфери, тобто не призводять до ураження людей і виходу з ладу засобів виробництва [30].

Оцінка стійкості об'єкта включає визначення: видів вражаючих факторів, вплив яких можливий на об'єкт, та їх параметрів; впливу ударної хвилі на

елементи об'єкта; можливості виникнення пожеж; впливу вторинних вражаючих факторів.

Світлове випромінювання - це електромагнітне випромінювання, основним джерелом якого є світна область вибуху (вогненна куля), що складається з розпечених продуктів вибуху і повітря. Температура в ній сягає від 6 тисяч градусів за С. Тривалість світіння залежить від потужності ядерного заряду: при вибуху малого калібру - 1-2 сек., середнього - 2-4 сек, крупного та надкрупного - 10 і більше сек.

На світлове випромінювання припадає приблизно 30 % всієї енергії ядерного вибуху. Воно складається з ультрафіолетових, інфрачервоних і видимих променів. Основна кількість енергії світлового випромінювання (85%) виділяється в перші секунди з моменту вибуху.

Кількість енергії світлового випромінювання, яке падає на 1 см 2 поверхні, перпендикулярної напрямку його поширення, за весь час світіння, називається світловим імпульсом. Його величина вимірюється в джоулях на квадратний метр (Дж/м2).

Уражуюча дія світлового випромінювання вимірюється, головним чином, величиною світлового імпульсу і часом дії. Чим більша величина світлового імпульсу, що випромінюється за менший час, тим сильніший уражуючий ефект, який пропорційний поглинутій кількості енергії. Остання перетворюється в тепло і здатна викликати опіки та приводити до спалахування різних предметів.

Ураження людини можливе, як в результаті безпосередньої дії світлового випромінювання на шкірні покриви - світлові (первинні) опіки, так і в результаті спалахування одягу і навколишніх предметів - опосередковані (вторинні) опіки.

Можливість виникнення пожеж встановлюють за займистістю матеріалів від світлового імпульсу ядерного вибуху, руйнування печей, газопроводів, пошкодження електромережі, які можуть виникнути при аваріях, землетрусах, бурях та ін.

При оцінці стійкості об'єкта проти світлового випромінювання ядерного вибуху необхідно визначити максимальне значення світлового імпульсу яке

може бути на об'єкті. Світловий імпульс можна розрахувати за температурою загорання або нагрівання матеріалів і виробів.

Для оцінки стійкості об'єкта проти світлового випромінювання необхідні такі вихідні дані: характеристика будівель і споруд, характер виробництва, які горючі матеріали застосовуються у виробництві; вид готової продукції та місце її зберігання.

Оцінку стійкості електроенергетичного об'єкта до світлового випромінювання ядерного вибуху доцільно проводити у такій послідовності:

- визначити мінімальну відстань до можливого центру вибуху Rx, км;
- визначити максимальне значення світлового імпульсу I св.max, кДж/м2;
- визначити ступінь вогнестійкості будинку цеху;
- виявити в конструкціях будівлі елементи, виготовлені із горючих матеріалів та визначити їх характеристики (наприклад: для дверей та віконних рам – дерев’яних, пофарбованих в темний колір I св.max =250, кДж/м2);
- визначити границю стійкості об’єкту до світлового випромінювання за мінімальним світловим імпульсом, що викликає спалахування в будівлі I св.lim. кДж/м2;
- здійснити порівняння та дати оцінку стійкості об’єкту: при I св.lim < I св.max об’єкт не стійкий до світлового випромінювання, при I св.lim > I св.max - стійкий;
- визначити ступінь руйнування будівлі від ударної хвилі при максимальному очікуваному надлишковому тиску;
- визначити зону пожеж, в якій може опинитися об’єкт.

На основі отриманих даних робиться відповідний висновок щодо стійкості електроенергетичного об'єкта до світлового випромінювання ядерного вибуху:

- чи викликає складну пожежну ситуацію на об’єкті при ядерному вибуху заданої потужності очікуваний максимальний світловий імпульс (кДж/м2) та надлишковий тиск ударної хвилі (кПа);
- чи опиниться об’єкт в зоні суцільних пожеж;
- чи об’єкт стійкий до світлового випромінювання за границею стійкості;

- що із обладнання, конструктивних елементів будівлі складає пожежну небезпеку для об’єкту;

- робитися висновок про доцільність підвищення границі стійкості об’єкту.

Підвищити границю стійкості можливо шляхом виконання наступних заходів: замінити крівлю об’єкту на азбестоцементові; замінити дерев’яні віконні рами на металеві; набити на двері сталлю по азбестовій прокладці; провести на об’єкті профілактичні протипожежні заходи.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи магістра було проведено комплексне дослідження проблем забезпечення кібербезпеки в архітектурі 5G Core, що функціонує в умовах віртуалізованої NFV/SDN-інфраструктури. Робота спрямована на підвищення стійкості ядра мережі до сучасних кібератак шляхом створення автономної, політико-керованої архітектури безпеки з підтримкою динамічного реагування на загрози.

У першому розділі було проаналізовано сучасний стан розвитку 5G Core та основні принципи його побудови, включно з концепціями сервісно-орієнтованої архітектури (SBA), віртуалізації мережевих функцій (NFV) та програмно-визначених мереж (SDN). Розглянуто елементи архітектури MANO та ZSM, визначено проблеми узгодженості політик між рівнями керування та безпеки, а також обґрунтовано актуальність переходу до автономних систем безпеки з замкненими контурами управління.

У другому розділі проведено детальний аналіз вразливостей і загроз у середовищі 5G Core. Визначено специфічні ризики, пов’язані з функціонуванням User Plane без повного integrity-захисту, уразливості stateful-фаєрволів, атаки на DHCP та Router Advertisement, а також потенційні загрози при взаємодії оркестраторів і VNF. Розроблено класифікацію типових векторів атак і формалізовано їхній вплив на доступність, цілісність і конфіденційність сервісів.

У третьому розділі спроєктовано автономну архітектуру безпеки 5G Core, що поєднує ієрархічну систему поширення політик між доменним (DSO) та локальним (LSO) оркестраторами безпеки, підсистему Policy Decision Point / Policy Enforcement Point (PDP/PEP) і модуль Policy Conflict Detector (PCD) для виявлення конфліктів між політиками оператора та користувацьких сегментів. Запропоновано механізм селективного керування state-таблицями фаєрволів і метод контентної рандомізації службових полів DHCP/RA із використанням криптографічних маркерів цілісності. Експериментальна перевірка на базі open-source стеку Open5GS і Kubernetes підтвердила ефективність рішень: скорочення

часу розповсюдження політик, зменшення кількості конфліктів та покращення стійкості до атак типу state pollution і MITM.

У результаті виконання роботи дістало подальший розвиток застосування контентної рандомізації службових протоколів у контексті 5G User Plane. Практичне впровадження отриманих рішень забезпечує підвищення рівня автономності, керованості та адаптивності систем кіберзахисту в мережах п’ятого покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. GeeksforGeeks. (2022, November 11). 5G Network Architecture - GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/5g-network-architecture/
2. Flinders, M. (n.d.). 5G Examples, Applications & Use Cases | IBM. IBM. https://www.ibm.com/think/topics/5g-use-cases
3. GeeksforGeeks. (2023, June 13). Cloud-Native Architecture - GeeksforGeeks. https://www.geeksforgeeks.org/cloud-computing/cloud-native-architecture/
4. Cloud-Native 5G Service-Based Architecture (SBA) Solution. (n.d.). F5, Inc. https://www.f5.com/resources/solution-guides/5g-sba-solution-overview
5. GeeksforGeeks. (2019, July 2). What is Software Defined Networking (SDN)? https://www.geeksforgeeks.org/computer-networks/software-defined-networking/
6. Goodwin, M. (n.d.). What Is Network Functions Virtualization (NFV)? | IBM. IBM. https://www.ibm.com/think/topics/network-functions-virtualization
7. OSM. (n.d.). OSM. https://osm.etsi.org/
8. 5G Core Network Architecture A Next-Generation Connectivity. (n.d.). Niral Networks. https://niralnetworks.com/5g-core-network-architecture/
9. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56. https://doi.org/10.31891/2219-9365-2024-79-7
10. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220. https://doi.org/10.31891/2219-9365-2024-80-26
11. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024;

Запоріжжя, Україна), 145-146. https://doi.org/10.62731/mcnd-24.05.2024.001

12. Virtualized Infrastructure Manager (VIM). (n.d.). Cisco. https://www.cisco.com/site/us/en/products/networking/software/virtualized-infrastructure-manager/index.html
13. GeeksforGeeks. (2023, October 5). Network Slicing in 5G Networks - GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/network-slicing-in-5g-networks/
14. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.
15. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.
16. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
17. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.
18. Lindemulder, G., & Kosinski, M. (n.d.). What Is Zero Trust? | IBM. IBM. https://www.ibm.com/think/topics/zero-trust
19. Lee, S. (n.d.). Documentation. Open5GS. https://open5gs.org/open5gs/docs/
20. GitHub - aligungr/UERANSIM: Open source 5G UE and RAN (gNodeB) implementation. (n.d.). GitHub. https://github.com/aligungr/UERANSIM
21. What is the CIA Triad and Why is it important? | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/cia-triad

22. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.
23. Lindemulder, G., & Kosinski, M. (n.d.-a). What Is a Man-in-the-Middle (MITM) Attack? | IBM. IBM. https://www.ibm.com/think/topics/man-in-the-middle
24. NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
25. Production-Grade Container Orchestration. (n.d.). Kubernetes. https://kubernetes.io/
26. Open5GS. (n.d.). GitHub. https://github.com/open5gs
27. GitHub - aligungr/UERANSIM: Open source 5G UE and RAN (gNodeB) implementation. (n.d.). GitHub. https://github.com/aligungr/UERANSIM
28. Install ueransim on Linux | Snap Store. (n.d.). Snapcraft. https://snapcraft.io/ueransim
29. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.
30. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі. Книга 2. [навчальний посібник]. Львів : "Магнолія 2006", 2014. 312 с.
31. Nedzelky, D., Derkach, M., Skarga-Bandurova, I., Shumova, L., Safonova, S., & Kardashuk, V. (2021, September). A Load Factor and its Impact on the Performance of a Multicore System with Shared Memory. In 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 499-503). IEEE.
32. Основи охорони праці: навчальний посібник / М. П. Купчі та ін. Київ: Основа, 2000. 416 с.
33. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль: ТНТУ. 2022. 150 с.

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

УДК 004.056.5
Д. Марчук; В. Тимощук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АРХІТЕКТУРА БЕЗПЕКИ ЯДРА 5G НА ОСНОВІ ВІРТУАЛІЗОВАНИХ МЕРЕЖЕВИХ ФУНКЦІЙ ТА УЗГОДЖЕНИХ ПОЛІТИК

UDC 004.056.5
D. Marchuk; V. Tymoshchuk

SECURITY ARCHITECTURE FOR THE 5G CORE BASED ON VIRTUALIZED NETWORK FUNCTIONS AND HARMONIZED POLICIES

Розвиток мобільних мереж п'ятого покоління із широким використанням NFV, SDN, сервісно-орієнтованої архітектури (SBA), network slicing та MEC радикально ускладнює завдання побудови цілісної системи кібербезпеки ядра 5G Core [1]. Інтенсивне впровадження віртуалізованих мережевих функцій, динамічне масштабування сервісів та поява великої кількості взаємодіючих доменів управління призводять до того, що традиційні засоби захисту та статичні політики доступу виявляються недостатніми. Додаткові ризики створюють компроміси на користь продуктивності, зокрема захист цілісності у площині користувача, як опція, кешування станів у stateful-фаєрволах та активне використання проксі та сервісної сітки (service mesh). Усе це суттєво ускладнює своєчасне виявлення загроз і точну локалізацію атак у межах 5G Core.

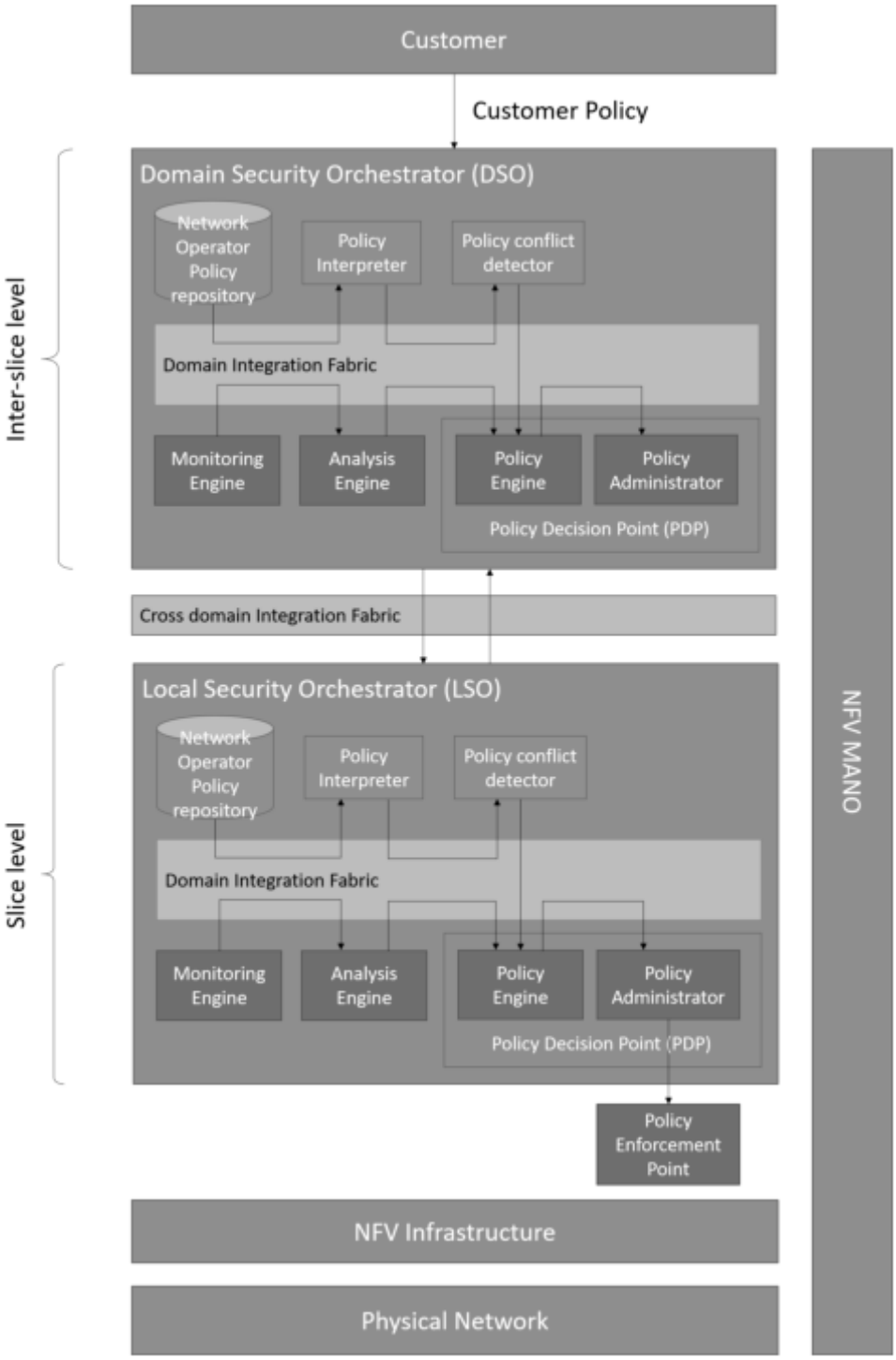
У роботі представлено політико-керовану архітектуру безпеки 5G Core зі замкненими контурами управління, що забезпечує узгоджену синхронізацію політик MANO/ZSM [2] та мінімізує побічний вплив контрзаходів на легітимні сервіси. Архітектура базується на ієрархії доменного та локальних оркестраторів безпеки з інтегрованими компонентами Policy Decision Point та Policy Enforcement Point, які використовують двоступеневу модель політик HSPL/MSPL і модуль Policy Conflict Detector для автоматизованої перевірки клієнтських політик відносно глобальних правил оператора. Особливу увагу приділено двом критичним класам вразливостей: атакам на таблиці станів stateful-фаєрволів для протоколів без стану з'єднання та маніпуляціям DHCP/RA-повідомленнями, що транспортуються через площину користувача без гарантованого захисту цілісності.

Для захисту від атак на таблиці станів запропоновано механізм таргетованого керування записами станів, який дозволяє локалізувати шкідливу активність без глобального скидання таблиці. Для протидії маніпуляціям DHCP/RA-повідомленнями запропоновано механізм автентифікації службових полів з використанням криптографічних перевірок, що забезпечують підтвердження походження повідомлень без необхідності повного увімкнення захисту цілісності для всього користувацького трафіку. Запропоновані підходи апробовано на експериментальному стенді з використанням Open5GS, контейнеризації CNF в Kubernetes та інтеграцією Suricata, Kafka й Drools, де продемонстровано скорочення часу реагування на атаки та зменшення кількості побічних відмов сервісу в сегментованих 5G-середовищах.

Література

1. 5G Core. Supermicro. URL: https://www.supermicro.com/en/glossary/5g-core (date of access: 01.12.2025)
2. . IETF | Internet Engineering Task Force. URL: https://www.ietf.org/proceedings/88/slides/slides-88-opsawg-6.pdf (дата звернення: 01.12.2025).
3. Open5GS. GitHub. URL: https://github.com/open5gs (date of access: 01.12.2025).

Додаток Б Багатошарове керування безпекою



Додаток В Логічна організація компонентів системи