ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту мережевих каналів передачі конфіденційних даних від несанкціонованого доступу на базі операційної системи Linux»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

_____ Бондаренко Нікіта Сергійович

Виконав: здобувач вищої освіти групи СЗДМ 61
Бондаренко Нікіта

Керівник: КОТЕНКО Андрій
к.т.н., професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

___ Бондаренко Нікіта Сергійович _____ ___
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Система захисту мережевих каналів передачі конфіденційних даних від несанкціонованого доступу на базі операційної системи Linux»
керівник кваліфікаційної роботи Котенко А.М канд. техн. наук, доц
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. №467

2. Строк подання кваліфікаційної роботи 20.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: Корпоративна мультисервісна мережа комерційного банку (наприклад, "Онлайн-Банк"), що віднесений до об'єктів критичної інфраструктури (ОКІ) у банківському секторі України.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1 Дослідження теоретичних основ захисту мережевих каналів та аналіз нормативних вимог щодо забезпечення конфіденційності даних у банківському секторі України.
4.2 Аналіз архітектури корпоративної мережі банку, розробка моделі порушника та формування моделі загроз для критичних каналів передачі даних.
4.3 Проєктне обґрунтування вибору технологічного стека (WireGuard, nftables) та розробка цільової архітектури програмно-визначеної системи захисту мережевих каналів.
4.4 Практична реалізація криптографічного шлюзу на базі ОС Linux, налаштування політик фільтрації трафіку та верифікація ефективності спроєктованої системи шляхом тестування.

5. Перелік графічного матеріалу: ___Презентаційний матеріал на_____слайдах.__ _____
_____

6. Дата видачі завдання_____15.10.2025_____

КАЛЕНДАРНИЙ ПЛАН

/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Підбір науково-технічної літератури		
	Написання першого розділу роботи		
	Написання другого розділу роботи		
	Написання третього розділу роботи		
	Написання висновків по роботі		
	Підготовка демонстраційних матеріалів		
	Підготовка доповіді		

Здобувач вищої освіти _____ Нікіта БОНДАРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Андрій КОТЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел та додатків. Загальний обсяг роботи складає 91 сторінок, містить 14 рисунків, 4 таблиці. Список використаних джерел містить 40 найменування і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення рівня захищеності мережевої інфраструктури банківської установи шляхом проектування та впровадження системи захисту каналів передачі даних на базі відкритого програмного забезпечення та операційної системи Linux.

В кваліфікаційній роботі проведено аналіз нормативних вимог Національного банку України до захисту інформації та сучасних загроз мережевій безпеці фінансових установ. Обґрунтовано вибір протоколу WireGuard та інструментів Linux (nftables, Suricata) для побудови захищених VPN-тунелів.

Розроблено схему захищеної мережевої взаємодії між філіями та центральним офісом банку. Практично реалізовано налаштування криптографічного шлюзу, міжмережевого екрану та системи виявлення вторгнень. Проведено тестування стійкості спроектованої системи до мережевих атак та оцінку її продуктивності.

Запропоновано комплекс організаційно-технічних заходів щодо протидії методам соціальної інженерії та підвищення обізнаності персоналу банку у питаннях кібербезпеки.

Апробація:

А.М. Котенко, Н.С. Бондаренко, ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У МЕРЕЖЕВИХ КАНАЛАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ШЛЯХОМ ВИКОРИСТАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.52-53. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА БАНКІВ, ЗАХИСТ КАНАЛІВ ЗВ'ЯЗКУ, VPN, LINUX, WIREGUARD, NFTABLES, СОЦІАЛЬНА ІНЖЕНЕРІЯ, КРИПТОГРАФІЧНИЙ ЗАХИСТ.

ABSTRACT

The text part of the qualification thesis consists of an introduction, four chapters, general conclusions, a list of references, and appendices. The total volume of the thesis is 85 pages and includes 14 figures and 4 tables. The list of references contains 42 sources and occupies 5 pages.

The aim of the qualification thesis is to increase the security level of the network infrastructure of a banking institution by designing and implementing a system for protecting data transmission channels based on open-source software and the Linux operating system.

The thesis analyses the regulatory requirements of the National Bank of Ukraine regarding information protection and current threats to the network security of financial institutions. The choice of the WireGuard protocol and Linux tools (nftables, Suricata) for building secure VPN tunnels is substantiated.

A scheme of secure network interaction between the bank's branches and its central office has been developed. The configuration of a cryptographic gateway, firewall, and intrusion detection system has been practically implemented. Testing of the resistance of the designed system to network attacks and an assessment of its performance have been carried out.

A set of organizational and technical measures has been proposed to counteract social engineering methods and to increase the cybersecurity awareness of the bank's staff.

Key words: INFORMATION SECURITY OF BANKS, PROTECTION OF COMMUNICATION CHANNELS, VPN, LINUX, WIREGUARD, NFTABLES, SOCIAL ENGINEERING, CRYPTOGRAPHIC PROTECTION.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

Скорочення Розшифрування

АБС – Автоматизована банківська система

ДБО – Дистанційне банківське обслуговування

КЗІ – Криптографічний захист інформації

НБУ – Національний банк України

ОС – Операційна система

ПЗ – Програмне забезпечення

ЦДЦ – Центральний дата-центр

AEAD – Authenticated Encryption with Associated Data (Автентифіковане шифрування з пов'язаними даними)

AES – Advanced Encryption Standard (Удосконалений стандарт шифрування)

API – Application Programming Interface (Інтерфейс прикладного програмування)

CIA – Confidentiality, Integrity, Availability (Конфіденційність, цілісність, доступність)

DDoS– Distributed Denial of Service (Розподілена атака на відмову в обслуговуванні)

DMZ – Demilitarized Zone (Демілітаризована зона)

GDPR – General Data Protection Regulation (Загальний регламент про захист даних)

IDS/IPS – Intrusion Detection/Prevention System (Система виявлення/запобігання вторгненням)

IPsec – Internet Protocol Security (Набір протоколів для захисту даних на мережевому рівні)

MitM – Man-in-the-Middle (Атака «Людина посередині»)

NAT – Network Address Translation (Трансляція мережевих адрес)

NGFW – Next-Generation Firewall (Міжмережевий екран нового покоління)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій США)

PCI DSS – Payment Card Industry Data Security Standard (Стандарт безпеки даних індустрії платіжних карток)

PFS – Perfect Forward Secrecy (Досконала пряма секретність)

SDS – Software-Defined Security (Програмно-визначена безпека)

SIEM – Security Information and Event Management (Система управління інформаційною безпекою та подіями)

SSH – Secure Shell (Протокол безпечного віддаленого управління)

TLS – Transport Layer Security (Протокол захисту транспортного рівня)

VPN – Virtual Private Network (Віртуальна приватна мережа)

ВСТУП

Сучасний етап розвитку банківського сектору України характеризується швидкою цифровізацією систем документообігу та бізнес-процесів. Сучасні банки переходять на онлайн обслуговування клієнтів та надання багатьох сервісів онлайн. Особливої актуальності питання захисту каналів зв'язку набуває при обробки персональних даних, платіжної інформації та внутрішніх документів які містять конфіденційну інформацію.

Регулятором питанням захисту інформації в банківському секторі займається Національний банк України. Розроблені постанови та вимоги повинні бути виконані банками та постійно підтримувати їх актуальність. Виконання цих вимог потребує від банківських установ впровадження комплексних технічних та організаційних рішень, здатних забезпечити криптографічний захист трафіку, контроль доступу, виявлення та блокування мережевих атак, а також належний рівень моніторингу подій інформаційної безпеки.

В умовах війни та активних дій з ворожої сторони об'єкти критичної інфраструктури, до яких належать банки, стають пріоритетними цілями для кібератак. Компрометація мережевих каналів передачі даних може призвести значних фінансових збитків, але й до дестабілізації фінансової системи держави.

У зв'язку з цим, актуальним є завдання побудови захищених каналів зв'язку (VPN) на базі відкритих операційних систем (ОС) сімейства Linux, які дозволяють гнучкі налаштування політик безпеки, забезпечують прозорість програмного коду та відповідають вимогам регуляторів.

Метою роботи є підвищення захисту мережі банку шляхом розробки та впровадження системи захисту каналу передачі конфіденційних даних на базі операційної системи Linux та програмного забезпечення з відкритим програмним кодом.

Для досягнення поставленої мети в роботі вирішуються такі завдання:

– **Систематизувати методи** захисту інформації в банківському секторі та проаналізувати нормативні вимоги НБУ що стосуються захисту мережевих каналів передачі конфіденційних даних у банківських

установах;

- **Визначити** основні вектори атак на корпоративну мережу.
- **Обґрунтувати вибір** програмного забезпечення а саме протоколу WireGuard та систем виявлення та запобігання вторгнень (nftables, Suricata), для побудови захищеного шлюзу та спроектувати топологію безпечної мережі банку.
- **Розробити та протестувати** захист каналів передачі даних на базі ОС Linux, оцінити її стійкість до типових мережевих атак та ефективність застосування в мережевій інфраструктурі банківської установи.

Об’єкт дослідження – мережеві канали передачі конфіденційних даних у розподіленій інфраструктурі банківської установи.

Предмет дослідження – методи, засоби та програмно-апаратні рішення захисту мережевих каналів передачі конфіденційних даних від несанкціонованого доступу на базі операційної системи Linux із використанням протоколу WireGuard, nftables та системи виявлення вторгнень Suricata.

Апробація роботи. Основний результат роботи доповідався на інноваційній науково-практичній конференції з питань кібербезпеки банківської сфери «Кібербезпека корпоративних мереж: технології, ризики та протидія».

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ МЕРЕЖЕВИХ КАНАЛІВ ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1. Поняття мережевого каналу та класифікація в корпоративних мережах

У корпоративній інфраструктурі мережевий канал передачі даних слід розглядати як комплексну сукупність фізичних середовищ, активного мережевого обладнання та логічних протокольних засобів, що забезпечують транспорт інформації між вузлами з гарантованими параметрами доступності (Availability), цілісності (Integrity) та конфіденційності (Confidentiality).

На фізичному та канальному рівнях (L1/L2 моделі OSI) сучасна корпоративна мережа базується на конвергенції технологій LAN, MAN та WAN, використовуючи як дротові (оптоволокно, вита пара), так і бездротові середовища передачі. Однак ключовим елементом для забезпечення зв’язності географічно розподілених філій є логічні надбудови, зокрема технології віртуальних приватних мереж (VPN) (рис. 1.1). Архітектура таких мереж дозволяє реалізовувати сценарії:

- Site-to-Site VPN: для об'єднання офісів (використовуючи IPsec, GRE over IPsec або DMVPN).
- Remote Access VPN: для підключення віддалених співробітників (SSL/TLS VPN, IKEv2).
- Host-to-Host: для захищеної взаємодії критичних серверів.

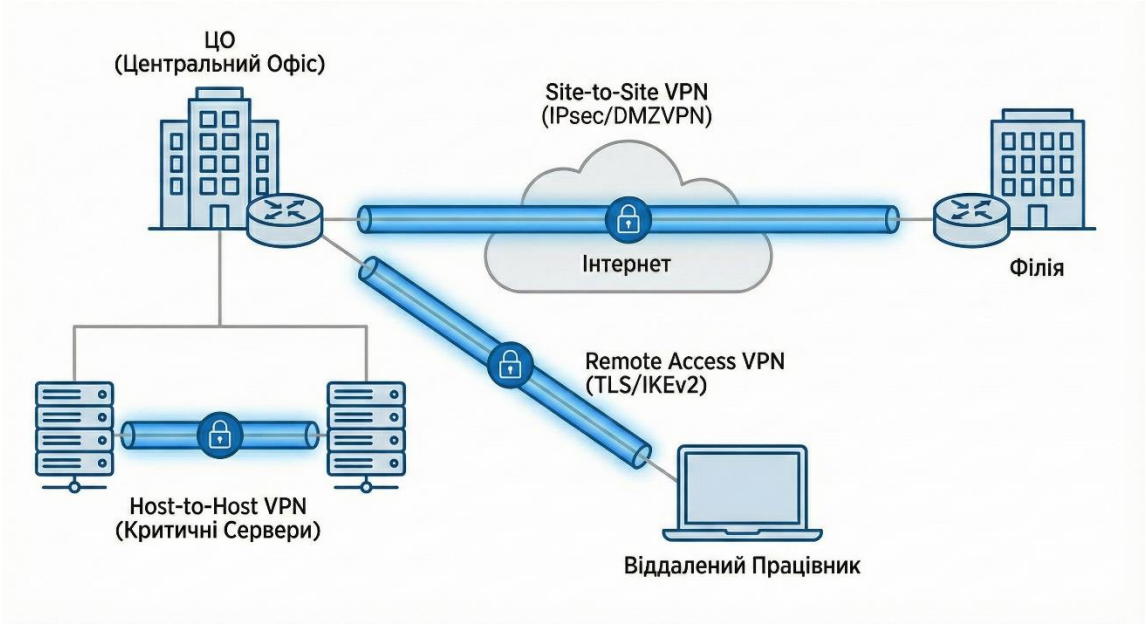


Рис. 1.1. Типові сценарії застосування технологій VPN у корпоративній мережі.

Класифікація, механізми інкапсуляції та криптографічного захисту таких каналів детально регламентуються міжнародними стандартами та найкращими практиками. Зокрема, базовий стандарт IETF **RFC 4301** («Security Architecture for the Internet Protocol») визначає архітектуру IPsec, а спеціальна публікація **NIST SP 800-77** («Guide to IPsec VPNs») надає рекомендації щодо налаштування безпечних тунелів, вибору криптографічних алгоритмів (AES-GCM, SHA-256) та управління ключами.

У сегменті захищених каналів критично важливим є застосування принципів «глибинного захисту» (Defense-in-Depth). Згідно з вимогами **Постанови Правління НБУ № 95** «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», обов’язковим є використання:

1. **Мережевого екранування (Firewalling):** контроль трафіку на межах периметра та між внутрішніми зонами.
2. **Сегментації мережі:** логічне відокремлення критичних ресурсів (VLAN, VRF).
3. **Демілітаризованих зон (DMZ):** винос публічних сервісів у ізольовані сегменти для мінімізації ризиків компрометації внутрішньої мережі.

Таким чином, ефективний мережевий канал у корпоративному середовищі це не просто засіб зв'язку, а керована система, що повинна відповідати суворим угодам про рівень надання послуг (SLA) щодо пропускної здатності (Bandwidth), затримки (Latency), джитера (Jitter) та відмовостійкості, забезпечуючи при цьому відповідність регуляторним нормам інформаційної безпеки.

1. Класифікація мережевих каналів у корпоративних інфраструктурах

У сучасних корпоративних мережах канали передачі даних класифікують за сукупністю ознак, що визначають їх фізичні параметри, логічну структуру та сферу застосування.

1.1. За територіальним масштабом:

- LAN (Local Area Network): Локальні мережі, що охоплюють межі одного офісу, будівлі або кампусу. Базуються переважно на стандарті Ethernet (IEEE 802.3) та бездротових технологіях Wi-Fi (IEEE 802.11).
- MAN (Metropolitan Area Network): Мережі міського масштабу, що забезпечують високошвидкісну комутацію між розрізненими локальними сегментами (наприклад, між відділеннями банку в межах одного міста).
- WAN (Wide Area Network): Глобальні мережі, що об’єднують територіально розподілені філії, дата-центри та хмарні ресурси. Реалізуються через канали інтернет-провайдерів, виділені MPLS-мережі або з використанням технології SD-WAN (Software-Defined WAN).

1.2. За типом фізичного середовища передачі:

- Дротові канали:
  - *Мідні лінії:* Вита пара (стандарти Cat 5e/6/6a/7) для підключення кінцевих пристроїв; технології xDSL для застарілих або резервних підключень.
  - *Оптоволоконні лінії:* Одномодові (SMF) для магістральних каналів на великі відстані та багатомодові (MMF) для високошвидкісних з’єднань у межах ЦОД.
- Бездротові канали:

- Wi-Fi для мобільності персоналу;
- Стільникові мережі (4G/LTE, 5G) як резервні канали зв’язку (Backup link);
- Радіорелейні та супутникові системи для забезпечення зв’язку у важкодоступних локаціях.

1.3. За логічною організацією та топологією:

- Виділені фізичні канали (Leased Lines): Прямі з’єднання типу «точка-точка», що орендуються в операторів зв’язку (Dark Fiber, L1/L2 VPN).
- Віртуальні приватні мережі (Overlay VPN): Логічно ізольовані захищені тунелі, побудовані поверх публічних мереж (Underlay). Основні технології включають IPsec-VPN, SSL/TLS-VPN (OpenVPN), WireGuard. Архітектуру та вимоги до безпеки таких мереж регламентовано стандартом NIST SP 800-77.
- Внутрішньомережеве тунелювання: Використання протоколів GRE, IP-in-IP, VXLAN для сегментації трафіку, створення віртуальних мереж поверх фізичної інфраструктури та забезпечення мобільності віртуальних машин.

1.4. За рівнем реалізації у моделі OSI:

- L2-канали (Data Link Layer): Технології VLAN (IEEE 802.1Q), QinQ, L2TP, що дозволяють передавати Ethernet-кадри між географічно віддаленими сегментами.
- L3-канали (Network Layer): Маршрутизовані з’єднання, IP-тунелі (GRE, IPIP), IPsec у тунельному режимі. Стандарт IETF RFC 4301 визначає архітектуру безпеки для IP-трафіку.
- L4–L7 канали (Transport/Application Layer): Сесії на базі TCP/UDP, захищені з’єднання SSL/TLS, SSH-тунелі, WebSocket-з’єднання.

2. Специфіка мережевих каналів у банківських установах

Для банківського сектору архітектура мережевих каналів формується під впливом жорстких вимог до відмовостійкості (High Availability) та інформаційної безпеки. Критичність каналів зумовлена характером інформації, що передається:

- фінансові транзакції та платіжні доручення (SWIFT, СЕП);
- персональні дані клієнтів (PII) та відомості, що становлять банківську таємницю;
- дані автентифікації та ключі шифрування;
- службовий трафік управління інфраструктурою.

Регуляторні вимоги: Діяльність українських банків у цьому аспекті суворо регламентується постановами Національного банку України (зокрема Постановою № 95), які вимагають обов'язкової сегментації мережі, відокремлення операційного середовища від тестового та суворого контролю міжсегментних потоків (Firewalling).

Додатково, міжнародний стандарт ISO/IEC 27001:2022 у додатку Annex A визначає конкретні контроли для мережевої безпеки:

- A.8.20 (Network security): Забезпечення безпеки мереж і захист інформації у них.
- A.8.21 (Security of network services): Визначення рівня послуг та вимог до безпеки мережевих сервісів.
- A.8.22 (Segregation of networks): Розділення мереж на сегменти (зони безпеки) для локалізації можливих атак.

Таким чином, корпоративна мережа банку це не просто набір каналів зв'язку, а складна ієрархічна система зон (CDE Cardholder Data Environment, DMZ, LAN користувачів, серверні сегменти), об'єднаних захищеними каналами з обов'язковим шифруванням та моніторингом.

1.2. Конфіденційні дані та вимоги до їх захисту у мережевих каналах

1.2.1. Класифікація інформаційних активів та модель загроз

У корпоративному контексті банківської установи поняття конфіденційної інформації виходить за межі загальних визначень і регламентується законодавчими актами. До критичних інформаційних активів, що передаються мережевими каналами, належать:

- Банківська таємниця: інформація про рахунки, операції та фінансово-

економічний стан клієнтів (згідно із Законом України «Про банки і банківську діяльність»).

- Персональні дані (PII): відомості про клієнтів та співробітників, захист яких регулюється Законом України «Про захист персональних даних» та європейським регламентом GDPR.
- Дані платіжних карток (PAN): повний номер картки, термін дії, CVV-коди (об’єкт захисту стандарту PCI DSS).
- Критична системна інформація: конфігураційні файли мережевого обладнання, ключі шифрування, схеми топології мережі та дані автентифікації.

Управління безпекою цих даних базується на класичній тріаді CIA (Confidentiality, Integrity, Availability), адаптованій до мережевого рівня:

1. Конфіденційність: гарантія того, що перехоплений у каналі трафік не може бути прочитаний сторонніми особами (досягається шифруванням).
2. Цілісність: гарантія того, що дані не були змінені або спотворені під час транзиту (забезпечується хешуванням та кодами автентифікації повідомлень HMAC).
3. Доступність: забезпечення безперервного доступу до каналів зв'язку та захист від атак типу DDoS.

1.2.2. Нормативні вимоги та міжнародні стандарти

Вимоги до захисту даних у мережевих каналах формуються на основі багаторівневої системи стандартів:

А. Стандарти серії ISO/IEC 27000:

- ISO/IEC 27001:2022: встановлює вимоги до Системи управління інформаційною безпекою (ISMS), визначаючи необхідність оцінки ризиків передачі даних.
- ISO/IEC 27033 (Network security): є профільним стандартом для даної роботи і складається з кількох частин:
  - *Part 1:* Огляд та концепції мережевої безпеки.
  - *Part 2:* Проєктування та впровадження безпеки мережі.

- *Part 3:* Еталонні мережеві сценарії (загрози, проєктування).
- *Part 4:* Захист комунікацій між мережами (шлюзи безпеки, firewall).
- *Part 5:* Безпека комунікацій через віртуальні приватні мережі (VPN).

Б. Галузеві стандарти (PCI DSS): Оскільки робота стосується банківської сфери, критичним є дотримання стандарту безпеки даних індустрії платіжних карток PCI DSS v4.0. Вимога 4 цього стандарту («Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks») прямо зобов'язує використовувати надійні криптографічні протоколи (наприклад, TLS 1.2/1.3, IPsec) для передачі даних через відкриті мережі та забороняє використання застарілих протоколів (SSL, ранні версії TLS, WEP).

В. Національне регулювання (НБУ): Постанови Правління Національного банку України (зокрема № 95) вимагають від банків забезпечення криптографічного захисту інформації (КЗІ) під час її передачі телекомунікаційними каналами, що виходять за межі контрольованої зони, а також використання засобів кваліфікованого електронного підпису (КЕП) для забезпечення юридичної значущості та цілісності транзакцій.

1.3. Моделі загроз і вразливостей мережевих каналів

1.3.1. Класифікація загроз та векторів атак

Аналіз безпеки корпоративної інфраструктури базується на ідентифікації актуальних загроз. У контексті банківських мереж доцільно застосовувати класифікацію, що враховує не лише джерело, а й вектор реалізації атаки (Attack Vector).

А. За джерелом походження (Threat Agents):

- Зовнішні: Кіберзлочинні угруповання (APT-групи), хактивісти, конкуренти, що діють через публічні мережі (Інтернет) або зламані зовнішні вузли партнерів (Supply Chain Attacks).
- Внутрішні (Інсайдери), серед яких: *зловмисні (Malicious Insider)* – співробітники, що навмисно саботують роботу або викрадають дані з корисливих мотивів та *ненавмисні (Negligent Insider)* – персонал, чиї дії

через некомпетентність або недбалість призводять до витоку даних (наприклад, помилки конфігурації, фішинг).

Б. За моделлю STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege): Ця методологія дозволяє структурувати загрози для кожного елемента мережі:

- Spoofing (Підміна): Видача себе за інший вузол мережі (IP/MAC/DNS Spoofing).
- Tampering (Модифікація): Зміна даних у процесі передачі (Man-in-the-Middle).
- Information Disclosure (Розкриття інформації): Сніфінг трафіку, аналіз метаданих.
- Denial of Service (Відмова в обслуговуванні): Атаки на виснаження каналів або ресурсів обладнання.

В. За рівнем моделі OSI/ISO:

- L1 (Physical): Фізичне пошкодження кабелів, несанкціоноване підключення до портів комутаторів або крос-панелей.
- L2 (Data Link): Атаки на протоколи комутації: MAC Flooding, ARP Spoofing, VLAN Hopping (спроба виходу за межі ізольованого сегмента), STP Manipulation.
- L3 (Network): IP Spoofing, фрагментація пакетів (Teardrop), атаки на протоколи маршрутизації (OSPF/BGP Injection), сканування портів.
- L4 (Transport): TCP Session Hijacking, SYN Flood, атаки на реалізацію SSL/TLS (наприклад, Downgrade attacks).
- L7 (Application): Тунелювання заборонених протоколів через дозволені (DNS Tunneling, ICMP Tunneling), експлуатація вразливостей VPN-клієнтів.

1.3.2. Типові сценарії атак на банківські канали (TTPs)

Згідно з класифікацією MITRE ATT&CK (Tactics, Techniques, and Procedures), для мережевої інфраструктури найбільш критичними є наступні сценарії:

1. Network Sniffing & Eavesdropping (T1040). Зловмисник, отримавши доступ до сегмента мережі, використовує аналізатори трафіку (Wireshark, tcpdump) для перехоплення нешифрованих даних. У локальних мережах це часто реалізується через *ARP Cache Poisoning*, що змушує трафік жертви проходити через вузол зловмисника.
2. Man-in-the-Middle (MitM) та SSL Stripping (T1557). У цьому сценарії атакуючий не просто слухає, а активно втручається у з'єднання. Особливу небезпеку становлять атаки типу *SSL Stripping*, коли зловмисник примусово понижує рівень захищеності з'єднання з HTTPS до HTTP, що дозволяє перехоплювати дані у відкритому вигляді навіть при спробі встановити захищене з'єднання.
3. Lateral Movement (Горизонтальне переміщення) (T1021). Критичний сценарій для банків. Після компрометації одного малозначущого вузла (наприклад, ПК секретаря або принтера), зловмисник намагається просунутися до критичних сегментів (процесинг, SWIFT, бази даних). Відсутність внутрішньої сегментації та контролю міжсегментних потоків робить цю атаку можливою.
4. Експлуатація вразливостей VPN та віддаленого доступу (T1190). Враховуючи поширеність віддаленої роботи, VPN-шлюзи стають пріоритетною ціллю. Використання вразливостей типу CVE (Common Vulnerabilities and Exposures) у ПЗ шлюзів (наприклад, Pulse Secure, Fortinet, Cisco) дозволяє зловмисникам обійти аутентифікацію та отримати доступ до внутрішньої мережі з правами адміністратора.
5. Tunneling & Data Exfiltration (T1048). Для прихованого виведення вкрадених даних зловмисники інкапсулюють їх у легітимні протоколи, які

зазвичай не блокуються фаєрволами (DNS, ICMP, HTTPS). Це дозволяє обходити прості засоби DLP (Data Loss Prevention).

1.3.3. Вразливості, як передумови реалізації загроз

Успішність атак зазвичай зумовлена наявністю вразливостей трьох типів:

1. Вразливості конфігурації (Misconfiguration):
    - Використання налаштувань за замовчуванням (default passwords).
    - Дозвільні правила міжмережевого екранування (Any-Any).
    - Відкриті службові порти управління на зовнішніх інтерфейсах.
    - Відсутність Port Security на рівні доступу.
2. Вразливості протоколів та архітектури:
    - Використання застарілих версій протоколів шифрування (SSLv3, TLS 1.0/1.1), які мають відомі криптографічні вади.
    - Передача даних у відкритому вигляді (Telnet, HTTP, FTP).
    - «Пласка» архітектура мережі без виділення зон безпеки (DMZ).
3. Вразливості програмного забезпечення:
    - Відсутність актуальних оновлень (патчів) безпеки на мережевому обладнанні (RouterOS, Cisco IOS, Linux-based systems).
    - Наявність «бегдорів» або недокументованих можливостей у прошивках.

Узагальнюючи, можна стверджувати, що сучасний ландшафт загроз вимагає переходу від периметрального захисту до моделі Zero Trust, де мережевий канал вважається скомпрометованим за замовчуванням, а кожна транзакція вимагає верифікації.

1.4. Методологічні підходи та стандарти захисту мережевих каналів

1.4.1. Родина міжнародних стандартів ISO/IEC 27000

Методологічною основою для побудови системи захисту мережевих каналів виступає серія стандартів ISO/IEC, яка забезпечує комплексний підхід до управління інформаційною безпекою (ISMS).

- ISO/IEC 27001:2022 – є базовим стандартом, що визначає вимоги до ISMS. У контексті мережевої безпеки критично важливим є Додаток А (Annex A), який містить контролі: *A.8.20 (Network Security)*, що вимагає встановлення механізмів управління мережею та відокремлення інформаційних сервісів. *A.8.22 (Segregation of Networks)*, що регламентує поділ мережі на логічні домени (VLAN, DMZ) з різними рівнями довіри.
- ISO/IEC 27033 (Information technology – Network security) – це спеціалізований стандарт, який є ключовим для даного дослідження, оскільки деталізує архітектуру захищених комунікацій:
  - *Part 1 (Overview and concepts)* визначає фундаментальні принципи «глибокого захисту» (Defense in Depth) стосовно мережевої інфраструктури.
  - *Part 2 (Guidelines for the design and implementation)* описує методологію проєктування захищених шлюзів та зон.
  - *Part 3 (Reference networking scenarios):* розглядає типові загрози для різних сценаріїв підключення (інтернет, партнери).
  - *Part 4 (Securing communications between networks)* фокусується на застосуванні міжмережевих екранів (Firewalls) та систем виявлення вторгнень (IDS/IPS).
  - *Part 5 (Securing communications across networks using VPNs)* надає вичерпні рекомендації щодо вибору протоколів тунелювання (IPsec, SSL/TLS), методів автентифікації вузлів та управління ключами шифрування, що безпосередньо стосується практичної частини даної роботи.

1.4.2. Методологія NIST (Cybersecurity Framework та SP-серія)

Національний інститут стандартів і технологій США (NIST) пропонує найбільш прикладну методологічну базу, яка де-факто є стандартом для банківського сектору.

NIST Cybersecurity Framework (CSF) 2.0 Це рамкова структура, яка дозволяє інтегрувати захист каналів у загальну стратегію кіберстійкості організації через шість ключових функцій (Рис.1.2):

1. Govern (Управління) – визначення політик шифрування та допустимого використання каналів.
2. Identify (Ідентифікація) – повна інвентаризація фізичних та логічних каналів, визначення потоків даних (Data Flow Mapping).
3. Protect (Захист) – впровадження технологій шифрування (VPN), сегментації та контролю доступу (NAC).
4. Detect (Виявлення) – моніторинг аномалій у трафіку за допомогою NDR (Network Detection and Response) та аналізу NetFlow.
5. Respond (Реагування) – автоматичне блокування підозрілих сесій на рівні шлюзів.
6. Recover (Відновлення) – забезпечення резервних каналів зв’язку (Redundancy) для швидкого відновлення доступності.

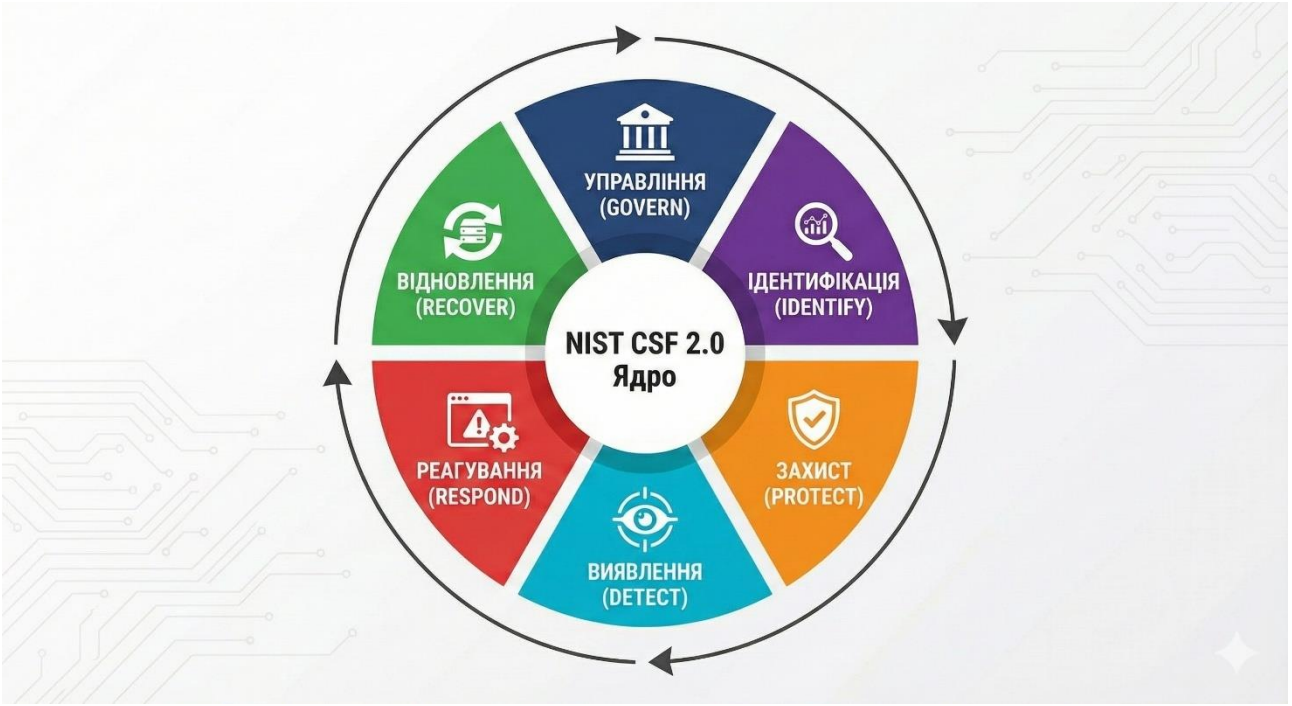


Рис. 1.2. Основні функції (ядро) структури кібербезпеки NIST CSF 2.0.

Спеціальні публікації (NIST Special Publications) Для технічної реалізації захисту мережевих каналів використовуються наступні керівництва:

- NIST SP 800-77 (Guide to IPsec VPNs) є основним документом для налаштування IPsec. Він визначає архітектуру безпеки ESP (Encapsulating Security Payload) та AH (Authentication Header), а також рекомендації щодо криптостійкості алгоритмів (наприклад, відмова від DES/3DES на користь AES-GCM).
- NIST SP 800-52 Rev. 2 (Guidelines for TLS) регламентує використання протоколу TLS для захисту каналів прикладного рівня, вимагаючи використання версій TLS 1.2 або 1.3 та забороняючи слабкі набори шифрів (Cipher Suites).
- NIST SP 800-41 Rev. 1 (Guidelines on Firewalls and Firewalls Policy) описує типи міжмережевих екранів та кращі практики створення правил фільтрації (принцип «Deny All» за замовчуванням).
- NIST SP 800-207 (Zero Trust Architecture) визначає перехід від традиційного захисту периметра до архітектури нульової довіри, де будь-який мережевий канал вважається ворожим, а кожен запит на доступ вимагає динамічної верифікації, незалежно від розташування користувача.

1.4.3. Практичне застосування стандартів у роботі

У рамках даної магістерської дисертації наведений комплекс стандартів використовується для:

1. Обґрунтування вибору протоколів VPN (на базі рекомендацій NIST SP 800-77).
2. Розробки схеми сегментації мережі банку (відповідно до ISO/IEC 27033-2 та Annex A ISO 27001).
3. Формування вимог до налаштування криптографічних параметрів тунелів.

1.5. Технічні засоби та механізми захисту мережевих каналів

1.5.1. Криптографічні протоколи та управління ключами

Фундаментом безпеки мережевих каналів є криптографічний захист, що забезпечує конфіденційність та цілісність . Залежно від рівня моделі OSI використовуються різні стеки протоколів.

IPsec (Internet Protocol Security, L3) стандарт для побудови Site-to-Site VPN. Згідно з рекомендаціями NIST SP 800-77, у банківських мережах доцільно використовувати режим ESP (Encapsulating Security Payload) у тунельному режимі, що шифрує як корисне навантаження, так і оригінальний IP-заголовок. Для забезпечення криптостійкості використовуються алгоритми AES-256-GCM або ChaCha20-Poly1305.

TLS (Transport Layer Security, L4/L7) використовується для захисту клієнтських підключень (Remote Access) та захисту API. Критично важливим є примусове використання версій TLS 1.2 або 1.3 із налаштованою властивістю Perfect Forward Secrecy (PFS), що гарантує неможливість розшифрування перехопленого трафіку навіть у разі компрометації довгострокового ключа сервера в майбутньому.

WireGuard (Modern L3 VPN) – це перспективний протокол, інтегрований у ядро Linux (починаючи з версії 5.6). Його перевагами перед IPsec є менша кодова база (~4000 рядків коду, що спрощує аудит), використання сучасної криптографії (Curve25519 для обміну ключами, BLAKE2s для хешування) та висока продуктивність. У роботі цей протокол розглядається як ефективна альтернатива для побудови внутрішніх тунелів між Linux-серверами.

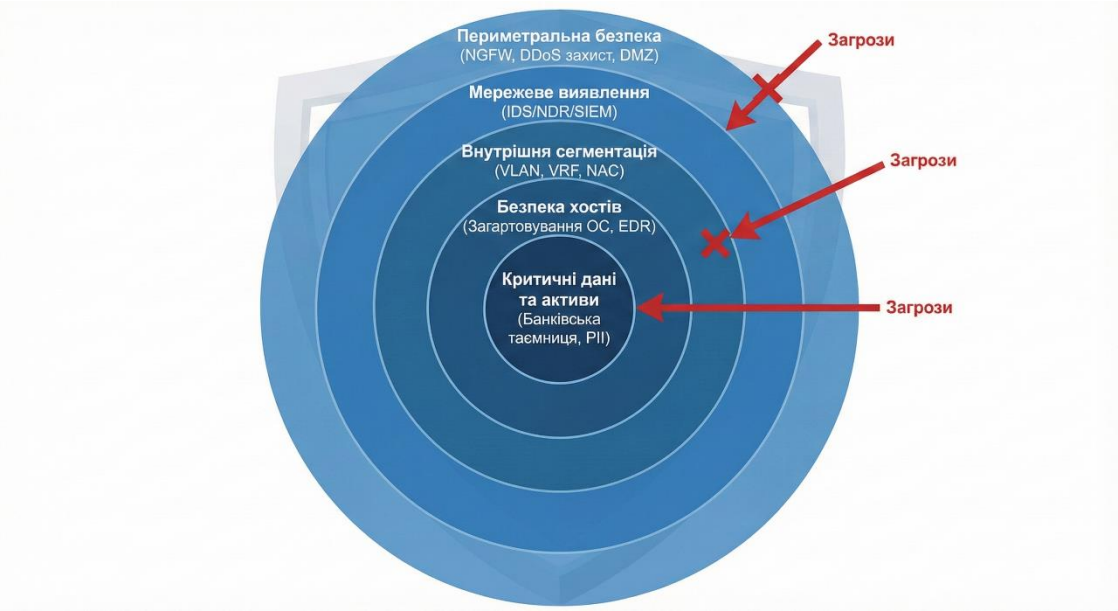


Рис. 1.3. Реалізація концепції глибокого захисту (Defense-in-Depth) в мережевій інфраструктурі.

1.5.2. Міжмережеве екранування та сегментація (Firewalling)

Фільтрація трафіку реалізується на кількох рівнях захисту. Базовий рівень, що реалізується на мережевому обладнанні або засобами ОС Linux (iptables, nftables) забезпечується за допомогою Packet Filtering (Stateless/Stateful). Він же й дозволяє Дозволяє фільтрувати трафік за IP-адресами та портами.

NGFW (Next-Generation Firewall) забезпечує глибоку інспекцію пакетів (DPI), дозволяючи ідентифікувати додатки (L7 Visibility) незалежно від порту, блокувати тунельований трафік та застосовувати політики на рівні користувачів, а не IP-адрес.

WAF (Web Application Firewall) – компонент для захисту DMZ, де розміщені веб-сервіси банку. WAF аналізує HTTP/HTTPS-трафік на предмет специфічних патернів атак (SQL Injection, XSS), які невидимі для звичайних фаєрволів.

Сегментація мережі (відповідно до ISO/IEC 27001 A.8.22) реалізується шляхом створення ізольованих VLAN та зон безпеки (Management, Server, User, Guest), взаємодія між якими суворо регламентована (принцип **Zero Trust**: «ніколи не довіряй, завжди перевіряй»).

1.5.3. Системи виявлення вторгнень та моніторингу (IDS/IPS/NDR)

Для активної протидії атакам та розслідування інцидентів використовуються системи аналізу трафіку:

1. IDS/IPS (Suricata) – здатна працювати в режимі пасивного моніторингу (IDS) або активного блокування (IPS in-line). Suricata використовує мультипотокову архітектуру та підтримує стандартні набори сигнатур (ET Open/Pro), а також розпізнавання протоколів.
2. Network Security Monitoring (Zeek/Bro). На відміну від сигнатурних IDS, Zeek фокусується на поведінковому аналізі та вилученні метаданих. Він генерує деталізовані логи транзакцій (conn.log, http.log, ssl.log), які є незамінними для Threat Hunting – пошуку прихованих загроз, що обійшли сигнатурний захист.
3. NDR (Network Detection and Response) – більш сучасний клас рішень, що використовує методи машинного навчання (ML) для виявлення аномалій у поведінці хостів (наприклад, нетиповий обсяг передачі даних або підключення до нових зовнішніх серверів), що часто свідчить про активність шкідливого ПЗ або інсайдера.

1.5.4. Централізація подій (SIEM) та організаційні заходи

Технічні засоби генерують великий обсяг логів, які необхідно агрегувати та корелювати. Для цього використовуються SIEM-системи (наприклад, ELK Stack, Splunk, Wazuh), що забезпечують централізоване зберігання подій безпеки, як того вимагає стандарт PCI DSS (вимога 10).

Організаційна складова захисту включає:

- Розробку та затвердження Політики мережевої безпеки.
- Впровадження процедури управління змінами (Change Management) – будь-які зміни в правилах фаєрволів мають бути авторизовані та протестовані.

- Регулярне проведення тестів на проникнення (Penetration Testing) та сканування вразливостей згідно з рекомендаціями NIST SP 800-115.

1.6. Особливості реалізації системи захисту мережевих каналів на базі ОС Linux

Операційна система Linux є де-факто промисловим стандартом для побудови захищених корпоративних шлюзів, маршрутизаторів та систем виявлення вторгнень. Її вибір для банківської інфраструктури обумовлений відкритістю вихідного коду (можливість аудиту безпеки), підтримкою сучасних криптографічних примітивів на рівні ядра та відповідністю вимогам регуляторів (зокрема, щодо відсутності «закладок»).

1.6.1. Архітектура мережевого стеку: Netfilter та eBPF

Основою мережевої безпеки Linux є підсистема ядра, яка еволюціонувала від простих фільтрів до програмованих інтерфейсів.

- Netfilter/nftables – це класичний фреймворк для фільтрації пакетів, трансляції адрес (NAT) та маніпуляцій із заголовками. На відміну від застарілого iptables, сучасний nftables використовує власну віртуальну машину в ядрі (bytecode interpretation), що дозволяє обробляти пакети швидше за рахунок атомарного завантаження правил та зменшення перемикань контексту між простором користувача та простором ядра.
- eBPF (Extended Berkeley Packet Filter) та XDP (eXpress Data Path) – новітня технологія, що дозволяє запускати безпечні, верифіковані програми безпосередньо в контексті ядра мережевого драйвера. XDP дозволяє відкидати шкідливі пакети (наприклад, під час DDoS-атак) ще до того, як операційна система витратить ресурси на їх обробку стеком TCP/IP. Для високошвидкісних банківських каналів (10G/40G) це єдина технологія, здатна забезпечити фільтрацію без втрати продуктивності.

1.6.2. Linux як платформа для криптографічних шлюзів (VPN)

Реалізація захищених каналів у Linux базується на взаємодії простору ядра (Kernel Space) та простору користувача (User Space). У Linux реалізація IPsec розділена: обробка шифрованих пакетів (ESP/AH) відбувається безпосередньо в ядрі (що забезпечує високу швидкість), тоді як управління ключами та узгодження параметрів (IKEv2) виконується демонами у просторі користувача, такими як strongSwan або Libreswan. Це дозволяє гнучко налаштовувати політики безпеки згідно з NIST SP 800-77.

На відміну від IPsec, WireGuard працює як модуль ядра (починаючи з версії 5.6), що мінімізує накладні витрати на перемикання контексту. Він використовує сучасну криптографію (Noise Protocol Framework) і в контексті Linux-шлюзів демонструє меншу затримку (latency), що критично для транзакційних систем.

1.6.3. Інтеграція засобів аналізу трафіку (IDS/IPS)

Linux надає унікальні механізми для інтеграції систем глибокого аналізу пакетів (DPI):

- NFQUEUE (Netfilter Queue) – механізм, що дозволяє передавати пакети з ядра до простору користувача для аналізу системою Suricata або Snort. Якщо Suricata працює в режимі IPS (запобігання), вона виносить вердикт (DROP/ACCEPT), і ядро виконує цю дію.
- AF_PACKET / PF_RING – дві технології захоплення трафіку (Zero Copy), які дозволяють системам моніторингу типу Zeek або Wazuh аналізувати копію трафіку на швидкостях лінії без впливу на основний потік даних.

1.6.4. Загартовування (Hardening) ОС для відповідності стандартам

Впровадження операційної системи Linux у банківську інфраструктуру вимагає обов’язкового застосування процедур загартовування (Hardening) для забезпечення повної відповідності галузевим стандартам CIS Benchmarks та міжнародному стандарту ISO 27001. Цей процес передбачає глибоке налаштування параметрів ядра через механізм sysctl, що включає деактивацію

ICMP redirects та source routing, а також активацію фільтра rp_filter для надійного захисту від атак із підміною IP-адрес.

Важливим елементом архітектури безпеки є використання систем примусового контролю доступу (MAC), таких як SELinux або AppArmor, які дозволяють жорстко обмежити права процесів, гарантуючи, наприклад, доступ VPN-сервісів лише до власних ключів та мережевих інтерфейсів без права доступу до системних директорій. Загальна стійкість системи посилюється шляхом мінімізації поверхні атаки, що досягається використанням вузькоспеціалізованих дистрибутивів, таких як Alpine Linux чи VyOS, або впровадженням технологій контейнеризації Docker для логічної ізоляції окремих сервісів безпеки.

Висновки до розділу 1

У першому розділі магістерської дисертації узагальнено теоретичні підходи, нормативно-правові вимоги та практичні технологічні засоби, що застосовуються для захисту мережевих каналів передачі конфіденційних даних у корпоративних мережах банківських установ. Отримані результати дозволяють окреслити ключові орієнтири, на яких має базуватися подальше проєктування системи захисту.

Зміна ролі мережевої інфраструктури та зростання її критичності. Встановлено, що корпоративні мережі банків еволюціонували від локальних і відносно простих схем до розподілених інфраструктур, які охоплюють кілька майданчиків та поєднують сегменти LAN/MAN/WAN. У такому середовищі “мережевий канал” слід розглядати не лише як фізичну лінію зв’язку, а як сукупність обладнання, протоколів і механізмів маршрутизації та керування трафіком. Показано, що для сценаріїв Site-to-Site, Remote Access і Host-to-Host базовим інструментом побудови довірених з’єднань залишаються VPN-рішення, які забезпечують захищений обмін даними через недовірені мережі.

Нормативні вимоги та базова модель безпеки. Аналіз регуляторної і стандартної бази підтвердив, що для фінансового сектору захист інформації має не рекомендаційний, а обов’язковий характер. Дотримання вимог НБУ (зокрема Постанови №95), стандартів ISO/IEC 27000 та PCI DSS визначає мінімально допустимий рівень організаційних і технічних контролів. Встановлено, що в основі побудови захисту залишається тріада CIA (конфіденційність, цілісність, доступність), а найбільш практичною реалізацією є підхід Defense-in-Depth. Окремо підкреслено важливість сегментації, DMZ та контролю міжсегментної взаємодії як необхідних умов для обмеження поширення інцидентів усередині мережі.

Ландшафт загроз і пріоритетні сценарії атак. Розгляд загроз із застосуванням підходів STRIDE та MITRE ATT&CK показав, що ризики для мережевих каналів формуються як зовнішніми, так і внутрішніми джерелами. Відповідно, виключно периметральна модель захисту є недостатньою. До

найбільш критичних для банківських мереж сценаріїв віднесено Man-in-the-Middle, SSL Stripping, тунелювання/екфільтрацію даних, а також горизонтальне переміщення зловмисника в мережі. Це обґрунтовує доцільність переходу до принципів Zero Trust, де кожне з'єднання та кожна транзакція розглядаються як такі, що потребують перевірки.

Технологічні засоби захисту каналів. Встановлено, що основою захисту мережевих каналів є криптографічні протоколи та механізми керування ключами.

- IPsec залишається поширеним і практичним стандартом для міжофісних тунелів (L3) з прогнозованою стабільністю та сумісністю.
- TLS 1.2/1.3 є ключовим механізмом захисту клієнтських підключень та прикладної взаємодії (включно з API).
- WireGuard визначено перспективним рішенням для реалізації VPN на базі Linux завдяки простішій архітектурі, сучасним криптографічним примітивам (Curve25519, ChaCha20-Poly1305) та високій продуктивності.

Також показано, що криптографії недостатньо без постійного контролю та реакції. Тому в технологічний контур мають входити NGFW/WAF для фільтрації та інспекції трафіку, а також IDS/IPS (наприклад, Suricata) і рішення класу NDR для виявлення аномалій та підтримки реагування.

Linux як платформа для побудови захищених мережевих вузлів. Доведено доцільність використання Linux у ролі мережевого шлюзу/концентратора захищених каналів. Перевагою є гнучкість і можливість детального контролю трафіку завдяки Netfilter/nftables, а також перспективам використання eBPF для моніторингу та безпекових сценаріїв. Відкритий код створює передумови для незалежного аудиту, що є важливим у банківському середовищі. Водночас застосування Linux потребує обов'язкового hardening за практиками на кшталт CIS Benchmarks: мінімізація ПЗ, налаштування параметрів ядра, використання SELinux/AppArmor, контроль сервісів і прав доступу.

Отримані результати підтверджують, що захист мережевих каналів у корпоративній мережі банку має будуватися як системна комбінація: виконання

регуляторних вимог, використання сучасних криптографічних протоколів та впровадження засобів моніторингу й активної протидії. Обґрунтовано необхідність відмови від застарілих рішень і протоколів (SSL, WEP, DES) на користь сучасних стандартів, рекомендованих провідними практиками та профільними організаціями. Таким чином, теоретична база першого розділу створює підґрунтя для подальшої розробки програмно-визначеної системи захисту мережевих каналів на базі ОС Linux, що буде деталізовано в наступних розділах роботи.

РОЗДІЛ 2. АНАЛІЗ КОРПОРАТИВНОЇ МЕРЕЖІ, МОДЕЛЬ ЗАГРОЗ ТА ПОСТАНОВКА ЗАДАЧІ ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ МЕРЕЖЕВИХ КАНАЛІВ НА БАЗІ ОС LINUX

Метою цього розділу є детальний аналіз архітектури типової корпоративної мережі банківської установи для визначення об’єкта захисту, ідентифікації потенційних векторів атак та формулювання вимог до системи захисту мережевих каналів.

Описана нижче інфраструктура відображає індустріальні стандарти побудови мереж у фінансовому секторі, що характеризуються високими вимогами до відмовостійкості, сегментації трафіку та відповідності регуляторним нормам (наприклад, PCI DSS, вимогам НБУ). Архітектура є географічно розподіленою, гетерогенною та включає критичні сегменти обробки платіжної інформації, зони взаємодії із зовнішніми клієнтами та адміністративні контури.

2.1.1. Логічна структура корпоративної мережі

Сучасна банківська мережа є складною ієрархічною системою, побудованою за модульним принципом. Логічна структура забезпечує ізоляцію процесів обробки даних різного рівня конфіденційності та критичності (Рис. 2.1.).

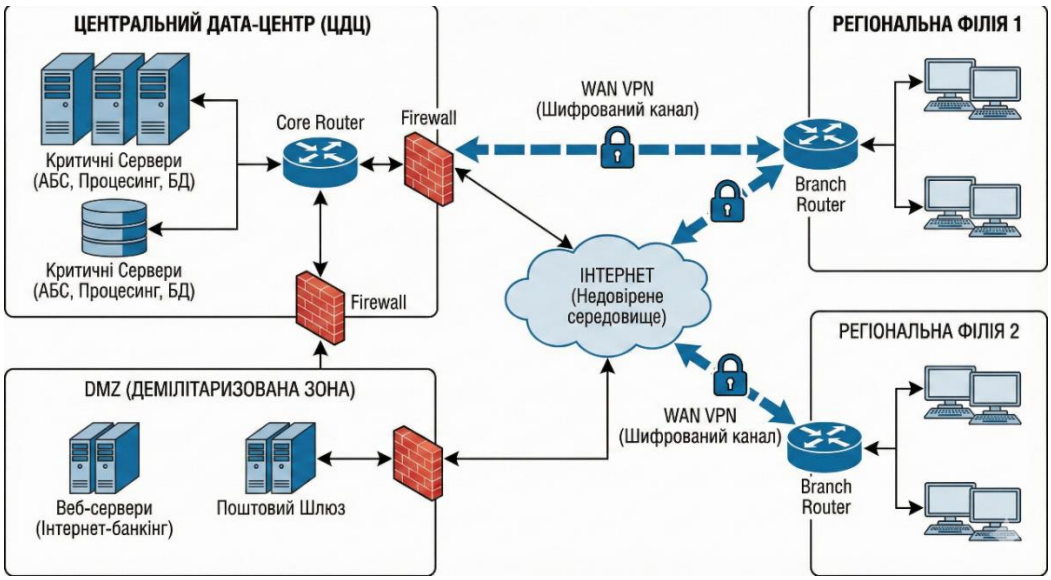


Рис. 2.1. Типова логічна архітектура корпоративної мережі банківської установи.

Центральний дата-центр (ЦДЦ) – Ядро мережі. ЦДЦ є головним технологічним майданчиком, де консолідуються основні обчислювальні потужності та зберігаються критичні дані банку. Цей сегмент вимагає найвищого рівня захисту та фізичної безпеки. До його складу входять:

- Сервери критичних бізнес-додатків, автоматизована банківська система (АБС), CRM-системи, процесингові центри для обробки карткових транзакцій, шлюзи до міжнародних платіжних систем (SWIFT, Visa/Mastercard). Тут обробляються дані, що становлять банківську таємницю.
- Інфраструктурні сервіси, серед яких контролери домену (Active Directory/LDAP), DNS/DHCP сервери, системи віртуалізації, файлові сховища та системи централізованого резервного копіювання (Backup & Restore).
- Системи централізованого збору логів (SIEM), платформи моніторингу продуктивності мережі та додатків (NMS/APM), сервери управління конфігураціями.
- Ядро мережевої безпеки – високопродуктивні міжмережеві екрани наступного покоління (NGFW) у кластерній конфігурації, системи

запобігання вторгненням (IPS), аналізатори мережевого трафіку (NDR) та центральні VPN-концентратори для термінації тунелів від філій.

Регіональні підрозділи (філії та відділення) – мережа відділень, що характеризується великою кількістю територіально віддалених точок присутності з меншим рівнем довіри до локального середовища порівняно з ЦДЦ. Типове відділення включає:

- Сегмент користувачів фронт-офісу: Робочі станції співробітників, що потребують доступу до АБС та CRM у ЦДЦ для обслуговування клієнтів.
- Сегмент пристроїв самообслуговування: Банкомати (ATM) та платіжні термінали (ПТКС). Цей сегмент є критичним з точки зору фізичної безпеки та ризиків підключення неавторизованих пристроїв, тому він часто ізолюється в окремий VLAN/VRF.
- Локальний мережевий вузол: Комутаційне обладнання та прикордонний маршрутизатор (або пристрій класу UTM/SD-WAN Edge). Його основна функція — забезпечення захищеного каналу зв'язку (Site-to-Site VPN) з ЦДЦ через недовірені транспортні мережі (Інтернет або MPLS канали провайдерів). Весь трафік від відділення до ЦДЦ має бути обов'язково шифрованим.

Демілітаризована зона (DMZ) – буферна зона. DMZ є контрольованим буферним сегментом між внутрішньою довіреною мережею банку (LAN) та зовнішнім недовіреним середовищем (Інтернет). Вона призначена для розміщення сервісів, доступних для зовнішніх користувачів та партнерів, мінімізуючи ризик прямого доступу до внутрішніх ресурсів у разі компрометації публічного сервісу. У DMZ розміщуються:

- Фронтенд-сервери систем дистанційного банківського обслуговування (ДБО): Веб-сервери Інтернет-банкінгу та сайти банку.
- Шлюзи для обслуговування запитів від мобільних додатків клієнтів та Open Banking API для партнерів.

- Сервери для фільтрації вхідної та вихідної електронної пошти перед її передачею на внутрішні поштові сервери.
- Точки взаємодії з зовнішніми кредитними бюро, державними реєстрами (наприклад, Дія) та іншими фінтех-сервісами.

Архітектурно DMZ зазвичай реалізується з використанням двох ешелонів міжмережевих екранів (зовнішній та внутрішній периметр), що дозволяє створити глибокоешелонований захист і суворо контролювати потоки трафіку між Інтернетом, DMZ та внутрішньою мережею.

2.2. Виділення критичних сегментів та каналів передачі даних

Побудова ефективної системи захисту вимагає диференціації активів мережі за ступенем їх критичності. З точки зору забезпечення безпеки мережевої взаємодії, не всі канали зв'язку потребують однакових механізмів захисту. Для мінімізації накладних витрат на шифрування та фільтрацію трафіку необхідно чітко окреслити периметр критичних сегментів.

Класифікація сегментів та каналів у даній роботі базується на оцінці потенційних збитків від порушення властивостей інформації (модель CIA):

- Конфіденційність: Ризик витоку персональних даних клієнтів (PII), даних платіжних карток (PCI DSS) та комерційної таємниці.
- Цілісність: Ризик несанкціонованої модифікації фінансових транзакцій або налаштувань систем.
- Доступність: Ризик блокування роботи бізнес-сервісів внаслідок DDoS-атак або логічних збоїв.

На основі аналізу бізнес-процесів банку виділено п'ять критичних зон, канали зв'язку з якими потребують пріоритетного захисту, наведених у таблиці 2.1:

Табл. 2.1 критичні зони та вимоги до їх захисту

Критична зона	**Характеристика трафіку**	**Рівень критичності та ризики**	**Вимоги до захисту**
Сегмент процесингу та АБС (Core Banking Zone)	Високоінтенсивний обмін даними між серверами застосунків та базами даних.	Найвища. Ризик прямих фінансових розкрадань та порушення цілісності балансів.	Сувора ізоляція, повне логування сесій, запобігання атакам типу MitM.
Ідентифікація та управління доступом (IAM)	Автентифікаційні дані: хеші паролів, Kerberos-тікети, запити на авторизацію.	Висока. Ризики атак "pass-the-hash" та горизонтального переміщення (lateral movement) мережею.	Необхідність захисту від перехоплення трафіку в сегменті.
Адміністративне керування (Management Plane)	Протоколи віддаленого управління: SSH, RDP, HTTPS, SNMP.	Критична. Загроза отримання повного контролю над інфраструктурою у разі перехоплення сесії.	Виділені VPN-тунелі для адміністраторів, використання 2FA.
Транспортні канали "Філія – ЦДЦ"	Мішаний трафік: дані клієнтів, внутрішній документообіг, IP-телефонія.	Висока. Вразливість до перехоплення та підміни через використання недовіреного середовища WAN.	Обов'язкове шифрування всього потоку даних та забезпечення їх цілісності.

Шлюзи DMZ <-> Internal	Запити від веб-застосунків до внутрішніх ресурсів через суворо визначені порти.	Висока. Основний вектор зовнішніх атак; ризик проникнення у внутрішню мережу через веб-сервер.	Запобігання створенню прямих тунелів у внутрішню мережу при компрометації DMZ.

2.3. Модель порушника та ідентифікація векторів атак на мережеві канали

Побудова ефективної системи захисту вимагає чіткого визначення моделі порушника – формалізованого опису потенційного зловмисника, його технічних можливостей, рівня доступу до системи та мотивації. Для проєктування захищених каналів зв'язку на базі ОС Linux у банківському секторі, модель порушника базується на припущенні, що канал передачі даних апріорі є ворожим середовищем (Рис. 2.2).

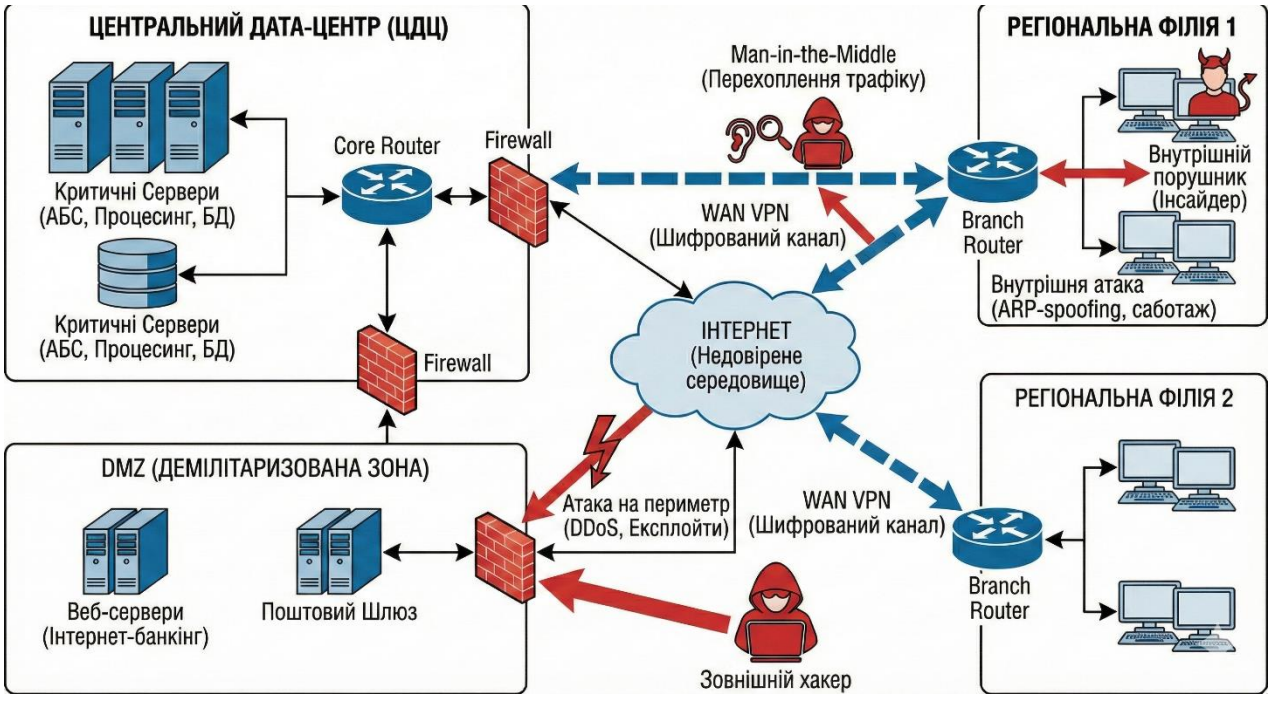


Рис. 2.2. Візуалізація основних векторів атак на мережеві канали банку.

2.3.1. Класифікація порушників та їх можливостей

У рамках даної роботи порушники класифікуються за рівнем доступу до мережевої інфраструктури (Location) та рівнем знань про систему (Knowledge).

Зовнішній порушник (Internet Attacker) діє із глобальної мережі без авторизованого доступу, володіючи рівнем знань «чорної скриньки» лише про публічні IP-адреси та відкриті порти. Основними векторами його атак є сканування периметра, експлуатація відомих вразливостей (CVE) у вебсерверах чи VPN-шлюзах, DDoS-атаки та спроби підбору паролів, а головною метою – проникнення в DMZ для подальшого просування вглиб банківської мережі.

Порушник на каналі передачі даних (Man-in-the-Middle) діє на транспортному рівні (наприклад, недобросовісний персонал провайдера чи оператор транзитного вузла), маючи частковий доступ до заголовків пакетів та характеристик трафіку. Загрози включають сніфінг незашифрованого трафіку, активні MitM-атаки, повторне відтворення пакетів та ін'єкції шкідливого коду в HTTP-сесії, що робить протидію цьому класу порушників пріоритетним завданням при проєктуванні VPN-каналів.

Внутрішній порушник – Адміністратор (High-Privilege Insider) має повний доступ до конфігурацій мережевого обладнання та серверів Linux, володіючи рівнем знань «білої скриньки» про топологію, паролі та ключі шифрування. Його вектори атак охоплюють модифікацію маршрутизації, вимкнення логування та створення прихованих тунелів для витоку даних, що потребує впровадження жорстких організаційних заходів та принципу розділення обов'язків для контролю його дій.

Компрометований довірений вузол (Compromised Endpoint) – легітимний пристрій співробітника або підрядника, заражений шкідливим програмним забезпеченням (Malware/Botnet). Головна небезпека цього класу полягає в можливості автоматизованого збору даних та використанні вже встановленого VPN-тунелю для здійснення атак на центральний дата-центр безпосередньо «зсередини» захищеного каналу.

Для наочності характеристики порушників зведено у Таблицю 2.2:

Табл. 2.2 – Матриця характеристик порушників

Тип порушника	**Місце дії**	**Основна мотивація**	**Ключова загроза для каналів**
Зовнішній	Інтернет (WAN)	Фінансова вигода, кіберхуліганство	DDoS, експлуатація вразливостей VPN-шлюзу
MITM (Провайдер)	Транзитна мережа	Промислове шпигунство, збір даних	Перехоплення даних, аналіз трафіку, підміна пакетів
Внутрішній	LAN (Філія/ЦДЦ)	Помста, фінансова вигода (інсайд)	ARP-spoofing, несанкціонований доступ

2.3.2. Формалізація моделей загроз для ключових каналів передачі даних

Базуючись на визначеній моделі порушника та архітектурі мережі, проведено декомпозицію загроз для критичних каналів зв'язку. Для систематизації векторів атак використано підхід, заснований на класифікації STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Аналіз проведено для трьох основних сценаріїв взаємодії.

Канали зв'язку «Філія – ЦДЦ» (Site-to-Site VPN), що функціонують у режимі 24/7, піддаються загрозам розкриття конфіденційності через пасивне перехоплення (sniffing) у разі використання слабких алгоритмів шифрування або через аналіз метаданих трафіку для вивчення бізнес-активності банку . Порушення цілісності (tampering) у таких каналах реалізується через ін’єкцію підроблених пакетів для розсинхронізації сесій або проведення атак повторного відтворення (replay attacks) зашифрованих фрагментів даних для дублювання транзакцій . Крім того, критичною є загроза відмови в обслуговуванні (DoS), що досягається вичерпанням ресурсів VPN-шлюзу шляхом масованого надсилання запитів на ініціалізацію з’єднань.

Адміністративні канали керування (Management Plane: SSH, VPN) є

найбільш критичним вектором, де загроза підміни особи (spoofing) реалізується через brute-force підбір паролів або викрадення приватних ключів адміністратора за допомогою шкідливого ПЗ . Атаки типу «людина посередині» (MitM) стають можливими при перехопленні процесу встановлення сесії, якщо не враховуються попередження про зміну цифрових відбитків сервера . Найбільш небезпечним сценарієм є ескалація привілеїв (elevation of privilege) шляхом експлуатації вразливостей у застарілому серверному ПЗ, що надає зловмиснику повний контроль над системою захисту.

Канали віддаленого доступу користувачів (Remote Access VPN), що часто базуються на особистих пристроях (BYOD), створюють ризики тунелювання атак, де заражений комп’ютер використовується як транспорт для проникнення Malware у внутрішню мережу банку в обхід периметрових екранів . Використання розділеного тунелювання (split tunneling) дозволяє зловмиснику атакувати пристрій через відкритий Інтернет і використовувати його як проміжний вузол (jump host) для доступу до корпоративних ресурсів . Додатково загрозу становить фішинг облікових даних, спрямований на отримання паролів та OTP-кодів через підроблені інтерфейси входу для несанкціонованої авторизації під виглядом легітимного персоналу.

Для наочності основні загрози та їх потенційний вплив на бізнес зведено у таблицю 2.3:

Таблиця 2.3 – Матриця загроз та їх впливу

Вектор атаки	**Об'єкт атаки**	**Порушена властивість (CIA)**	**Рівень ризику**
Сніфінг трафіку	Канал "Філія-ЦДЦ"	Конфіденційність	Критичний
Brute-force SSH	Адмін-доступ	Конфіденційність / Цілісність	Високий
DDoS на шлюз	VPN-концентратор	Доступність	Високий
Replay Attack	Протокол обміну	Цілісність	Середній

Malware через VPN	Remote Access	Цілісність внутрішньої мережі	Високий

2.4. Аналіз ефективності існуючих засобів захисту та ідентифікація недоліків

Для визначення вектору проєктування було проведено аналіз типової моделі захисту банківської мережі, що базується на традиційних апаратних рішеннях та орендованих каналах зв'язку.

Станом на момент дослідження, базовий профіль захисту (As-Is) характеризується наступними параметрами:

- Використання апаратних міжмережевих екранів (Firewalls) на межі ЦДЦ.
- Довіра до технології MPLS L3VPN від провайдера як основного засобу ізоляції трафіку філій.
- Фрагментарне використання IPsec-тунелів на застарілому обладнанні (SOHO-роутери) для малих точок присутності.
- Базове журналювання подій (Syslog) без централізованої кореляції.

У ході аналізу цієї архітектури виявлено ряд системних недоліків, які унеможливлюють забезпечення належного рівня безпеки в умовах сучасних кіберзагроз.

2.4.1. Критичні недоліки поточної архітектури

Проблема довіреного середовища (MPLS Security Fallacy) Покладання на безпеку каналів MPLS є концептуальною помилкою. Хоча MPLS забезпечує логічне розділення трафіку (Routing Isolation), дані в магістральній мережі провайдера передаються у відкритому вигляді (Clear Text).

Наслідок – високий ризик пасивного перехоплення (Sniffing) на транзитних вузлах або інсайдерами провайдера.

Відсутність криптографічної гнучкості (Lack of Crypto Agility) Існуюче апаратне забезпечення має жорстко зафіксовані (Hardcoded) набори криптографічних примітивів. Виявлено використання застарілих алгоритмів (3DES, SHA-1, DH Group 2), які визнані вразливими NIST.

Наслідок – неможливість швидкої заміни скомпрометованого алгоритму без заміни фізичного обладнання. Відсутність підтримки Perfect Forward Secrecy (PFS) створює загрозу дешифрування історичного трафіку в разі викрадення ключів.

Розмитий периметр та слабка сегментація Внутрішній трафік VPN-каналів сприймається системою як "довірений". Відсутність інспекції (Deep Packet Inspection) всередині тунелів призводить до того, що скомпрометована філія стає плацдармом для атак на ЦДЦ.

Наслідок – ризик реалізації атак типу Lateral Movement (горизонтальне переміщення) без спрацювання систем захисту периметра.

"Клаптева" керованість (Configuration Drift) – налаштування обладнання виконується вручну ("точково"), що призводить до десинхронізації політик безпеки. Відсутня єдина точка правди (Source of Truth) щодо конфігурацій доступу.

Наслідок – людський фактор стає основною причиною появи "дірок" у безпеці та застарілих правил доступу (Shadow Rules).

2.4.2. Обґрунтування переходу на Software-Defined Security (Linux)

Для усунення виявлених недоліків доцільно перейти від апаратно-центричної моделі до програмно-визначеної (Software-Defined) на базі ОС Linux. Порівняльний аналіз підходів наведено в таблиці 2.4.

Таблиця 2.4 – Порівняльний аналіз підходів до побудови VPN-мереж

Критерій порівняння	**Традиційний підхід (Proprietary Hardware)**	**Пропонований підхід (Linux-based SDS)**
Довіра до коду	Низька ("Чорна скринька", закритий код)	Висока (Open Source, можливість аудиту)
Адаптивність	Низька (залежність від прошивок вендора)	Висока (модульна архітектура, швидкі патчі)
Криптографія	Обмежений набір (IPsec legacy)	Підтримка сучасних стандартів (WireGuard, TLS 1.3, IKEv2)

Вартість масштабування	Висока (ліцензії за тунелі/швидкість)	Низька (обмежена лише CPU сервера)
Інтеграція з SIEM	Обмежена (стандартний Syslog)	Повна (можливість кастомних агентів збору логів)

2.5. Постановка задачі на проєктування системи захисту мережевих каналів

На основі проведеного аналізу архітектури корпоративної мережі, моделей загроз та недоліків існуючих рішень, виникає необхідність розробки нової системи захисту. Оскільки апаратна модернізація є економічно недоцільною, приймається рішення про проєктування програмно-визначеної системи (Software-Defined Security) на базі ОС Linux.

У цьому підрозділі формулюються технічні вимоги до проєктованої системи та конкретний перелік задач, що будуть вирішені в практичній частині роботи.

2.5.1. Функціональні вимоги до системи захисту

Проєктована система повинна вирішувати проблему захисту даних при їх передачі через недовірені канали зв'язку (Інтернет) та забезпечувати наступні характеристики:

1. Конфіденційність даних (Confidentiality):
   - Весь трафік між філіями та центральним офісом повинен інкапсулюватися в захищені тунелі.
   - Використання сучасних криптостійких алгоритмів шифрування (наприклад, ChaCha20-Poly1305 або AES-256-GCM).
   - Забезпечення досконалої прямої секретності (Perfect Forward Secrecy - PFS) для захисту від дешифрування "заднім числом".
2. Цілісність та автентичність (Integrity & Authenticity):
   - Захист від модифікації пакетів у дорозі (HMAC або AEAD).

- Сувора взаємна автентифікація вузлів (Mutual Authentication) на основі криптографічних ключів або сертифікатів, щоб унеможливити підключення неавторизованих пристроїв.

3. Мережева сегментація (Segmentation):
   - Реалізація політик фільтрації (Firewalling) безпосередньо на точках термінації тунелів.
   - Блокування прямого доступу філій до критичних сегментів ЦДЦ за принципом "Zero Trust" (дозволено тільки те, що явно необхідно для роботи).
4. Спостережуваність (Observability):
   - Система повинна генерувати детальні логи подій (підключення, помилки автентифікації, спроби сканування).
   - Можливість інтеграції з системами збору метрик для моніторингу стану каналів у реальному часі.

2.5.2. Етапи та задачі практичної реалізації

Для досягнення відповідності сформульованим вимогам, у третьому розділі роботи необхідно вирішити наступні інженерні задачі:

Задача 1. Розробка топології захищеної накладеної мережі (Overlay Network). Спроєктувати логічну схему мережі за топологією "Hub-and-Spoke" (Зірка), де Linux-сервер у ЦДЦ виступає концентратором. Розробити план IP-адресації для тунельних інтерфейсів, щоб уникнути конфліктів з існуючими локальними мережами.

Задача 2. Обґрунтування та налаштування технологічного стека Linux. Вибрати оптимальний VPN-протокол (порівняння WireGuard та IPsec/IKEv2) з точки зору продуктивності та простоти конфігурації. Налаштувати мережевий стек Linux (sysctl forwarding) та базове зміцнення ОС (OS Hardening) для роботи в якості шлюзу безпеки.

Задача 3. Реалізація механізмів управління трафіком та доступом. Розробити та впровадити набір правил міжмережевого екрану (використовуючи nftables або iptables), що дозволяють трафік лише визначених бізнес-додатків.

Налаштувати маршрутизацію трафіку між тунелями та внутрішньою мережею (NAT/Masquerading при необхідності).

Задача 4. Побудова системи моніторингу та діагностики. Розгорнути засоби локального логування активності VPN-сервісу. Реалізувати скрипти або агенти для перевірки доступності тунелів (Keepalive checks) та сповіщення про збої.

Задача 5. Верифікація ефективності розробленого рішення. Створити тестовий стенд для емуляції роботи "Центр – Філія". Провести імітацію атаки "Man-in-the-Middle" (перехоплення трафіку) для підтвердження надійності шифрування. Виміряти вплив впровадженого шифрування на пропускну здатність каналу та затримки (Latency) за допомогою утиліт навантажувального тестування (наприклад, iperf3).

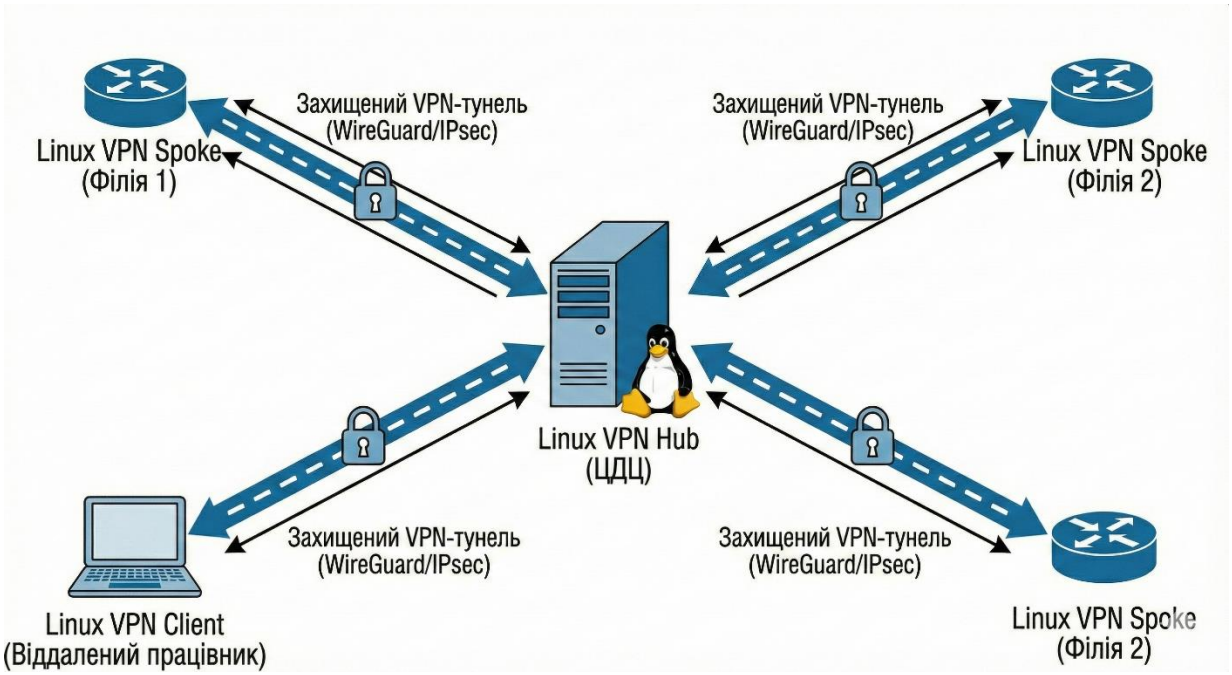


Рис. 2.3. Цільова топологія захищеної накладеної мережі (Hub-and-Spoke).

Вирішення цих задач дозволить отримати робочий прототип програмного маршрутизатора на базі Linux, готовий до інтеграції в корпоративну інфраструктуру банку.

Висновок до розділу 2

У другому розділі магістерської дисертації здійснено комплексний

системний аналіз об’єкта захисту – корпоративної мережі банківської установи. Проведено ідентифікацію критичних сегментів і каналів передачі даних, розроблено модель порушника та систематизовано вектори атак, актуальні для розподілених мережевих інфраструктур. На основі виявлених недоліків існуючих підходів сформульовано вимоги та здійснено постановку задачі на проєктування системи захисту мережевих каналів на базі операційної системи Linux.

Результати проведеного дослідження дозволяють зробити наступні висновки:

1. Архітектурний аналіз та категоризація критичних активів. Встановлено, що сучасна корпоративна мережа банку є гетерогенною, географічно розподіленою системою, функціонування якої регламентується жорсткими нормативними вимогами та необхідністю забезпечення безперервності бізнес-процесів. Логічна структура мережі декомпозована на три базові компоненти: Центральний дата-центр (ЦДЦ) як ядро системи, мережу регіональних філій (периферія) та демілітаризовану зону (DMZ) для взаємодії із зовнішнім середовищем. На основі моделі CIA (Confidentiality, Integrity, Availability) проведено категоризацію сегментів мережі. Визначено п’ять зон пріоритетної критичності, серед яких транспортні канали типу «Філія – ЦДЦ» (Site-to-Site VPN) ідентифіковано як найбільш вразливий елемент архітектури. Це зумовлено поєднанням двох факторів: передачею значних обсягів бізнес-критичної інформації (банківська таємниця, персональні дані) та використанням для транзиту недовіреного середовища (публічні мережі або інфраструктура провайдерів), що створює системні передумови для реалізації кібератак.

2. Моделювання загроз та векторів атак. Розроблена модель порушника враховує специфіку банківських мереж, що характеризується наявністю як зовнішньої, так і внутрішньої поверхні атаки, а також ризиками на рівні транспортної інфраструктури. Узагальнено три категорії порушників: зовнішній (Internet Attacker), внутрішній (Insider) та порушник на каналі зв’язку (Man-in-the-Middle). Прийнято засадниче припущення, що будь-який канал зв’язку за

межами контрольованого фізичного периметра слід розглядати як вороже середовище. Із застосуванням методології STRIDE систематизовано актуальні загрози, серед яких для каналів «Філія – ЦДЦ» критичними визначено: пасивне перехоплення (Sniffing), порушення цілісності та ін’єкцію пакетів (Tampering), атаки повторного відтворення (Replay Attacks) та відмову в обслуговуванні (DoS). Для каналів адміністративного керування додатковими критичними векторами є компрометація автентифікаційних даних та ескалація привілеїв.

3. Оцінка ефективності існуючих рішень (модель «As-Is»). Аналіз поточного стану захисту виявив низку системних обмежень традиційних підходів, що базуються на використанні орендованих MPLS-каналів та пропрієтарного апаратного забезпечення. Зокрема, ідентифіковано проблему «ілюзії безпеки MPLS», коли логічна ізоляція маршрутів помилково ототожнюється з конфіденційністю даних. Встановлено недостатню криптографічну гнучкість (Crypto Agility) застарілого обладнання, що ускладнює оперативну заміну скомпрометованих алгоритмів. Відсутність механізмів Perfect Forward Secrecy створює загрозу ретроспективного дешифрування трафіку. Окрім того, виявлено ризики горизонтального переміщення зловмисників (Lateral Movement) через відсутність глибокої інспекції трафіку на точках термінації тунелів, а також проблему неузгодженості конфігурацій (Configuration Drift) внаслідок ручного керування політиками безпеки.

4. Обґрунтування переходу до Software-Defined Security (SDS). Доведено доцільність впровадження програмно-визначеної системи захисту мережевих каналів на базі ОС Linux. Такий підхід забезпечує прозорість та можливість аудиту коду (Open Source), високу адаптивність до нових загроз завдяки швидкому оновленню криптографічного стека, а також необмежену масштабованість без ліцензійних бар’єрів. Визначено, що концепція SDS дозволяє інтегрувати механізми захисту (шифрування, фільтрацію, моніторинг) у єдиний керований контур, забезпечуючи перехід від статичного захисту периметра до динамічної моделі з безперервним контролем стану та автоматизацією процесів.

5. Постановка задачі на проєктування. Сформульовано технічні вимоги до проєктованої системи, які включають забезпечення конфіденційності, цілісності, суворої взаємної автентифікації вузлів, реалізацію принципу найменших привілеїв (Zero Trust) через мережеву сегментацію, а також забезпечення спостережуваності та керованості інфраструктури. Для досягнення мети роботи визначено перелік інженерних задач, що підлягають вирішенню у наступному розділі:

1. Розробка топології накладеної мережі (Overlay Network) за архітектурою «Hub-and-Spoke».
2. Обґрунтування вибору та налаштування VPN-протоколу (порівняльний аналіз WireGuard та IPsec/IKEv2).
3. Реалізація політик міжмережевого екранування (nftables) для контролю доступу.
4. Впровадження засобів моніторингу та діагностики стану тунелів.
5. Верифікація ефективності розробленого рішення шляхом моделювання атак та проведення навантажувального тестування.

РОЗДІЛ 3.ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ МЕРЕЖЕВИХ КАНАЛІВ ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ НА БАЗІ ОС LINUX

3.1. Формулювання вимог до системи захисту

Базуючись на результатах аналізу загроз та недоліків існуючої інфраструктури (Розділ 2), визначено, що проєктована система (далі — ПС) повинна являти собою програмно-апаратний комплекс на базі ОС Linux, що виконує функції криптографічного шлюзу, міжмережевого екрану та сенсора безпеки.

Вимоги до системи класифіковано за трьома групами: функціональні вимоги безпеки, вимоги до спостережуваності та нефункціональні вимоги (продуктивність і відмовостійкість).

3.1.1. Функціональні вимоги безпеки

Система повинна забезпечувати реалізацію наступних функцій захисту інформації:

1. Конфіденційність та цілісність каналів зв'язку (Confidentiality & Integrity)

- Криптографічні стандарти: Використання виключно сучасних алгоритмів шифрування з автентифікацією даних (AEAD), таких як ChaCha20-Poly1305 або AES-256-GCM.
- Forward Secrecy (PFS): Обов'язкова підтримка досконалої прямої секретності (наприклад, через обмін ключами ECDHE), що гарантує неможливість розшифрування перехопленого трафіку навіть у разі компрометації довгострокових ключів у майбутньому.
- Мультипротокольна підтримка: Здатність одночасно обслуговувати різні типи тунелів на одному логічному інтерфейсі:
    - *Site-to-Site:* Для постійного з'єднання філій з ЦДЦ (рекомендовано WireGuard або IPsec IKEv2).
    - *Remote Access:* Для підключення мобільних користувачів та адміністраторів.

2. Сувора автентифікація суб'єктів (Strong Authentication)

- Mutual Authentication (mTLS/PSK): Використання взаємної автентифікації, де і клієнт (філія), і сервер (ЦДЦ) перевіряють цифрові сертифікати або криптографічні ключі один одного перед встановленням з'єднання.
- Захист від неавторизованих пристроїв: Блокування будь-яких спроб з'єднання від хостів, чиї публічні ключі не внесені до білого списку (Allowlist) на стороні сервера.

3. Сегментація та фільтрація трафіку (Access Control & Filtering)

- Stateful Inspection: Реалізація міжмережевого екрану з контролем стану з'єднань (за допомогою підсистеми nftables ядра Linux). Система повинна відстежувати стани NEW, ESTABLISHED, RELATED та INVALID.
- Принцип найменших привілеїв (PoLP): Заборона проходження будь-якого транзитного трафіку між тунелями за замовчуванням (Default Drop). Дозвіл надається виключно для конкретних пар IP-адрес та портів, необхідних для бізнес-процесів (наприклад, Філія А -> АБС:443).
- Ізоляція підмереж: Блокування прямого доступу філій до сегменту управління (Management VLAN) та інших філій (Spoke-to-Spoke), якщо це не передбачено технологічною необхідністю.

3.1.2. Вимоги до аудиту та спостережуваності

Для забезпечення можливості розслідування інцидентів та оперативного реагування система повинна:

1. Журналювання подій безпеки (Security Logging)

- Реєструвати події встановлення та розриву тунелів (Handshake success/failure) із зазначенням часової мітки, IP-адреси ініціатора та ідентифікатора ключа.
- Фіксувати факти відхилення пакетів фаєрволом (Dropped packets) з деталізацією (src/dst IP, proto, port).
- Забезпечувати сумісність форматів логів (JSON або Syslog RFC 5424) для автоматизованої передачі в SIEM-систему (наприклад, ELK Stack або Splunk).

2. Моніторинг стану (Health Monitoring)

- Надавати метрики в реальному часі: статус інтерфейсів, обсяг трафіку (rx/tx bytes), затримка (latency) в тунелі, час останнього успішного рукостискання (Latest Handshake).
- Підтримувати інтеграцію з системами моніторингу (Zabbix, Prometheus) через експортери або SNMP-агенти.

3.1.3. Нефункціональні вимоги

1. Продуктивність (Performance)
   - Впровадження засобів шифрування не повинно призводити до деградації пропускної здатності каналу більше ніж на 15-20% порівняно з "чистим" каналом (overhead).
   - Мінімальний вплив на затримку (Jitter/Latency), що критично для роботи VDI (Virtual Desktop Infrastructure) та IP-телефонії.
2. Відмовостійкість (Reliability)
   - Система повинна підтримувати механізми швидкого відновлення з'єднання (Dead Peer Detection - DPD) у разі короткочасних збоїв провайдера.
   - Можливість роботи в режимі кластера (High Availability) з використанням протоколів VRRP (Keepalived) для забезпечення безперервності сервісу при виході з ладу одного з фізичних серверів (опціонально для ЦДЦ).
3. Сумісність та масштабованість
   - Можливість розгортання на стандартному x86-сумісному обладнанні.
   - Підтримка автоматизованого управління конфігураціями (Configuration Management) для швидкого підключення нових філій без ручного налаштування кожного параметра**.**

3.1.2. Нефункціональні вимоги та експлуатаційні характеристики

Окрім безпосередніх функцій захисту, проєктуєма система повинна відповідати ряду якісних характеристик, що гарантують її стабільну роботу в критичній інфраструктурі банку.

1. Надійність та забезпечення безперервності бізнесу (Reliability & Business Continuity) Враховуючи вимоги до доступності банківських сервісів (SLA 99.9% і вище), система повинна забезпечувати:

- Високу доступність (High Availability - HA): Підтримка кластеризації шлюзів у режимі *Active/Standby* або *Active/Active* з використанням протоколів VRRP (Virtual Router Redundancy Protocol) або CARP. Час перемикання на резервний вузол не повинен перевищувати критичний поріг розриву TCP-сесій (зазвичай < 3 секунд).
- Механізми самовідновлення (Self-Healing): Автоматичний перезапуск служб VPN та фаєрвола у разі програмних збоїв (через systemd watchdogs).
- Детекцію "мертвих" сусідів (Dead Peer Detection - DPD): Налаштування тайм-аутів для оперативного виявлення втрати зв'язку з протилежною стороною тунелю та ініціації перепідключення.

2. Продуктивність та ефективність використання ресурсів Впровадження засобів криптографічного захисту не повинно створювати "вузьких місць" (bottlenecks) у мережевій інфраструктурі.

- Апаратна акселерація: Обов'язкове використання інструкцій процесора AES-NI або AVX-512 для прискорення симетричного шифрування, що дозволяє обробляти гігабітні потоки даних з мінімальним навантаженням на CPU.
- Оптимізація TCP/IP стека: Налаштування параметрів ядра Linux (sysctl) для роботи з високошвидкісними з'єднаннями (збільшення розмірів буферів TCP window scaling, черг backlog).
- Масштабованість (Scalability): Архітектура повинна допускати горизонтальне масштабування — збільшення пропускної здатності шляхом додавання нових шлюзів та балансування навантаження (Load Balancing) без зміни логіки роботи клієнтів.

3. Керованість та експлуатаційна придатність (Maintainability) Система повинна підтримувати парадигму Infrastructure as Code (IaC):

- Версіонування конфігурацій: Усі налаштування (правила nftables, конфіги WireGuard/IPsec) повинні зберігатися у вигляді текстових файлів з можливістю відстеження змін через систему контролю версій (Git).
- Модульність: Розділення логіки налаштування інтерфейсів, маршрутизації та політик безпеки для спрощення аудиту та внесення змін.
- Документованість процедур: Наявність регламентів (Runbooks) для типових операцій: ротація ключів, додавання нової філії, оновлення ядра ОС та патчинг безпеки.

4. Відповідність регуляторним нормам (Compliance) Проєктоване рішення повинно задовольняти вимогам національних та міжнародних стандартів:

- ISO/IEC 27001 (Annex A.13.1): Забезпечення безпеки мережевої інфраструктури та захисту інформації в мережах.
- Постанови НБУ №95 (щодо захисту інформації в банківській системі): В частині використання надійних алгоритмів шифрування та забезпечення цілісності каналів зв'язку.

3.2. Обґрунтування вибору ОС Linux як технологічної платформи

Вибір операційної системи є стратегічним рішенням, що впливає на вартість володіння (TCO), рівень безпеки та гнучкість майбутньої системи. У даній роботі проведено порівняльний аналіз трьох основних підходів: використання апаратних комплексів (Proprietary Appliances), рішень на базі Windows Server та рішень на базі Open Source (Linux/*BSD).

3.2.1. Переваги використання Linux для задач мережевої безпеки

Вибір ОС Linux (ядро версії 5.10 LTS або новіше) як базової платформи зумовлений наступними факторами:

1. Прозорість та довіра (Security through Transparency) На відміну від пропрієтарних рішень ("Black Box"), де замовник змушений довіряти вендору на слово, відкритий вихідний код Linux дозволяє:

- Проводити незалежний аудит реалізації криптографічних примітивів та мережевого стека.

- Мінімізувати ризики наявності недокументованих можливостей ("бекдорів"), що є критичним для фінансових установ державного значення.
- Використовувати перевірені світовою спільнотою реалізації протоколів (OpenSSL, strongSwan, WireGuard), які проходять регулярні перевірки безпеки.

2. Технологічна незалежність (Vendor Independence) Використання Linux дозволяє уникнути жорсткої прив'язки до апаратного забезпечення конкретного виробника (Vendor Lock-in).

- Апаратна гнучкість: Система може бути розгорнута на серверному обладнанні будь-якого вендора (HPE, Dell, Lenovo), на недорогих міні-ПК для малих філій або у віртуальному середовищі (VMware, KVM).
- Уніфікація середовища: Можливість використання єдиної ОС для фізичних серверів, хмарних інстансів та контейнерів спрощує адміністрування.

3. Потужний інтегрований мережевий стек Сучасне ядро Linux містить вбудовані засоби, що за функціональністю не поступаються, а часто й перевершують комерційні аналоги:

- Netfilter/nftables: Потужний фреймворк для класифікації пакетів, NAT та фільтрації трафіку, що працює на рівні ядра (Kernel Space), забезпечуючи мінімальні затримки.
- XFRM framework: Вбудована в ядро підтримка IPsec, що дозволяє виконувати шифрування/дешифрування пакетів без їх переміщення в простір користувача (User Space), що значно підвищує продуктивність.
- WireGuard: Сучасний VPN-протокол, інтегрований безпосередньо в ядро Linux (починаючи з версії 5.6), що забезпечує меншу поверхню атаки порівняно зі старими протоколами завдяки компактній кодовій базі.

4. Економічна ефективність (Cost Efficiency) Відсутність ліцензійних відрахувань за кількість VPN-тунелів, кількість ядер процесора або пропускну здатність дозволяє суттєво знизити операційні витрати (OPEX),

перенаправляючи бюджет на закупівлю більш надійного апаратного забезпечення або навчання персоналу (табл. 3.1).

Табл. 3.1 – Порівняльна характеристика платформ для побудови VPN-шлюзу

Характеристика	**Апаратний NGFW (Cisco/Fortinet)**	**Windows Server (RRAS)**	**Linux (Open Source)**
Вартість ліцензій	Висока (підписка)	Середня (CALs)	Відсутня (Free)
Доступ до коду	Закритий	Закритий	Відкритий
Гнучкість налаштувань	Обмежена CLI/GUI	Середня	Необмежена
Підтримка WireGuard	Обмежена/Відсутня	Стороння	Нативна (Kernel)
Автоматизація (DevOps)	Специфічна для вендора	PowerShell	Ansible/Bash/Terraform

3.2.2. Архітектурні особливості підсистеми Netfilter та перехід до nftables

Основою реалізації функцій міжмережевого екранування в ОС Linux є фреймворк Netfilter, що забезпечує перехоплення та маніпуляцію пакетами на різних етапах проходження через мережевий стек ядра. Традиційним інструментом керування Netfilter протягом десятиліть був iptables, проте в рамках даної роботи для реалізації фільтрації обрано сучасну підсистему nftables. Вибір nftables обумовлений наступними архітектурними перевагами:

1. Висока продуктивність класифікації: На відміну від iptables, що використовує лінійний пошук правил (O(n)), nftables підтримує структури даних типу "множини" (sets) та "словники" (maps). Це дозволяє перевіряти приналежність IP-адреси до списку з тисяч записів за фіксований час (O(1)), що критично для високонавантажених шлюзів.
2. Атомарність змін: Оновлення правил у nftables відбувається транзакційно. Це виключає ситуації, коли під час завантаження нових політик шлюз на частки секунди залишається незахищеним або перебуває у невизначеному стані.

3. Уніфікація синтаксису: Єдина утиліта nft замінює набір розрізнених інструментів (iptables, ip6tables, arptables, ebtables), спрощуючи адміністрування dual-stack мереж (IPv4/IPv6).
4. Програмованість: nftables використовує власну віртуальну машину (BVF) всередині ядра, що дозволяє завантажувати складніші правила фільтрації без необхідності перекомпіляції модулів ядра.

3.2.3. Аналіз ризиків використання Open Source рішень

Впровадження системи на базі відкритого ПЗ (OSS) вимагає врахування специфічних експлуатаційних ризиків, які відсутні або мінімізовані в комерційних продуктах (COTS). У таблиці 3.2 наведено ідентифіковані ризики та стратегії їх мінімізації**.**

Табл. 3.2 – Ризики впровадження Linux-шлюзів та контрзаходи

Категорія ризику	**Опис проблеми**	**Стратегія мінімізації (Mitigation)**
Операційний	Відсутність SLA від вендора. Відповідальність за працездатність повністю лягає на штатних адміністраторів.	Впровадження резервування (HA Cluster). Наявність детальної документації (Disaster Recovery Plan).
Кадровий	Високий поріг входження. Адміністратори, які звикли до GUI, можуть не впоратися з CLI/config-файлами.	Використання систем управління конфігураціями (Ansible) для автоматизації. Розробка внутрішніх інструкцій.
Управління змінами	Ризик "Configuration Drift" — неконтрольовані ручні зміни на серверах призводять до хаосу.	Принцип "Infrastructure as Code": заборона ручних змін, всі налаштування через Git-репозиторій.

3.3. Обґрунтування вибору технологічного стека

Для побудови захищених каналів зв'язку проведено порівняльний аналіз трьох найбільш поширених VPN-протоколів: IPsec (IKEv2), OpenVPN та WireGuard.

3.3.1. Порівняльний аналіз VPN-протоколів

1. IPsec (на базі strongSwan/Libreswan)

- Архітектура: Індустріальний стандарт, що працює на мережевому рівні (L3) моделі OSI.
- Переваги: Нативна підтримка всіма сучасними ОС (Windows, macOS, iOS, Android) без встановлення стороннього ПЗ. Повна сумісність з апаратним обладнанням (Cisco, Fortinet) для побудови Site-to-Site тунелів.
- Недоліки: Висока складність конфігурації (безліч параметрів фаз IKE), проблеми з проходженням через NAT, "важкий" код.

2. OpenVPN

- Архітектура: Протокол рівня додатків (User Space), що використовує SSL/TLS для захисту даних.
- Переваги: Надзвичайна гнучкість, можливість роботи через TCP (порт 443), що дозволяє обходити суворі фаєрволи та проксі-сервери. Широкі можливості автентифікації (LDAP, RADIUS).
- Недоліки: Низька продуктивність порівняно з аналогами через постійне перемикання контексту між простором користувача та ядром (Context Switching).

3. WireGuard

- Архітектура: Новітній протокол, інтегрований безпосередньо в ядро Linux (Kernel Space). Використовує сучасну криптографію (Noise Protocol Framework, Curve25519, ChaCha20-Poly1305).
- Переваги: Мінімальна кодова база (~4000 рядків), що спрощує аудит. Найвища пропускна здатність та найменша затримка (Ping) серед конкурентів. Миттєве перемикання між мережами (Roaming).
- Недоліки: Відсутність гнучкої системи розподілу ключів "з коробки" (вимагає зовнішніх інструментів управління для великих мереж).

Висновок щодо вибору: Для реалізації системи обрано гібридний підхід:

1. WireGuard – як основний протокол для каналів "Філія – ЦДЦ" (Site-to-Site) через його високу продуктивність та стабільність на Linux-каналах.
2. IPsec (IKEv2) – як резервний варіант для підключення мобільних клієнтів (Remote Access), оскільки він підтримується смартфонами нативно.

3.3.2. Вибір засобів фільтрації та моніторингу

Засіб фільтрації: На основі аналізу в п. 3.2.2, для реалізації міжмережевого екрану обрано nftables. Це забезпечить можливість створення єдиних, структурованих правил фільтрації, що легко читаються та масштабуються.

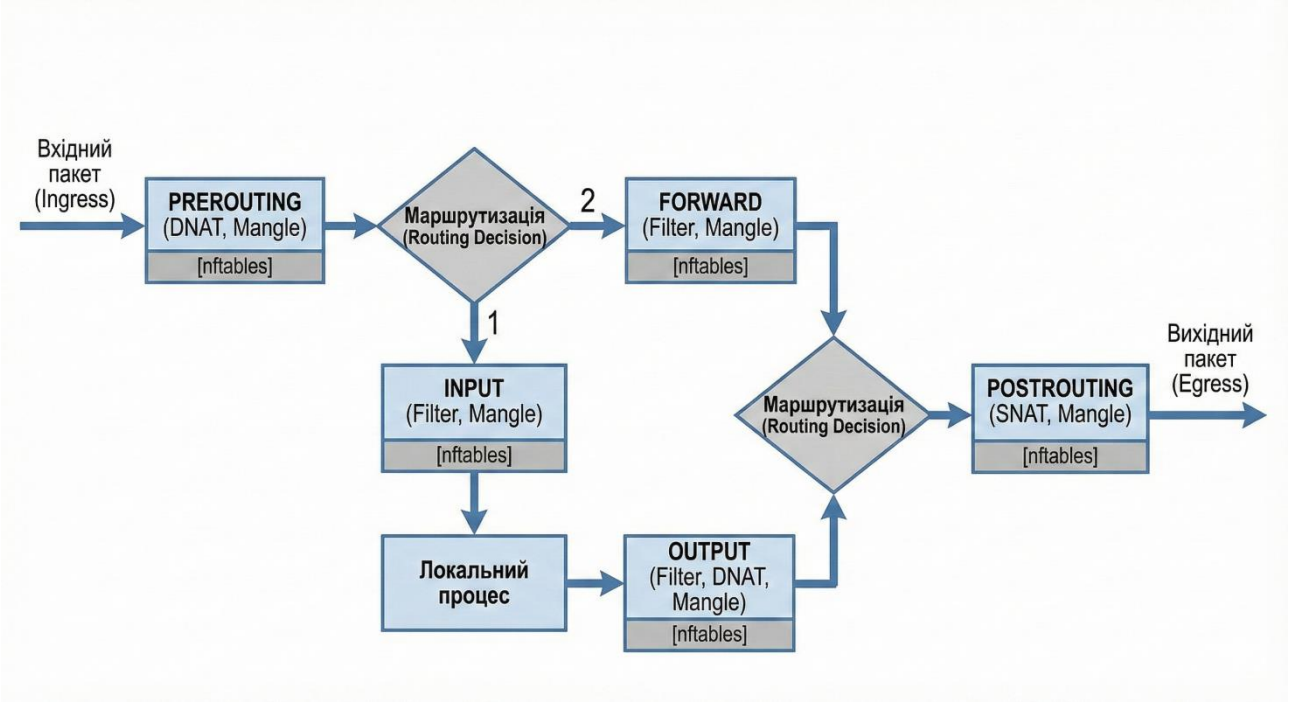


Рис. 3.1. Схема обробки пакетів у ядрі Linux з використанням підсистеми nftables.

Засоби моніторингу та детекції загроз: Для забезпечення спостережуваності (Observability) пропонується дворівнева схема:

1. Рівень метрик (Performance Monitoring): Використання Prometheus Node Exporter для збору технічних метрик (CPU, Bandwidth, WG peers status).

2. Рівень подій безпеки (Security Logging): Централізований збір логів (syslog-ng) з подальшою передачею в SIEM.
3. Аналіз трафіку (NTA): У якості сенсора для виявлення аномалій та сигнатурного аналізу атак обрано Suricata (у режимі IDS), що працює паралельно з VPN-процесами, аналізуючи розшифрований трафік на внутрішніх інтерфейсах шлюзу.

3.4. Цільова архітектура системи захисту

На основі сформульованих вимог та обраних технологій розроблено цільову архітектуру системи захисту, яка базується на топології "Hub-and-Spoke" (Зірка) (Рис. 3.2).

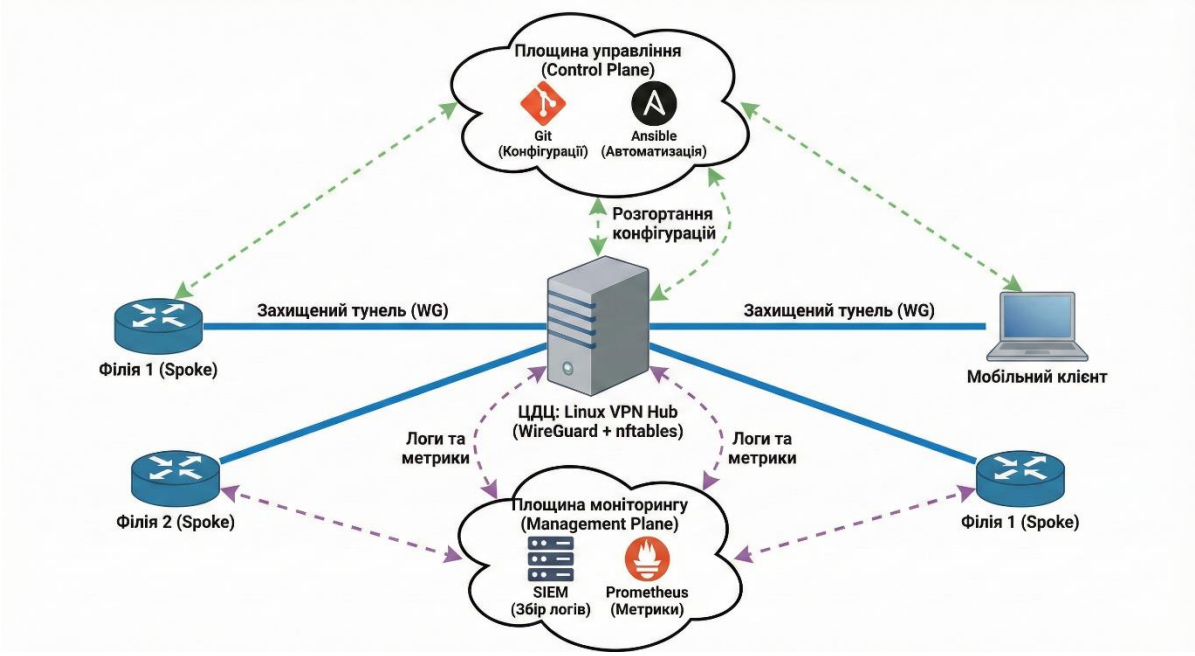


Рис. 3.2. Цільова архітектура програмно-визначеної VPN-мережі із розділенням на функціональні площини.

Система складається з трьох логічних площин (Planes):

1. Площина даних (Data Plane) Відповідає за безпосередню передачу користувацького трафіку.

- Центральний вузол (Hub): Високопродуктивний сервер у ЦДЦ під управлінням Linux, на якому термінуються всі VPN-тунелі. Він виступає шлюзом до внутрішніх ресурсів (АБС, CRM).
- Периферійні вузли (Spokes): Linux-шлюзи (або мікрокомп'ютери) у філіях, що інкапсулюють весь трафік локальної мережі у WireGuard-тунель.
- Ізоляція: Кожна філія має власний віртуальний інтерфейс на Hub-сервері, що дозволяє застосовувати індивідуальні правила фаєрволу.

2. Площина управління (Control Plane) Забезпечує налаштування та розповсюдження ключів.

- Використання системи управління конфігураціями (Ansible) для автоматизованого розгортання ключів WireGuard та правил nftables на всі вузли мережі.
- Зберігання еталонної конфігурації у приватному Git-репозиторії.

3. Площина моніторингу (Management Plane) Забезпечує контроль стану системи.

- Центральний сервер моніторингу опитує шлюзи через захищений службовий канал.
- Логи подій безпеки (спроби підбору паролів, сканування портів) автоматично відправляються на сервер кореляції подій.

Така архітектура дозволяє досягти необхідного балансу між безпекою, керованістю та вартістю впровадження.

3.5. Проєктування схеми адресації та маршрутизації

Для коректного функціонування VPN-мережі та уникнення конфліктів IP-адрес розроблено план адресації з використанням приватних діапазонів згідно з RFC 1918 (Рис. 3.3.).

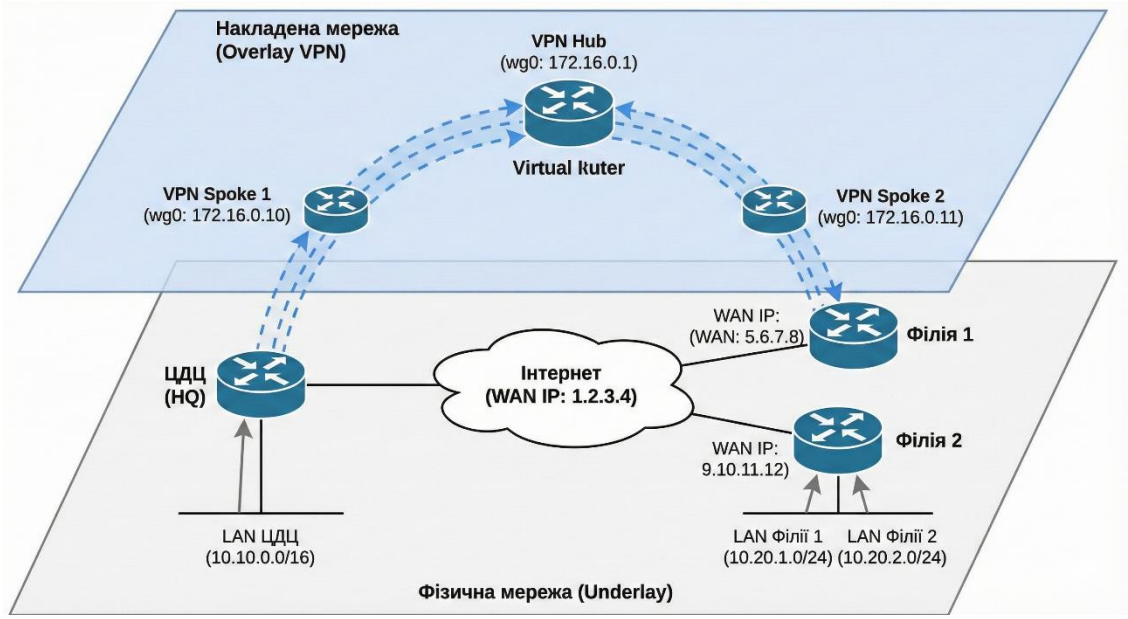


Рис. 3.3. Схема розподілу IP-адрес для накладеної (overlay) та фізичних мереж.

Використання чіткої ієрархічної структури IP-адрес спрощує налаштування правил фільтрації та маршрутизації.

1. **Внутрішня мережа ЦДЦ (HQ Network):**
   - Діапазон: 10.10.0.0/16
   - Серверний сегмент (АБС, CRM): 10.10.10.0/24
   - Сегмент адміністраторів: 10.10.99.0/24
2. **Транспортна мережа VPN (Overlay Network):**
   - Для тунельних інтерфейсів WireGuard виділено окрему підмережу, яка не перетинається з фізичними мережами.
   - Діапазон: 172.16.0.0/24
   - Адреса шлюзу ЦДЦ (Hub): 172.16.0.1/32
   - Адреси філій (Spokes): 172.16.0.10, 172.16.0.11 і т.д.
3. **Мережі філій (Branch Networks):**
   - Для кожної філії виділяється /24 підмережа на основі географічного або номерного ідентифікатора.
   - Філія 1: 10.20.1.0/24
   - Філія 2: 10.20.2.0/24

Такий розподіл дозволяє використовувати сумарні маршрути (Route Summarization). Наприклад, для доступу до *будь-якої* філії з центру достатньо одного маршруту 10.20.0.0/16 через VPN-інтерфейс, що зменшує таблицю маршрутизації.

3.6. Розробка матриці доступу (Firewall Policy Design)

Ключовим етапом проєктування системи захисту є формалізація правил розмежування доступу. Замість хаотичного додавання правил, сформовано Матрицю доступу, яка буде імплементована засобами nftables.

Система будується за принципом Default Drop (заборонено все, що не дозволено явно).

Таблиця 3.3 – Проєкт матриці доступу міжмережевого екрану

№ Правила	**Джерело (Source)**	**Призначення (Destination)**	**Сервіс / Порт**	**Дія**	**Опис**
1	Будь-яка Філія	ЦДЦ (VPN Hub)	UDP/51820	**ACCEPT**	Дозвіл встановлення WireGuard тунелю (Transport Layer)
2	Мережа Філії	Сервер АБС	TCP/443 (HTTPS)	**ACCEPT**	Доступ операціоністів до банківського ПЗ
3	Мережа Філії	Контролер домену	UDP/TCP 53, 88, 389	**ACCEPT**	DNS, Kerberos, LDAP (авторизація користувачів)
4	Мережа Філії	Інші Філії	Будь-який	**DROP**	Ізоляція філій (Spoke-to-Spoke communication blocked)
5	Адміністратор VPN	Мережеве обладнання	TCP/22 (SSH)	**ACCEPT**	Технічне управління

					інфраструктуро ю
6	Інтернет (Світ)	ЦДЦ (Internal)	Будь-який	**DROP**	Захист від зовнішніх атак через VPN-шлюз

Висновки до розділу 3

У третьому розділі магістерської дисертації розв’язано комплексне науково-прикладне завдання проєктування системи захисту мережевих каналів корпоративної мережі банківської установи. На відміну від традиційного підходу, що ґрунтується на використанні набору різнорідних апаратних засобів, у роботі сформовано архітектуру уніфікованого програмно-визначеного комплексу захисту (Software-Defined Security), реалізованого на базі операційної системи Linux. Запропоноване рішення поєднує криптографічний захист, сегментацію доступу та політико-орієнтоване керування мережевими потоками в єдиній керованій моделі, що підвищує відтворюваність, керованість і контрольованість безпеки в розподіленій інфраструктурі.

Отримані результати проєктування дозволяють сформулювати такі узагальнюючі висновки щодо якості, ефективності та елементів новизни запропонованого технічного рішення:

1. Переорієнтація на модель Zero Trust та мінімізація довіри до транспортного середовища. У процесі проєктування обґрунтовано відмову від суто «периметральної» логіки захисту на користь концепції Zero Trust Network Access (ZTNA). Встановлено, що в умовах використання публічних мереж як середовища передачі даних сам факт підняття VPN-тунелю не може розглядатися як достатня умова для надання широких повноважень у внутрішніх сегментах. Спроєктована система реалізує принцип логічної мікросегментації: кожне віддалене підключення трактується як окремий ізольований контур доступу, трафік якого підлягає обов’язковій фільтрації та верифікації на основі матриці дозволених

потоків. Такий підхід знижує ймовірність і потенційний масштаб горизонтального переміщення (Lateral Movement) у разі компрометації периферійного вузла або облікового запису, що є критично важливим для банківської інфраструктури.

2. Обґрунтування технологічного суверенітету, прозорості та керованості платформи.

   Вибір Linux як базової платформи для шлюзів безпеки здійснено на основі порівняльного аналізу з пропрієтарними апаратними рішеннями за критеріями керованості, контрольованості конфігурації, можливості аудиту та гнучкості масштабування. Використання відкритого коду підвищує прозорість реалізації механізмів захисту та спрощує незалежну верифікацію відсутності недокументованих функцій. Додатково Linux-підхід забезпечує апаратну незалежність (фізичні сервери x86/ARM, віртуалізація, хмарні середовища) без зміни концепції функціонування, що знижує ризики vendor lock-in і дає можливість оптимізувати витрати на розгортання та масштабування (CAPEX/OPEX) без втрати керованості.

3. Оптимізація криптографічного захисту на основі WireGuard як мінімалістичного та криптографічно актуального протоколу.
   За результатами порівняльного аналізу IPsec / OpenVPN / WireGuard за критеріями швидкодії, криптостійкості та складності підтримки обрано WireGuard як базовий протокол тунелювання. Переваги такого вибору полягають у наступному:
   - Зменшення поверхні атаки: компактна кодова база WireGuard суттєво спрощує аудит та зменшує ймовірність накопичення критичних дефектів у порівнянні з великими комплексними стеком.
   - Криптографічна актуальність: використання сучасних примітивів (зокрема Curve25519, ChaCha20, Poly1305) та жорстко визначених криптонаборів мінімізує ризики помилкових конфігурацій і сценаріїв downgrade.

- Продуктивність і стабільність: інтеграція на рівні ядра Linux знижує накладні витрати та підтримує високу пропускну здатність, що є принциповим для фінансових сервісів із чутливістю до затримок та втрат.

4. Ефективність підсистеми фільтрації та реалізація політики “Default Deny”. Для міжмережевого екранування обрано nftables як сучасну підсистему фільтрації, що забезпечує продуктивну обробку великих наборів правил за рахунок оптимізованих структур даних (множини/мапи) та ядрової логіки застосування політик. У межах проєктування сформовано матрицю доступу як формалізований перелік дозволених інформаційних потоків і сервісів. Реалізація принципу “заборонено все, що не дозволено явно” в ланцюжках вхідної та транзитної фільтрації створює послідовний бар’єр, який знижує результативність сканування, спроб несанкціонованого доступу та нецільових з’єднань до критичних сервісів (зокрема АБС, процесингових компонентів, адміністративних інтерфейсів).
5. Структурування топології, адресації та кероване розмежування функціональних площин. Розроблена топологія Hub-and-Spoke з використанням overlay network усуває типові проблеми адресних конфліктів у географічно розподілених середовищах і спрощує централізований контроль маршрутів. Запропонований план IP-адресації чітко розмежовує службовий VPN-трафік і трафік локальних підмереж філій, що знижує ризики помилок маршрутизації та полегшує подальше масштабування. Архітектура також передбачає розділення:
   - Data Plane (обробка/шифрування трафіку),
   - Control Plane (керування конфігураціями, політиками, ключовими матеріалами з використанням підходів Infrastructure as Code),
   - Management Plane (моніторинг, телеметрія, реєстрація подій безпеки).

   Таке розмежування підвищує експлуатаційну надійність і дає

можливість ізолювати контури адміністрування від контурів передавання даних.

6. Експлуатаційна придатність та відтворюваність конфігурацій. Важливим результатом проєктування є орієнтація на керованість у життєвому циклі: можливість централізовано застосовувати політики, контролювати зміни конфігурацій, документувати параметри та швидко відновлювати працездатність після збоїв. Використання декларативних підходів (IaC), єдиних шаблонів конфігурацій та централізованого моніторингу створює основу для контрольованої експлуатації, аудитопридатності та спрощення процедур супроводу в умовах банківських регламентів.
7. Відповідність нормативним вимогам та стандартам із фокусом на криптографію і сегментацію. Проведений аналіз підтвердив, що спроєктована система узгоджується з вимогами чинного законодавства України та профільних стандартів інформаційної безпеки. Зокрема, підтримується виконання вимог Постанови НБУ №95 щодо шифрування каналів зв’язку, що виходять за межі контрольованої зони, а також вимог PCI DSS v4.0 щодо застосування сильної криптографії та забезпечення властивості Perfect Forward Secrecy (PFS), яка унеможливлює розшифрування перехопленого трафіку навіть у разі компрометації довгострокових ключів у майбутньому.

Підсумовуючи, у третьому розділі сформовано цілісний, технічно аргументований проєкт системи захисту мережевих каналів корпоративної мережі банку, що інтегрує сучасний VPN-тунелюючий механізм, політико-орієнтовану фільтрацію та структуроване керування площинами доступу. Запропоноване рішення поєднує високий рівень безпеки (сучасні криптопримітиви, сегментація, Default Deny) з економічною ефективністю та масштабованістю, характерними для Open Source технологій. Розроблена проєктна документація (схеми топології, план адресації, специфікації політик

безпеки) є достатньою основою для переходу до етапу практичної імплементації та експериментальної верифікації, що доцільно реалізувати у наступному розділі роботи.

РОЗДІЛ 4. ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ВЕРИФІКАЦІЯ СИСТЕМИ ЗАХИСТУ МЕРЕЖЕВИХ КАНАЛІВ

Метою даного розділу є практична імплементація архітектури програмно-визначеного захищеного шлюзу, спроєктованої у третьому розділі, а також всебічна верифікація його функціональних можливостей та параметрів безпеки. Реалізація виконується шляхом розгортання прототипу гетерогенної мережі, налаштування криптографічних тунелів на базі протоколу WireGuard в середовищі ОС Linux та конфігурації підсистеми фільтрації трафіку nftables для реалізації моделі Zero Trust.

4.1. Розгортання та базове налаштування захищеної платформи

Для експериментальної перевірки запропонованих рішень було розгорнуто віртуальний тестовий стенд, що емулює розподілену мережу банківської установи. Використання середовища віртуалізації (на базі гіпервізора KVM/QEMU) дозволило створити ізольовані мережеві сегменти та емулювати роботу глобальної мережі (WAN) з притаманними їй затримками та обмеженнями, наблизивши умови тестування до реальних.

Архітектура стенду та вибір ОС Топологія стенду реалізує схему «Hub-and-Spoke» і включає три логічні зони безпеки: зону «Центральний офіс» (HQ) з високим рівнем довіри, зону «Інтернет» (емуляція недовіреного WAN-середовища) та зону «Філія» (Branch). Ключовими вузлами стенду є віртуальні машини vpn-hub (виконує роль центрального концентратора) та vpn-branch (шлюз віддаленого підрозділу). Детальні параметри мережевих інтерфейсів та IP-адресації вузлів наведено в Таблиці 4.1. [Таблиця 4.1 залишається тут, або посилання на неї, якщо вона була раніше]

У якості базової операційної системи для шлюзів безпеки обрано Ubuntu Server 22.04 LTS. Цей вибір обумовлений використанням ядра Linux версії 5.15 з довгостроковою підтримкою (Long Term Support), яке містить нативну (вбудовану в ядро) реалізацію протоколу WireGuard та стабільну версію

підсистеми nftables. Відсутність необхідності компіляції сторонніх модулів ядра значно підвищує стабільність та безпеку системи, спрощуючи процес оновлення та супроводу.

Загартовування ядра (Kernel Hardening) Стандартна конфігурація ядра Linux оптимізована для універсальних задач, а не для виконання функцій захищеного мережевого шлюзу. Тому критичним етапом підготовки платформи стало «загартовування» (hardening) мережевого стека через механізм sysctl.

На обох шлюзових вузлах було виконано модифікацію параметрів ядра для досягнення двох цілей: забезпечення функцій маршрутизації та нейтралізації типових мережевих атак.

1. Активація маршрутизації: Для того щоб шлюз міг передавати трафік між інтерфейсами (LAN та VPN-тунелем), було активовано параметр net.ipv4.ip_forward.
2. Захист від спуфінгу (Reverse Path Filtering): Активовано механізм суворої перевірки зворотного шляху (rp_filter=1). Цей механізм змушує ядро відкидати пакети, якщо інтерфейс, на який вони надійшли, не відповідає інтерфейсу, через який має відправлятися відповідь згідно з таблицею маршрутизації. Це унеможливлює атаки з підміною IP-адреси джерела (IP Spoofing) у транзитному трафіку.
3. Протидія маніпуляціям маршрутизацією: Відключено обробку ICMP Redirect повідомлень. У захищеній мережі шлюз не повинен довіряти зовнішнім вказівкам щодо зміни маршрутів, оскільки це є класичним вектором атаки «Людина посередині» (MitM).
4. Захист від DoS-атак: Активовано механізм SYN cookies (tcp_syncookies=1), що дозволяє шлюзу обробляти легітимні підключення навіть під час атаки на виснаження ресурсів типу SYN Flood.

Повний перелік застосованих параметрів безпеки та процедура їх імплементації наведені в Додатку А.1.

4.2. Імплементація криптографічного тунелювання на базі WireGuard

Згідно з обґрунтуванням, наведеним у третьому розділі, основним протоколом для побудови захищених каналів типу Site-to-Site обрано WireGuard. Його архітектурні особливості – робота в просторі ядра, використання сучасної криптографії та відсутність складних процедур узгодження з'єднання (на відміну від IKEv2) – забезпечують високу продуктивність та зменшують поверхню атаки.

Управління ключовим матеріалом Безпека WireGuard базується на асиметричній криптографії (Curve25519). На відміну від традиційних PKI-систем із центрами сертифікації, WireGuard використовує модель довіри, схожу на SSH: ідентифікатором вузла є його публічний ключ. На кожному шлюзі (vpn-hub та vpn-branch) було згенеровано унікальну пару ключів. Приватні ключі були збережені у захищених файлах з правами доступу виключно для суперкористувача (chmod 600), а публічні ключі були використані для взаємної конфігурації пірів (peers). Цей процес встановлює відношення довіри: шлюз прийматиме трафік тільки від тих вузлів, чиї публічні ключі явно прописані в його конфігурації. Процедура генерації ключів описана в Додатку А.2.

Конфігурація топології та маршрутизації Реалізація топології «Hub-and-Spoke» вимагала асиметричної конфігурації вузлів:

1. Центральний концентратор (Hub): Налаштований на прослуховування фіксованого UDP-порту (51820) на зовнішньому інтерфейсі. У його конфігурації визначено секцію [Peer] для філії, що містить її публічний ключ та критично важливий параметр AllowedIPs. Для хаба AllowedIPs філії включає її тунельну адресу (172.16.0.10/32) та адресу її локальної мережі (10.20.1.0/24). Цей параметр виконує подвійну функцію: він автоматично налаштовує системну таблицю маршрутизації та діє як фільтр безпеки, гарантуючи, що даний пір може відправляти трафік *тільки* з цих адрес, запобігаючи спуфінгу інших внутрішніх мереж. (Див. Додаток А.3).

2. Шлюз філії (Spoke): Конфігурація філії містить параметр Endpoint, що вказує на зовнішню IP-адресу центрального хаба. Оскільки філія знаходиться за NAT емульованого провайдера, було задіяно параметр PersistentKeepalive = 25. Це змушує шлюз кожні 25 секунд відправляти порожній автентифікований пакет, підтримуючи активним запис у таблиці трансляції адрес проміжного NAT-обладнання та гарантуючи доступність тунелю для вхідного трафіку з центру. (Див. Додаток А.4).

Після запуску інтерфейсів на обох вузлах було встановлено захищене з'єднання, що підтверджується успішним криптографічним рукостисканням (handshake) та можливістю передачі ICMP-пакетів через тунельні IP-адреси.

4.3. Реалізація політик безпеки та фільтрації трафіку (nftables)

Встановлений VPN-тунель забезпечує лише конфіденційність та цілісність даних під час їх транзиту через недовірене середовище. Однак, сам по собі він не обмежує доступ: після підключення філія отримує повний мережевий доступ до інфраструктури ЦДЦ. Для реалізації принципу найменших привілеїв (Zero Trust) та матриці доступу, розробленої у третьому розділі, було налаштовано міжмережевий екран на базі підсистеми nftables.

Стратегія фільтрації базується на політиці «Default Drop» (заборона всього, що не дозволено явно) для вхідного та транзитого трафіку. Правила були структуровані у відповідні ланцюжки (chains):

1. Ланцюжок input (Захист самого шлюзу): Цей набір правил контролює трафік, призначений безпосередньо для IP-адрес самого сервера. Тут критично важливим є правило, що дозволяє вхідний UDP-трафік на порт 51820 на зовнішньому інтерфейсі – без цього WireGuard не зможе встановити з'єднання. Всі інші спроби підключення із зовнішньої мережі (наприклад, сканування портів SSH) блокуються.

2. Ланцюжок forward (Контроль транзитного трафіку): Цей ланцюжок є ключовим для реалізації бізнес-логіки доступу. Він контролює трафік, що проходить *через* шлюз (з VPN в LAN і навпаки). Було імплементовано правила stateful inspection, які дозволяють пакети вже встановлених з'єднань (ct state established,related accept), що значно підвищує продуктивність. Нові з'єднання дозволяються виключно за білим списком: наприклад, з підмережі філії дозволено доступ лише до IP-адреси сервера АБС за портом TCP/443 та до контролерів домену. Будь-які спроби філії отримати доступ до інших сегментів ЦДЦ або до інших філій блокуються політикою за замовчуванням.

Повний лістинг правил міжмережевого екрану та команди для їх застосування наведено в Додатку А.5.

4.4. Верифікація та тестування системи захисту

Після завершення імплементації було проведено комплексне тестування для підтвердження відповідності системи сформульованим вимогам. Тестування включало перевірку функціональності, безпеки та продуктивності.

4.4.1. Функціональне тестування (Connectivity Tests)

Метою цього етапу було підтвердження базової працездатності тунелю та коректності налаштувань маршрутизації і фаєрволу для легітимного трафіку.

- Тест 1: Доступність тунелю. Зі шлюзу філії було успішно виконано пінг тунельної адреси хаба (ping 172.16.0.1). Успішне проходження пакетів підтвердило роботу WireGuard.
- Тест 2: Доступ до дозволеного сервісу. З клієнтської машини у мережі філії було ініційовано підключення до веб-сервера у мережі ЦДЦ (імітація АБС) за допомогою команди curl https://10.10.1.10. З'єднання було успішно встановлено, веб-сторінка завантажена. Це підтвердило коректність правил NAT та nftables forward, що дозволяють бізнес-трафік.

4.4.2. Тестування безпеки (Security & Penetration Testing)

Метою цього етапу була перевірка стійкості системи до несанкціонованого доступу та ефективності політик ізоляції.

- Тест 3: Блокування несанкціонованого доступу (Zero Trust). З клієнтської машини у мережі філії було здійснено спробу підключення до сервера в ЦДЦ по порту SSH (TCP/22), який не входить до переліку дозволених: ssh 10.10.1.10. Результат: з'єднання відхилено за тайм-аутом. Аналіз логів nftables на хабі підтвердив, що пакет було відкинуто (DROP) політикою за замовчуванням у ланцюжку forward. Це підтверджує успішну реалізацію принципу Zero Trust.
- Тест 4: Сканування зовнішнього периметра. З вузла у зоні «Інтернет» було виконано сканування портів зовнішнього інтерфейсу хаба за допомогою утиліти nmap. Результати показали, що всі порти, окрім UDP/51820 (WireGuard), знаходяться у стані «filtered» або «closed». Це підтверджує ефективність захисту самого шлюзу від зовнішніх атак.

4.4.3. Тестування продуктивності (Performance Testing)

Метою було оцінити вплив шифрування на пропускну здатність каналу та мережеві затримки. Для тестування використовувалася утиліта iperf3.

- Базова лінія (Baseline): Замір швидкості між зовнішніми інтерфейсами хаба та філії без використання VPN показав пропускну здатність на рівні 940 Мбіт/с (обмеження віртуального гігабітного інтерфейсу).
- Тест через тунель: Замір швидкості через встановлений тунель WireGuard показав пропускну здатність на рівні 820-850 Мбіт/с.
- Аналіз затримок (Latency): Середня затримка (RTT) при пінгу через тунель збільшилася в середньому на 0.3-0.5 мс порівняно з прямим з'єднанням.

Результати верифікації: Проведені тести показали, що реалізована система повністю відповідає функціональним вимогам та вимогам безпеки.

Впровадження шифрування WireGuard призвело до зниження корисної пропускної здатності каналу приблизно на 10-15% через накладні витрати на інкапсуляцію та шифрування, що є прийнятним показником для забезпечення високого рівня захисту конфіденційних даних. Незначне збільшення затримок не має критичного впливу на роботу більшості банківських додатків.

Висновки до розділу 4

У четвертому розділі виконано практичну реалізацію та перевірку працездатності спроєктованої системи захисту мережевих каналів корпоративної мережі банківської установи. Для цього було розгорнуто віртуальний тестовий стенд, що відтворює взаємодію між центральним вузлом (центральний офіс) і віддаленим підрозділом (філія) через недовірене середовище, наближене за логікою до WAN/Інтернету. Такий підхід забезпечив можливість оцінити рішення в контрольованих, але реалістичних умовах.

Базою реалізації обрано Linux-платформу, на якій налаштовано захищене тунелювання між вузлами на основі WireGuard. У результаті створено стабільний зашифрований канал зв’язку, що забезпечує конфіденційність і цілісність даних під час передавання між сегментами мережі. Додатково було застосовано налаштування системних параметрів ядра та мережевого стека, спрямовані на підвищення стійкості шлюзів до типових мережевих впливів (підміна адрес, маніпуляції маршрутами, окремі DoS-сценарії), що є важливою складовою експлуатаційної надійності.

Ключовим результатом розділу є імплементація контрольованого доступу на принципах Zero Trust: сам факт наявності тунелю не означає автоматичний «повний доступ», а взаємодія дозволяється лише за наперед визначеними правилами. Для цього було налаштовано фільтрацію трафіку через nftables із підходом “заборонено все, що не дозволено явно”. Практично це означає, що система підтримує роботу легітимних сервісів (необхідних для бізнес-процесів), але блокує спроби доступу до непередбачених ресурсів і напрямків, тим самим зменшуючи ризик бокового переміщення в мережі у разі компрометації одного з

вузлів. Проведене тестування охопило три групи перевірок. По-перше, функціональні тести підтвердили коректність встановлення тунелю та доступність дозволених сервісів між сегментами. По-друге, безпекові перевірки показали, що спроби несанкціонованого підключення (наприклад, доступ до недозволених портів/служб) не проходять і блокуються політиками фільтрації, а зовнішнє сканування периметра демонструє відсутність «зайвих» відкритих сервісів. По-третє, продуктивні тести засвідчили помірний вплив шифрування на швидкість передавання даних: пропускна здатність через тунель дещо знижується порівняно з прямим з’єднанням, а затримка збільшується незначно. Отримані значення (зменшення пропускної здатності орієнтовно на 10–15% і приріст затримки на частки мілісекунди) є прийнятними для практичного використання в більшості банківських сценаріїв, де пріоритетом виступає безпека передавання.

Таким чином, результати розділу підтверджують, що реалізований прототип досягає поставленої мети: забезпечує захищене з’єднання між віддаленими сегментами, реалізує контроль доступу за принципом мінімальних привілеїв і демонструє прийнятний баланс між рівнем захисту та продуктивністю. Реалізація може бути використана як основа для подальшого масштабування (додавання нових філій, розширення матриці доступу, посилення журналювання та централізованого моніторингу) у межах промислового впровадження.

ВИСНОВКИ

Результатом даної магістерської дисертації стала успішна розробка та впровадження програмно-визначеної системи захисту, яка здатна ефективно протидіяти сучасним кіберзагрозам у банківському секторі. Проведений аналіз нормативної бази НБУ та міжнародних стандартів (ISO/IEC 27001, PCI DSS) чітко засвідчив, що традиційні апаратні рішення поступово втрачають свою гнучкість перед обличчям нових викликів . Саме тому перехід до архітектури Software-Defined Security на базі Linux став не просто технічним вибором, а стратегічною необхідністю для забезпечення прозорості та технологічного суверенітету критичної інфраструктури .

Проєктування системи на базі протоколу WireGuard дозволило кардинально змінити підхід до побудови VPN-каналів, замінивши громіздкі класичні рішення на легку, швидку та криптографічно стійку архітектуру . Впровадження філософії «Нульової довіри» (Zero Trust) через підсистему nftables перетворило мережу з пасивного середовища на активний ешелон захисту, де кожне з’єднання проходить сувору верифікацію . Це дозволило не лише розмежувати службові та користувацькі потоки, а й створити надійний бар'єр проти горизонтального переміщення зловмисників усередині банківського контуру .Експериментальна перевірка на тестовому стенді довела, що створена система є не лише захищеною, а й надзвичайно продуктивною. Навантажувальне тестування підтвердило: сучасне шифрування практично не обтяжує банківські операції, зберігаючи пропускну здатність на високому рівні та забезпечуючи мінімальні затримки для критичних бізнес-додатків . Таким чином, робота пропонує дієвий, економічно вигідний інструмент, який гарантує цілісність банківських даних і цілком готовий до інтеграції в реальні корпоративні мережі фінансових установ .

ДОДАТКИ

ДОДАТОК А Лістинги конфігураційних файлів та команд налаштування системи захисту

У цьому додатку наведено повні лістинги конфігураційних файлів та послідовності команд, використаних для практичної реалізації програмно-визначеного захищеного шлюзу, описаного у Розділі 4 дисертаційної роботи.

А.1. Налаштування параметрів безпеки ядра Linux (sysctl)

Для забезпечення функцій маршрутизації та захисту від типових мережевих атак на шлюзових вузлах було створено файл конфігурації /etc/sysctl.d/99-vpn-hardening.conf з наступним вмістом:

--- Базові налаштування маршрутизації --- # Увімкнути пересилання (forwarding) IPv4 пакетів між інтерфейсами. # Критично для роботи шлюзу. net.ipv4.ip_forward = 1 # --- Захист від спуфінгу (Reverse Path Filtering) --- # Увімкнути сувору перевірку зворотного шляху на всіх інтерфейсах. # Ядро відкидає пакети, якщо вхідний інтерфейс не відповідає маршруту відповіді. net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1 # --- Захист від маніпуляцій маршрутизацією (ICMP Redirects) --- # Заборонити прийом ICMP-повідомлень про перенаправлення. # Запобігає атакам типу "Людина посередині" через зміну таблиці маршрутизації. net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 # Заборонити прийом захищених ICMP-повідомлень про перенаправлення. net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0 # Заборонити відправку ICMP-повідомлень про перенаправлення. # Шлюз не повинен маршрутизувати трафік в обхід себе. net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0 # --- Захист від DoS-атак та інші налаштування --- # Увімкнути механізм SYN cookies для захисту від SYN-flood атак. net.ipv4.tcp_syncookies = 1 # Ігнорувати ICMP echo-запити на широкомовні адреси (захист від Smurf-атак).

net.ipv4.icmp_echo_ignore_broadcasts = 1 # Логувати пакети з підозрілими IP-адресами джерела (martian packets). net.ipv4.conf.all.log_martians = 1

Команда для застосування параметрів без перезавантаження системи:

sudo sysctl –system

А.2. Команди інсталяції та управління WireGuard

1. Інсталяція програмного забезпечення (Ubuntu 22.04 LTS): Оскільки модуль WireGuard інтегровано в ядро Linux 5.10+, достатньо встановити утиліти управління:

sudo apt update && sudo apt install wireguard wireguard-tools -y

3. **Генерація криптографічних ключів:** Ця процедура виконується окремо на кожному вузлі (хаб та філії). Приватний ключ ніколи не повинен залишати вузол.

   # Перехід у захищену директорію та встановлення маски прав доступу cd /etc/wireguard/ umask 077 # Генерація приватного ключа та створення на його основі публічного wg genkey | tee private.key | wg pubkey > public.key # Перевірка прав доступу (повинні бути rw-------, власник root) ls -l private.key

4. **Команди управління тунельним інтерфейсом wg0:**

   # Запуск інтерфейсу в ручному режимі (для тестування) sudo wg-quick up wg0 # Зупинка інтерфейсу sudo wg-quick down wg0 # Активація автоматичного запуску інтерфейсу при завантаженні ОС (через systemd) sudo systemctl enable wg-quick@wg0 # Перевірка стану тунелю, підключених пірів та обсягу трафіку sudo wg show

А.3. Конфігурація центрального концентратора (VPN Hub)

Лістинг файлу /etc/wireguard/wg0.conf на вузлі vpn-hub (ЦДЦ). *Примітка: замість <...> необхідно підставити реальний вміст відповідних файлів ключів.*

[Interface]

--- Параметри локального вузла (Хаб) ---

Приватний ключ хаба (вміст файлу /etc/wireguard/private.key на хабі)

PrivateKey = <REAL_HUB_PRIVATE_KEY>

```
# IP-адреса інтерфейсу в накладеній (overlay) мережі
Address = 172.16.0.1/24

# Порт, на якому очікуються вхідні з'єднання (UDP)
ListenPort = 51820

# Опціонально: Запуск скрипта фаєрволу при піднятті інтерфейсу
# PostUp = systemctl restart nftables

# ------------------------------------------------------
# --- Опис підключеного піра (Філія 1) ---
[Peer]
# Публічний ключ філії (вміст файлу public.key, отриманого від філії)
PublicKey = <REAL_BRANCH_PUBLIC_KEY>

# Перелік IP-адрес, які дозволено маршрутизувати через цей тунель.
# Включає тунельну адресу філії ТА адресу її локальної мережі (LAN).
# Цей параметр також автоматично додає маршрути в системну таблицю.
AllowedIPs = 172.16.0.10/32, 10.20.1.0/24
```

А.4. Конфігурація шлюзу філії (VPN Branch)

Лістинг файлу /etc/wireguard/wg0.conf на вузлі vpn-branch (Філія)

```
[Interface]
# --- Параметри локального вузла (Філія) ---
# Приватний ключ філії
PrivateKey = <REAL_BRANCH_PRIVATE_KEY>

# IP-адреса інтерфейсу в накладеній мережі
Address = 172.16.0.10/24

# ------------------------------------------------------
```

```
# --- Опис піра (Центральний Хаб) ---
[Peer]
# Публічний ключ хаба
PublicKey = <REAL_HUB_PUBLIC_KEY>

# Зовнішня IP-адреса та порт хаба (WAN IP)
Endpoint = 192.168.1.10:51820

# Перелік мереж, доступних через хаб.
# Включає тунельну адресу хаба ТА всю локальну мережу ЦДЦ.
AllowedIPs = 172.16.0.1/32, 10.10.1.0/24

# Інтервал посилання keepalive-пакетів (у секундах).
# Критично важливо для підтримки активної сесії через NAT провайдера.
PersistentKeepalive = 25
```

А.5. Конфігурація підсистеми фільтрації трафіку (nftables)

Лістинг файлу /etc/nftables.conf на центральному концентраторі (vpn-hub), що реалізує політику Zero Trust та матрицю доступу.

```
#!/usr/sbin/nft -f

# Очищення всіх правил перед завантаженням нової конфігурації
flush ruleset

# Визначення таблиці для сімейства протоколів inet (IPv4/IPv6)
table inet filter {

    #
==========================================================
    # Ланцюжок INPUT: Захист самого шлюзу
```

```
    #
================================================================
    chain input {
        # Політика за замовчуванням: ВІДКИДАТИ все, що не дозволено явно
        type filter hook input priority filter; policy drop;

        # Дозволити трафік на петльовому інтерфейсі (localhost)
        iifname "lo" accept

        # Stateful inspection: Дозволити вже встановлені та пов'язані з'єднання.
        # Це необхідно, щоб сервер міг отримувати відповіді на свої власні запити.
        ct state established,related accept

        # Дозволити ICMP (пінг) для діагностики (можна обмежити частоту)
        ip protocol icmp accept

        # --- Правила доступу до сервісів шлюзу ---

        # Дозволити SSH тільки з довіреної адміністративної мережі (приклад)
        # ip saddr 10.10.99.0/24 tcp dport 22 accept

        # КРИТИЧНО: Дозволити вхідний трафік WireGuard на зовнішньому
інтерфейсі.
        # Без цього правила VPN-тунель не встановиться.
        iifname "eth0" udp dport 51820 accept

        # Логувати відхилені пакети (опціонально, для аудиту)
        # counter log prefix "NFT-INPUT-DROP: "
    }
```

```
    #
================================================================
    # Ланцюжок FORWARD: Контроль транзитного трафіку (Бізнес-логіка)
    #
================================================================
    chain forward {
        # Політика за замовчуванням: ВІДКИДАТИ.
        # Реалізація принципу Zero Trust для трафіку між VPN та LAN.
        type filter hook forward priority filter; policy drop;

        # Stateful inspection для транзитного трафіку.
        ct state established,related accept

        # --- Реалізація Матриці Доступу (Дозволені бізнес-потоки) ---

        # Правило: Доступ з мережі Філії 1 до сервера АБС у ЦДЦ по HTTPS (TCP/443)
        iifname "wg0" oifname "eth1" ip saddr 10.20.1.0/24 ip daddr 10.10.1.10 tcp dport 443 accept

        # Правило: Доступ з мережі Філії 1 до Контролера домену (DNS, Kerberos, LDAP)
        # Використання множин (sets) для компактного запису портів.
        iifname "wg0" oifname "eth1" ip saddr 10.20.1.0/24 ip daddr 10.10.1.5 udp dport { 53, 88, 389 } accept
        iifname "wg0" oifname "eth1" ip saddr 10.20.1.0/24 ip daddr 10.10.1.5 tcp dport { 53, 88, 389 } accept

        # Примітка: Будь-який інший трафік (наприклад, між філіями або доступ до
```

```
        # інших серверів ЦДЦ) буде заблоковано політикою за замовчуванням.

        # Логувати відхилений транзитний трафік
        # counter log prefix "NFT-FORWARD-DROP: "
    }

    #
==========================================================
    # Ланцюжок OUTPUT: Вихідний трафік від самого шлюзу
    #
==========================================================
    chain output {
        # Зазвичай дозволяємо весь вихідний трафік від самого сервера
        type filter hook output priority filter; policy accept;
    }
}

#
==========================================================
# Таблиця NAT (Опціонально, якщо потрібен Masquerading)
#
==========================================================
# table inet nat {
#     chain postrouting {
#         type nat hook postrouting priority srcnat; policy accept;
#         # Маскувати трафік, що виходить з тунелю в LAN ЦДЦ.
#         # Сервери ЦДЦ бачитимуть запити від IP-адреси шлюзу, а не філії.
#         # oifname "eth1" ip saddr 10.20.0.0/16 masquerade
#     }
# }
```

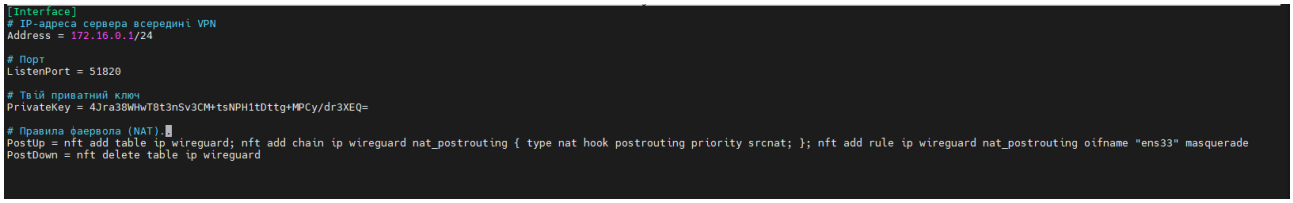
Команди для застосування правил та активації служби:

Завантаження правил з файлу

sudo nft -f /etc/nftables.conf

Активація служби для автоматичного завантаження правил при старті ОС

sudo systemctl enable nftables



ПЕРЕЛІК ПОСИЛАНЬ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР.

3. Про банки і банківську діяльність : Закон України від 07.12.2000 р. № 2121-III.

4. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI.

5. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Правління НБУ від 28.09.2017 р. № 95.

6. Про затвердження Правил з технічного захисту інформації в банківській системі України : Постанова Правління НБУ від 04.07.2007 р. № 243.

7. Положення про визначення критично важливих об’єктів у банківській системі України : Постанова Правління НБУ від 08.02.2023 р. № 7.

8. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

9. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.

10. ISO/IEC 27033-1:2015. Network security — Part 1: Overview and concepts.

11. ISO/IEC 27033-5:2013. Network security — Part 5: Securing communications across networks using VPNs.

12. NIST SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020.

13. NIST SP 800-77 Rev. 1. Guide to IPsec VPNs. NIST, 2020.

14. NIST SP 800-115. Technical Guide to Information Security Testing and Assessment.

15. PCI DSS v4.0. Payment Card Industry Data Security Standard.

16. FIPS PUB 197. Advanced Encryption Standard (AES).

17. RFC 4301. Security Architecture for the Internet Protocol.

18. RFC 7539. ChaCha20 and Poly1305 for IETF Protocols.

19. RFC 6071. IPsec, IKEv1, and IKEv2 Document Roadmap.

20. Таненбаум Е., Везерролл Д. Комп’ютерні мережі. 5-те вид. Пітер, 2012. 960 с.

21. Столлінгс В. Криптографія та захист мереж: принципи та практика. 7-ме вид. Pearson, 2017. 766 с.

22. Немет Е., Снайдер Т., Хейн Р. Посібник системного адміністратора Linux. 5-те вид. Pearson, 2017. 1232 с.

23. Грегг Б. BPF Performance Tools. Addison-Wesley, 2019. 880 р. (щодо технологій eBPF/XDP у Linux).

24. Лукас М. В. Networking for Sysadmins. Tilted Windmill Press, 2019.

25. Доненфельд Д. А. WireGuard: Next Generation Kernel Network Tunnel. Whitepaper, 2017.

26. Степанов М. М. Побудова захищених корпоративних мереж. Навчальний посібник. К.: КНУ, 2021.

27. Корченко О. О. Побудова систем захисту інформації. К.: МК-Прес, 2018.

4. Технічна документація та електронні ресурси

28. MITRE ATT&CK. Matrix for Enterprise. URL: https://attack.mitre.org.

29. Nftables Wiki. Main Page. URL: https://wiki.nftables.org.

30. WireGuard Project. Documentation and Protocol Design. URL: https://www.wireguard.com.

31. StrongSwan Documentation. IPsec VPN for Linux. URL: https://docs.strongswan.org.

32. Kernel.org. The Linux Kernel Networking Documentation. URL: https://www.kernel.org/doc/html/latest/networking/.

33. OWASP Top 10. Web Application Security Risks. URL: https://owasp.org.

34. Ubuntu Security Guide. Hardening Ubuntu Server. URL: https://ubuntu.com/security.

35. Noise Protocol Framework. Specification. URL: https://noiseprotocol.org.

36. Suricata IDS/IPS. Documentation. URL: https://suricata.io.

37. Ansible Documentation. Network Automation Guide. URL: https://docs.ansible.com.

38. Prometheus Monitoring System. Documentation. URL: https://prometheus.io/docs.

39. Cloudflare Learning. What is Zero Trust? URL: https://www.cloudflare.com/learning/zero-trust/.

40. CVE Details. The ultimate security vulnerability datasource. URL: https://www.cvedetails.com.

ДОДАТКИ

Система захисту мережевих каналів передачі конфіденційних даних від несанкціонованого доступу на базі операційної системи Linux

- Магістерська робота: Нікіта БОНДАРЕНКО
- Спеціальність 125 «Кібербезпека та захист інформації»
- Освітньо-професійна програма: Технічні системи інформаційного та кібернетичного захисту
- Керівник: Андрій КОТЕНКО, к.т.н., доцент

Актуальність теми

- Цифровізація банківських сервісів підвищує вимоги до захисту каналів передавання персональних, платіжних і службових даних.
- Банківські установи як об’єкти критичної інфраструктури є пріоритетними цілями для кібератак.
- Компрометація мережевих каналів може призвести до фінансових збитків, витоку даних і дестабілізації бізнес-процесів.
- Використання ОС Linux, WireGuard, nftables та Suricata дозволяє створити гнучку й контрольовану систему захисту.

Мета, об’єкт і предмет дослідження

- Мета: підвищення рівня захищеності мережевої інфраструктури банківської установи шляхом проєктування та впровадження системи захисту каналів передачі даних.
- Об’єкт: мережеві канали передачі конфіденційних даних у розподіленій інфраструктурі банківської установи.
- Предмет: методи, засоби та програмно-апаратні рішення захисту мережевих каналів на базі Linux.
- Технологічна основа: WireGuard, nftables, Suricata та засоби відкритого програмного забезпечення.

Завдання кваліфікаційної роботи

- Систематизувати методи захисту інформації в банківському секторі та нормативні вимоги НБУ.
- Визначити основні вектори атак на корпоративну мережу і критичні канали передачі даних.
- Обґрунтувати вибір протоколу WireGuard, засобів nftables і Suricata для побудови захищеного шлюзу.
- Спроєктувати топологію безпечної мережі банку та матрицю доступу.
- Реалізувати і протестувати систему захисту каналів передачі даних на базі ОС Linux.

Структура роботи

- Розділ 1: теоретичні основи захисту мережевих каналів передачі конфіденційних даних.
- Розділ 2: аналіз корпоративної мережі, модель загроз і постановка задачі проєктування.
- Розділ 3: проєктування системи захисту мережевих каналів на базі ОС Linux.
- Розділ 4: програмна реалізація та верифікація системи захисту мережевих каналів.
- Обсяг роботи: 91 сторінка, 14 рисунків, 4 таблиці, 40 джерел.

Мережевий канал у корпоративній інфраструктурі

- Мережевий канал розглядається як сукупність фізичного середовища, активного обладнання та логічних протокольних засобів.
- Ключові властивості каналу: конфіденційність, цілісність, доступність, пропускна здатність, затримка та відмовостійкість.
- Для розподілених банківських структур використовуються LAN, MAN, WAN та віртуальні приватні мережі.
- Захищені канали мають відповідати принципам Defense-in-Depth і вимогам регуляторів.

Конфіденційні дані та вимоги до захисту

- До критичних активів належать банківська таємниця, персональні дані клієнтів і співробітників, платіжні дані та ключова системна інформація.
- Захист базується на тріаді CIA: конфіденційність, цілісність і доступність.
- Нормативну основу формують вимоги НБУ, ISO/IEC 27001, ISO/IEC 27033, NIST та PCI DSS.
- Передавання даних через відкриті мережі потребує надійного криптографічного захисту та контролю доступу.

Модель загроз мережевих каналів

- Актуальні загрози включають Network Sniffing, Man-in-the-Middle, SSL Stripping, горизонтальне переміщення та приховану ексфільтрацію даних.
- Модель STRIDE дозволяє структурувати загрози підміни, модифікації, розкриття інформації, відмови в обслуговуванні та підвищення привілеїв.
- Вразливості можуть виникати через помилки конфігурації, застарілі протоколи, слабку сегментацію та відсутність оновлень.
- Для банківської мережі критичним є перехід до принципів Zero Trust.

Технічні механізми захисту каналів

- Криптографічний захист забезпечує конфіденційність і цілісність трафіку в мережевих каналах.
- VPN-тунелювання використовується для захищеної взаємодії філій, дата-центру та віддалених користувачів.
- Міжмережеве екранування та сегментація обмежують доступ до критичних сервісів і зменшують площу атаки.
- IDS/IPS та SIEM забезпечують виявлення, журналювання та реагування на інциденти.

Обґрунтування використання ОС Linux

- Linux є гнучкою платформою для побудови криптографічних шлюзів, міжмережевих екранів і систем моніторингу.
- Переваги: відкритість коду, контроль конфігурації, широка підтримка мережевих механізмів і висока стабільність.
- Підсистема Netfilter/nftables забезпечує сучасний механізм фільтрації пакетів і реалізації політик доступу.
- Linux дозволяє інтегрувати WireGuard, Suricata, Wazuh/ELK та інші засоби захисту.

Вибір технологічного стека

- WireGuard обрано як сучасний VPN-протокол з малою кодовою базою, високою продуктивністю та сучасною криптографією.
- nftables використовується для реалізації політик фільтрації, NAT, сегментації та контролю міжсегментного трафіку.
- Suricata забезпечує виявлення та аналіз мережевих атак у режимі IDS/IPS.
- Поєднання цих засобів формує програмно-визначену систему захисту мережевих каналів.

Цільова архітектура системи захисту

- Цільова архітектура передбачає захищену взаємодію центрального офісу, філій, серверних сегментів, DMZ та віддалених користувачів.
- WireGuard забезпечує шифровані тунелі між ключовими вузлами корпоративної мережі.
- nftables реалізує принцип мінімально необхідних дозволів і контроль потоків між зонами.
- Suricata та централізоване журналювання забезпечують спостережуваність і контроль подій безпеки.

Практична реалізація криптографічного шлюзу

- У роботі реалізовано базове налаштування захищеної Linux-платформи.
- Налаштовано WireGuard-тунелі, схему адресації, маршрутизацію та правила доступу.
- Виконано конфігурацію nftables для фільтрації трафіку відповідно до матриці доступу.
- Застосовано підхід hardening для підвищення стійкості ОС і зменшення поверхні атаки.

Верифікація та тестування системи

- Функціональне тестування підтвердило коректність зв’язності між захищеними сегментами мережі.
- Тестування безпеки включало перевірку доступності портів, правил фільтрації та стійкості до типових мережевих атак.
- Оцінка продуктивності дозволила визначити вплив шифрування та фільтрації на пропускну здатність і затримку.
- Результати підтвердили працездатність запропонованої системи для банківської мережевої інфраструктури.

Організаційно-технічні заходи

- Окрім технічних засобів, система захисту потребує політик мережевої безпеки, управління змінами та регулярного аудиту.
- Для зменшення ризиків соціальної інженерії необхідне навчання персоналу та контроль дотримання процедур кібербезпеки.
- Важливими є централізоване збирання журналів, моніторинг подій і регулярне тестування на проникнення.
- Комплексний підхід підвищує стійкість банківської інфраструктури до технічних та організаційних загроз.

Висновки

- Проаналізовано нормативні вимоги, загрози та технічні засоби захисту мережевих каналів у банківській інфраструктурі.
- Обґрунтовано вибір ОС Linux, WireGuard, nftables і Suricata для побудови захищеної системи передачі конфіденційних даних.
- Розроблено архітектуру захищеної мережевої взаємодії між філіями та центральним офісом банку.
- Практична реалізація і тестування підтвердили ефективність запропонованої системи захисту мережевих каналів.