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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Організація захисту закритої лінії передачі даних»

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
Сергій КУЛІНІЧ

Виконав: здобувач вищої освіти групи СЗДМ-61
Сергій КУЛІНІЧ

Керівник: ПЕПА Юрій
к.т.н., доцент (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

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУРОБОТУ

_____Кулініч Сергій Русланович_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Організація захисту закритої лінії передачі даних»
керівник кваліфікаційної роботи Юрій ПЕПА к.т.н., доцент
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «_15__» _____10_____ 2024 р. №320
2. Строк подання кваліфікаційної роботи 15.12.2024 р.
3. Вихідні дані до кваліфікаційної роботи: закриті лінії передачі даних, алгоритми шифрування даних, протоколи шифрування даних, алгоритми аутентифікації.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1 Дослідження понять та сутності закритих ліній передачі даних, аналіз існуючих видів і технологічних характеристик таких ліній;
4.2 Вивчення сучасних методів шифрування (зокрема AES, RSA, ECC) і криптографічних протоколів (SSL/TLS, IPsec), оцінка їх ефективності у захисті інформації, яка передається закритими лініями, від різних типів кіберзагроз;
4.3 Розробка нового закритого каналу передачі даних на основі існуючих технологій, проведення його дослідження та оцінка його захищеності.
5. Перелік графічного матеріалу: ___Презентаційний матеріал на_____слайдах.__ _____
_____

6. Дата видачі завдання_____15.10.2024_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Сергій КУЛІНІЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Юрій ПЕПА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, що займають загалом 120 сторінки. У роботі міститься 11 рисунків, 2 таблиці, 14 формул. Список використаних джерел налічує 42 найменувань.

Метою кваліфікаційної роботи є дослідження, розробка та оцінка ефективних методів побудови й використання закритих ліній передачі даних для забезпечення безпеки інформації в умовах сучасних кіберзагроз.

Об’єктом дослідження є закриті лінії передачі даних, їхні технології захисту та шифрування.

Методи дослідження включають аналіз літературних джерел, математичне моделювання, симуляцію роботи захищених каналів передачі даних, дослідження методів шифрування (AES, RSA, ECC), а також аналіз ризиків.

У кваліфікаційній роботі:

- визначено сутність і класифікацію закритих ліній передачі даних, а також проаналізовано існуючі види й технологічні характеристики таких ліній;
- проаналізовано сучасні методи шифрування (симетричні та асиметричні алгоритми), криптографічні протоколи (IPsec, SSL/TLS), а також оцінено їх ефективність у захисті інформації, яка передається закритими лініями, від різних типів кіберзагроз;
- розроблено та змодельовано рішення для захищеного каналу зв’язку з використанням VPN-технологій, проведено оцінку його ефективності та захисту на основі змодельованих ситуацій від впливів потенційних атак на захищеність каналу.

Ключові результати дослідження підтверджують доцільність використання комбінованого підходу, який включає шифрування та багатофакторну автентифікацію для зниження ризиків несанкціонованого доступу.

Апробація:

Кулініч С.Р., Пепа Ю.В. Роль шифрування в забезпеченні безпеки закритих ліній передачі даних *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.9 - 10.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Ключові слова: ЗАКРИТІ ЛІНІЇ ПЕРЕДАЧІ ДАНИХ, ШИФРУВАННЯ, КРИПТОГРАФІЧНІ ПРОТОКОЛИ, VPN, КІБЕРБЕЗПЕКА, АСИМЕТРИЧНЕ ТА СИМЕТРИЧНЕ ШИФРУВАННЯ, КОНФІДЕНЦІЙНІСТЬ, АУТЕНТИФІКАЦІЯ.

ABSTRACT

The text part of the qualification work consists of an introduction, three sections, general conclusions, a list of sources used, appendices, which occupy a total of 120 pages. The work contains 11 figures, 2 tables, 14 formulas. The list of sources used includes 42 items.

The purpose of the qualification work is to study, develop and evaluate effective methods for building and using closed data transmission lines to ensure information security in the face of modern cyber threats.

The object of the study is closed data transmission lines, their protection and encryption technologies.

The research methods include analysis of literary sources, mathematical modeling, simulation of the operation of protected data transmission channels, research of encryption methods (AES, RSA, ECC), as well as risk analysis.

The qualification work:

- defines the essence and classification of closed data transmission lines, and also analyzes the existing types and technological characteristics of such lines;
- analyzed modern encryption methods (symmetric and asymmetric algorithms), cryptographic protocols (IPsec, SSL/TLS), and also assessed their effectiveness in protecting information transmitted over closed lines from various types of cyber threats;
- developed and modeled a solution for a secure communication channel using VPN technologies, assessed its effectiveness and protection based on simulated situations from the effects of potential attacks on the security of the channel.

The key results of the study confirm the feasibility of using a combined approach, which includes encryption and multi-factor authentication to reduce the risks of unauthorized access.

Approbation:

Kulinich S.R., Pepa Y.V. The role of encryption in ensuring the security of

closed data transmission lines All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 03, 2024, Kyiv: RVC DUIKT. – 024. P.9 - 10.

https://duikt.edu.ua/uploads/p_2661_93669247.pdfKeywords: CLOSED DATA TRANSMISSION LINES, ENCRYPTION, CRYPTOGRAPHIC PROTOCOLS, VPN, CYBERSECURITY, ASYMMETRIC AND SYMMETRIC ENCRYPTION, CONFIDENTIALITY, AUTHENTICATION.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

5G-AKA	–	5th Generation Authentication and Key Agreement
AES	–	Advanced Encryption Standard
CA	–	Certificate Authority
DoS	–	Denial of Service
EAP-AKA	–	Extensible Authentication - Protocol - Authentication and Key Agreement
EAP-TLS	–	Extensible Authentication Protocol - Transport Layer Security
ECC	–	Elliptic Curve Cryptography
EPS	–	Evolved Packet System
ESP	–	Encapsulating Security Payload
HSM	–	Hardware Security Module
IKEv2	–	Internet Key Exchange version 2
IPsec	–	Internet Protocol Security
MITM	–	Man-in-the-Middle Attack
QKD	–	Quantum Key Distribution
RSA	–	Rivest-Shamir-Adleman
SSL	–	Secure Sockets Layer
TLS	–	Transport Layer Security
VPN	–	Virtual Private Network

ВСТУП

Актуальність теми. У сучасному світі, що характеризується стрімким розвитком інформаційних технологій, питання забезпечення безпеки передачі даних стає одним із ключових викликів. Зростаючий обсяг переданої інформації, поява нових кіберзагроз та еволюція методів атак вимагають впровадження ефективних механізмів захисту. Закриті лінії передачі даних відіграють центральну роль у збереженні конфіденційності, цілісності та доступності інформації в різних сферах діяльності, зокрема у державному управлінні, банківському секторі, оборонній промисловості та великих корпораціях.

Поширення кібератак, таких як перехоплення даних, атаки «людина посередині» (Man-in-the-Middle) та шкідливе програмне забезпечення, ставить під загрозу не лише економічні активи, а й національну безпеку. У таких умовах забезпечення захищеності каналів зв’язку стає критично важливим.

Ця робота присвячена дослідженню закритих ліній передачі даних, які забезпечують високий рівень захисту за допомогою сучасних технологій шифрування, фізичної ізоляції каналів та автентифікації доступу.

Мета роботи – дослідити сутність, значення та ефективність закритих ліній передачі даних у забезпеченні інформаційної безпеки, а також розробити рекомендації щодо покращення їх захищеності.

Завдання дослідження:

- визначити поняття та сутність закритих ліній передачі даних, а також проаналізувати існуючі види й технологічні характеристики таких ліній;

- вивчити сучасні методи шифрування (зокрема AES, RSA, ECC) і криптографічні протоколи, такі як SSL/TLS і IPsec, а також оцінити їх ефективність у захисті інформації, яка передається закритими лініями, від різних типів кіберзагроз;
- створити новий закритий канал передачі даних на основі існуючих технологій, провести його дослідження та оцінити його захищеність.

Об’єкт дослідження – закриті лінії передачі даних і технології їхнього використання.

Предмет дослідження – методи забезпечення безпеки даних під час їх передачі через закриті канали зв’язку.

Методи дослідження базуються на аналізі сучасних технологій кібербезпеки, моделюванні функціонування захищених каналів, порівняльному аналізі методів шифрування та дослідженні ризиків кіберзагроз.

Структура роботи.

Кваліфікаційна робота складається з трьох розділів:

У першому розділі аналізуються сутність і класифікація закритих ліній передачі даних, а також їх основні технічні характеристики.

У другому розділі досліджуються методи шифрування та захисту інформації, а також основні кіберзагрози й способи протидії їм.

У третьому розділі виконано дослідження захищеності спроектованої закритої лінії передачі даних та проведено оцінку її ефективності.

Фактологічну основу роботи складають наукові праці, стандарти у сфері кібербезпеки, технічна документація та практичні дослідження.

РОЗДІЛ 1 АНАЛІЗ ПОНЯТТЯ ЗАКРИТИХ ЛІНІЙ ПЕРЕДАЧІ ДАНИХ

1.1 Вступ до закритих ліній передачі даних

1.1.1 Визначення поняття закритих ліній передачі даних

На даний момент не існує точного визначення закритих або захищених ліній передачі даних, але на основі зібраних мною даних його формулювання виглядало б так:

Закрита (захищена) лінія передачі даних — це канал зв'язку, спеціально розроблений для забезпечення конфіденційної та безпечної передачі даних між двома або більше сторонами. Такі лінії використовують технології шифрування та інші методи захисту для мінімізації ризику перехоплення чи несанкціонованого доступу до переданих даних. Основна мета закритих ліній — забезпечити цілісність, конфіденційність та автентифікацію переданих даних, що особливо важливо для урядових, військових і корпоративних мереж.

Або так:

Закриті лінії передачі даних — це захищені канали зв'язку, які використовуються для передачі інформації між обмеженою кількістю користувачів. Такі системи зазвичай створюються з використанням захищених фізичних ліній, шифрування або інших технологій, щоб гарантувати конфіденційність і безпеку даних. Ці лінії можуть бути використані в державних установах, корпоративних мережах або для військових цілей.

1.1.2 Значення закритих ліній для сучасних організацій та державних установ

Закриті лінії передачі даних відіграють критично важливу роль для сучасних організацій та державних установ, оскільки вони забезпечують високий рівень безпеки переданої інформації. У світі, де кіберзагрози стають все більш поширеними, використання публічних мереж для передачі конфіденційної інформації стає надто ризикованим, захист даних є пріоритетом для будь-якої установи, що працює з конфіденційною або критичною інформацією. Закриті

лінії дозволяють мінімізувати ризик перехоплення даних, оскільки доступ до цих каналів обмежений і суворо контролюється. Це, що інформація, яка передається між підрозділами або філіями, захищена від перехоплення сторонніми особами або зловмисниками. Це особливо важливо для державних установ, військових організацій, банків та великих корпорацій, що оперують чутливими даними, такими як фінансова звітність, персональні дані клієнтів або державні таємниці.

Одним з ключових аспектів закритих ліній є можливість повного контролю над доступом до мережі. Організації можуть чітко визначати, хто має право підключатися до мережі, а також контролювати, які саме дії можуть виконувати користувачі. Це дозволяє уникнути несанкціонованих доступів і забезпечити безперебійну роботу в межах політики безпеки організації. Для державних установ та силових структур, де безпека інформації є питанням національної безпеки, такий рівень контролю є критично важливим.

Ще однією вагомою перевагою закритих ліній є їх здатність захищати від кіберзагроз, які постійно еволюціонують. Порівняно з відкритими мережами, такими як Інтернет, закриті канали передачі даних значно менш вразливі до атак. Вони часто використовують шифрування і додаткові механізми захисту, що забезпечує конфіденційність і цілісність даних. Для організацій, що працюють у таких критично важливих сферах, як енергетика, фінанси або охорона здоров’я, збереження безпеки даних є необхідною умовою для їхньої діяльності. Наприклад, лікарні використовують закриті лінії для обміну медичними записами пацієнтів, оскільки ці дані підпадають під суворі вимоги щодо конфіденційності.

Закриті лінії передачі даних також забезпечують високу надійність і стабільність зв’язку, що робить їх особливо цінними для організацій, які не можуть дозволити собі збої в роботі. На відміну від публічних мереж, які можуть бути перевантажені або піддаватися атакам, закриті лінії функціонують незалежно і забезпечують безперебійний зв'язок навіть у випадках критичних ситуацій. Це є ключовим фактором для державних установ, особливо у сфері управління кризами або реагування на надзвичайні події, коли швидкий і

надійний обмін інформацією може врятувати життя або зберегти важливі ресурси.

Крім того, закриті лінії передачі даних дозволяють організаціям підтримувати інтегровану внутрішню інфраструктуру, яка з'єднує всі відділи, філії та офіси в єдину мережу. Це сприяє кращій координації та управлінню процесами всередині організації. Наприклад, великий банк може використовувати закриті лінії для об’єднання своїх відділень у різних регіонах, що дозволяє централізовано керувати фінансовими операціями, захищати дані клієнтів і забезпечувати безперебійне обслуговування.

Окрім безпеки та надійності, закриті лінії допомагають організаціям відповідати нормативним вимогам. Багато галузей, зокрема фінансова і медична, підпадають під суворі регуляції щодо захисту інформації. Використання закритих каналів дозволяє установам дотримуватися цих стандартів і зменшувати ризик санкцій за порушення конфіденційності або витік даних, і уникати штрафів або юридичних проблем. Для державних установ це питання особливо актуальне, оскільки вони часто працюють з секретною інформацією, де найменший витік може мати серйозні наслідки для національної безпеки.

Завдяки цим перевагам закриті лінії передачі даних є ключовим елементом у забезпеченні інформаційної безпеки сучасних організацій та державних установ. Вони дозволяють уникати загроз перехоплення даних, забезпечують контроль доступу, мінімізують кібер-ризики та гарантують надійний зв'язок у будь-якій ситуації. У сучасному світі, де інформаційні війни та кіберзлочинність стають дедалі поширенішими, роль закритих ліній буде тільки зростати[5-7].

1.2 Класифікація та види закритих ліній передачі даних

1.2.1 Огляд основних видів закритих ліній передачі

Класифікація та види закритих ліній передачі даних зазвичай базується на таких критеріях, як технології захисту, тип передачі сигналу, а також сфера використання. Закриті лінії передачі даних можна поділити на фізичні(Фізичні захищені лінії передачі, супутникові захищені лінії) і віртуальні(Лінії з

шифруванням даних, VPN (Віртуальні приватні мережі), мобільні захищені мережі). Розглянемо їх більш детально з їх основними перевагами та недоліками[8-13]:

1. **Фізичні захищені лінії передачі даних:** Фізичні захищені лінії передачі даних – це важлива складова систем безпеки в організаціях, де необхідно забезпечити високий рівень захисту даних, що передаються. Основні типи таких ліній включають оптоволоконні кабелі та виділені лінії зв'язку, які мінімізують можливість перехоплення та несанкціонованого доступу.

Оптоволоконні лінії передають дані за допомогою світлових сигналів. Вони особливо важливі для організацій, що передають великі обсяги інформації. Оптоволоконні лінії зв'язку мають значні переваги над іншими видами каналів: висока швидкість передачі даних, відсутність електромагнітних випромінювань(значно ускладнює їхнє перехоплення), кабель дуже важко пошкодити або перехопити сигнал без втручання у саму структуру волокна. Використовується у військових, фінансових та урядових установах, де критично важлива конфіденційність переданих даних.

Але наявні і значні недоліки: вартість установки (інсталяція оптоволоконних мереж є дорогим процесом), фізична вразливість (якщо кабель все ж пошкодили це може призвести до збоїв у передачі даних і потребує дорогого ремонту), вимоги до спеціального обладнання (потрібне спеціалізоване обладнання для прийому і передачі світлових сигналів, яке не є сумісним зі звичайними мідними кабелями), затрати на обслуговування (регулярне технічне обслуговування оптоволоконних мереж дороге і потребує висококваліфікованого персоналу).

Виділені лінії зв'язку використовуються тільки між двома точками без стороннього доступу до каналу. Така система важко піддається атакам через її обмежений доступ і фізичну ізоляцію. Їх основні переваги: обмежений доступ до каналу, що мінімізує ризики атак і робить легким визначення зловмисника, якщо атака сталась. Часто використовуються у банках та інших організаціях, де критичним є контроль над передачею даних.

До недоліків можна віднести: висока вартість (виділені лінії зв'язку коштують дорожче, компанія повинна утримувати окремий канал між двома точками, який не використовується іншими клієнтами), обмежена масштабованість (масштабувати виділені лінії для великої кількості точок або міжнародних зв'язків складно та дорого), менш гнучке налаштування (виділені лінії не можуть бути легко переналаштовані або змінені для нових користувачів або точок без встановлення додаткового обладнання).

2. Лінії з шифруванням даних: Ці лінії забезпечують захист за допомогою криптографічних технологій. Дані шифруються перед передачею, що дозволяє зберігати їх у конфіденційності навіть при перехопленні. TLS (Transport Layer Security)/SSL(Secure Sockets Layer) - це один із прикладів протоколи шифрування, які використовуються для захисту веб-трафіку. Це поширена технологія для захисту конфіденційної інформації, що передається через загальнодоступні мережі (наприклад, паролів і фінансових даних).

Переваги даного закритого каналу передачі даних наступні: конфіденційність даних (всі передані дані шифруються, що захищає їх від перехоплення і читання зловмисниками), інтеграція з веб-протоколами (TLS/SSL легко налаштувати для захисту HTTP-трафіку (HyperText Transfer Protocol), що робить його ідеальним для забезпечення безпеки веб-додатків, онлайн-банкінгу, інтернет-магазинів і інших веб-сервісів), аутентифікація (SSL-сертифікати підтверджують справжність серверів або клієнтів, що мінімізує ризик "людини посередині" (man-in-the-middle attack)), гнучкість (підтримує широкий спектр криптографічних алгоритмів, що дозволяє налаштувати рівень безпеки залежно від потреб організації).

Недоліки ж наступні: вартість сертифікатів (купівля та встановлення SSL-сертифікатів затратна для малих організацій), продуктивність (шифрування і розшифрування інформації потребує обчислювальних ресурсів, що збільшує час затримки для користувачів і знижує продуктивність системи при великому навантаженні), незахищеність при неправильному налаштуванні (якщо SSL налаштовано неправильно або використовується застаріла версія протоколу

(наприклад, SSL 3.0), зловмисники можуть скористатися відомими вразливостями).

3. VPN: Віртуальні приватні мережі створюють зашифрований тунель для передачі даних через загальнодоступні мережі, зокрема Інтернет. Це дозволяє забезпечити конфіденційність, анонімність і безпеку під час передачі даних. Існують різні типи VPN, зокрема Remote Access VPN для захисту віддаленого доступу до корпоративних ресурсів і Site-to-Site VPN для з'єднання локальних мереж через Інтернет.

1. Remote Access VPN

Цей тип VPN дозволяє користувачам підключатися до корпоративних мереж або інших ресурсів з будь-якого місця через Інтернет. Всі дані, що передаються між клієнтом і мережею, зашифровані.

Переваги: захист віддаленого доступу (співробітники або клієнти можуть безпечно підключатися до корпоративних мереж з будь-якої точки світу), простота використання (для підключення до VPN часто достатньо встановити VPN-клієнт і налаштувати з'єднання), шифрування даних (всі дані передаються через зашифрований тунель, що захищає або значно утруднює їх перехоплення або аналіз зловмисникам).

Недоліки: потенційне зниження продуктивності (через шифрування і додаткові шари обробки уповільнюється передача даних), безпека на стороні клієнта (якщо кінцевий пристрій (наприклад, комп'ютер або смартфон користувача) заражений шкідливим ПЗ, це може призвести до витоку даних навіть через VPN), необхідність підтримки (підтримка VPN-клієнтів і налаштування інфраструктури потребує технічного обслуговування та оновлень).

2. Site-to-Site VPN

Цей тип VPN з'єднує дві або більше локальних мереж через Інтернет, створюючи захищений тунель між ними. Найчастіше використовується для з'єднання офісів або філій компаній.

Переваги: ефективний доступ до ресурсів (організації можуть об'єднувати свої мережі і надавати доступ до загальних ресурсів (сервери, файли, програми) з різних локацій), безпека з'єднань (всі передані дані між двома мережами шифруються, що забезпечує їх захист під час передачі через Інтернет), зручність в управлінні (адміністратори можуть централізовано керувати доступом до мереж).

Недоліки: складність налаштування (Site-to-Site VPN потребує професійного налаштування на обох кінцях з'єднання, що є складним для невеликих організацій без відповідних технічних навичок), залежність від Інтернет-з'єднання (якість і стабільність VPN залежить від якості підключення до Інтернету в кожній локації що може призвести до повільної передачі даних або нестабільного з'єднання), обмежена гнучкість (на відміну від Remote Access VPN, Site-to-Site VPN менш гнучкий у випадках, коли потрібен доступ із багатьох різних місць або мобільних пристроїв).

4. Супутникові захищені лінії: Супутникові канали зв'язку є важливим засобом для передачі даних, особливо у віддалених регіонах або в місцях, де немає доступу до традиційних кабельних мереж. Вони використовують супутники на орбіті Землі для передачі сигналів між точками на поверхні. Такі системи часто застосовуються у військових, рятувальних операціях, а також у сільськогосподарських або важкодоступних регіонах.

Переваги: глобальне покриття (супутникові канали зв'язку здатні забезпечити зв'язок у будь-якій точці планети, включаючи важкодоступні або віддалені райони), незалежність від наземної інфраструктури (для функціонування супутникових каналів не потрібна розвинута наземна інфраструктура, що робить їх ідеальними для країн з недостатньо розвиненою телекомунікаційною інфраструктурою), використання в екстремальних умовах. (військові, рятувальні служби та інші організації, що працюють в екстремальних умовах, часто покладаються на супутникові канали, оскільки вони надійні в будь-яких умовах: наземні катастрофи, війни, природні лиха).

Недоліки: затримки (через відстань між Землею і супутником сигнал може мати значну затримку, що створює проблеми при передачі даних, які вимагають миттєвого відгуку, таких як відеоконференції), високі витрати (установка супутникових систем потребує значних початкових витрат на запуск і обслуговування супутників, а також на придбання спеціалізованого обладнання для підключення), обмежена пропускна здатність (хоча сучасні супутникові системи можуть забезпечувати високу швидкість передачі даних, обмеження пропускної здатності все ще існує, особливо у випадку одночасного підключення великої кількості користувачів), погодні умови (супутникові сигнали можуть бути порушені погодними умовами, такими як дощ, сніг або сильний вітер, що призводить до погіршення якості зв'язку або втрати сигналу), безпека (незважаючи на шифрування, супутникові канали можуть бути вразливими для перехоплення даних через фізичну відкритість сигналу, що вимагає використання передових криптографічних методів для захисту переданої інформації).

5. Мобільні захищені мережі: Мобільні захищені мережі забезпечують надійний рівень безпеки передачі даних завдяки використанню спеціальних протоколів шифрування та аутентифікації. Мобільні стандарти зв'язку, такі як 4G (LTE - Long-Term Evolution - довготривала еволюція, технологія мобільного зв’язку 4G) та 5G, інтегрують передові технології для захисту від перехоплення та несанкціонованого доступу.

Переваги: вбудовані механізми шифрування (сучасні мобільні мережі використовують високорівневі алгоритми шифрування, такі як AES(Advanced Encryption Standard), для захисту даних під час їх передачі, що значно ускладнює перехоплення або підробку даних зловмисниками), аутентифікація користувачів (LTE та 5G мережі вимагають взаємної аутентифікації між користувачем та мережею перед встановленням з'єднання, що ускладнює підключенню неавторизованих користувачів або пристроїв), безпека на фізичному рівні (мобільні мережі мають спеціальні заходи для захисту від атак на фізичному

рівні, зокрема захист від підміни базових станцій, наприклад, атаки типу "man-in-the-middle" з використанням фальшивих базових станцій).

Недоліки: залежність від мобільних операторів (безпека в мобільних мережах залежить від операторів, і користувачі не мають контролю над тим, наскільки ефективно застосовуються протоколи захисту на їхньому рівні), можливість атаки через слабкі місця протоколів (хоча LTE та 5G мають вдосконалені механізми безпеки, існують дослідження, які демонструють вразливості, зокрема можливість атак через радіо-інтерфейс або компрометацію аутентифікаційних протоколів), фальшиві базові станції (незважаючи на заходи захисту, зловмисники можуть використовувати фальшиві базові станції для перехоплення мобільних сигналів або атаки на користувачів).

1.2.2 Методи шифрування та захисту в закритих лініях

Зараз ми детально розглянемо основні методи шифрування та захисту в закритих лініях зв'язку, про які згадувалося раніше. Методи шифрування та захисту в закритих лініях включають комбінацію шифрування даних і фізичного захисту каналів для забезпечення максимальної безпеки. Серед ключових алгоритмів шифрування використовуються:

- AES — симетричний шифр, що шифрує дані у блоках розміром 128 біт з ключами на 128, 192 або 256 біт. Використовується у VPN, супутникових і оптоволоконних мережах для швидкої та безпечної передачі даних.

- IPsec(Internet Protocol Security) — забезпечує шифрування трафіку на рівні IP. Має два режими: транспортний (шифрує лише дані) і тунельний (шифрує весь пакет). Забезпечує також автентифікацію та контроль цілісності даних.

- TLS/SSL — використовується для захисту веб-трафіку. TLS/SSL шифрує дані за допомогою комбінації симетричного та асиметричного шифрування, забезпечуючи захист з'єднання і підтвердження автентичності сторін.

- QKD(Quantum Key Distribution) — передає ключі за допомогою квантових частинок, що робить втручання у процес неможливим без виявлення. Використовується в найкритичніших середовищах, як-от військові структури.

Окрім шифрування, важливу роль грає фізичний захист ліній, наприклад, через використання оптоволоконних або виділених ліній, які фізично ізольовані від загальнодоступних мереж і важкі для перехоплення. Такі канали активно використовуються в банківській сфері, урядових і військових структурах.

Ще один важливий аспект — взаємна автентифікація, яка забезпечує підтвердження автентичності обох сторін зв'язку, що мінімізує ризик підробки або втручання. Наприклад, в IPsec і TLS використовуються сертифікати для цього процесу.

Контроль цілісності даних (HMAC - hash-based message authentication code) гарантує, що дані не були змінені під час передачі. Цей метод широко застосовується в закритих лініях, де критично важливо виявити будь-яке втручання в інформацію, особливо в корпоративних і військових мережах[1, 11, 15].

1.2.3 Технологічні характеристики закритих ліній передачі

Технологічні характеристики закритих ліній передачі включають кілька ключових аспектів: пропускну здатність, швидкість передачі, надійність та стійкість до загроз, а також мережеву архітектуру. Пропускна здатність та швидкість визначають ефективність передачі даних, а надійність залежить від фізичної безпеки та використаних методів захисту. Важливо також враховувати архітектуру та інфраструктурні вимоги мереж, оскільки різні види захищених ліній мають свої вимоги до апаратного та програмного забезпечення для забезпечення їх ефективної роботи.

Фізичні захищені лінії передачі, зокрема оптоволоконні мережі, забезпечують найвищий рівень пропускної здатності та швидкості передачі даних. Їхні ключові характеристики[3, 9]:

- Пропускна здатність і швидкість передачі даних: Оптоволоконні лінії здатні передавати дані зі швидкістю до 100 Гбіт/с і більше, що робить їх найефективнішими серед закритих ліній передачі даних .

- Надійність і стійкість до зовнішніх загроз: Ці лінії мають високу стійкість до зовнішніх загроз через фізичну ізоляцію. Оптоволоконні кабелі майже неможливо перехопити без фізичного втручання, що робить їх одними з найбезпечніших варіантів для захищених комунікацій. Ймовірність перехоплення сигналу дуже низька (менше ніж 1 на 10 мільйонів випадків).

- Мережева архітектура та інфраструктурні вимоги: Архітектура фізичних ліній включає виділені оптоволоконні канали та спеціальне обладнання для контролю трафіку (маршрутизатори, комутатори). Апаратне забезпечення потребує оптичних приймачів/передавачів і високошвидкісних комутаторів. Програмне забезпечення використовується мінімально, оскільки фізична ізоляція забезпечує більшу частину безпеки. Розгортання таких ліній вимагає значних інвестицій, особливо на великі відстані.

Лінії з шифруванням даних використовують криптографічні методи для забезпечення безпеки переданих даних. Їхні ключові характеристики[3, 10]:

- Пропускна здатність і швидкість передачі даних: Пропускна здатність ліній з шифруванням може сягати до 10 Гбіт/с, однак процес шифрування вимагає додаткових обчислювальних ресурсів, що може призводити до затримок і зниження швидкості на деяких етапах.

- Надійність і стійкість до зовнішніх загроз: Лінії з шифруванням забезпечують високий рівень захисту від перехоплення та модифікації даних завдяки використанню сучасних криптографічних алгоритмів (наприклад, TLS/SSL, IPsec). Проте вразливості можуть виникати через неправильні налаштування або використання застарілих версій протоколів. При правильній реалізації ймовірність успішної атаки дуже низька (менше 0,01%).

- Мережева архітектура та інфраструктурні вимоги: Лінії з шифруванням даних використовують загальнодоступні мережі (наприклад, Інтернет) з додаванням шифрувальних протоколів для захисту даних. Апаратне

забезпечення може включати стандартне мережеве обладнання, але для підтримки високої продуктивності можуть знадобитися спеціалізовані шифрувальні пристрої. Програмне забезпечення, зокрема протоколи, як-от TLS або IPsec, відповідає за шифрування даних у мережі.

VPN забезпечують захищений зв'язок через загальнодоступні мережі, використовуючи шифрування для передачі даних. Основні характеристики[11, 14-15]:

- Пропускна здатність і швидкість передачі даних: Пропускна здатність VPN залежить від мережі, через яку передаються дані, та апаратного забезпечення для шифрування/дешифрування трафіку. Висококласні корпоративні рішення можуть забезпечити швидкість до 10 Гбіт/с, тоді як звичайні підключення мають швидкість 1-2 Гбіт/с. Шифрування додає додаткові затримки, що може знижувати загальну швидкість.

- Надійність і стійкість до зовнішніх загроз: VPN забезпечує високий рівень захисту через зашифровані тунелі (OpenVPN, IPsec). Проте стійкість до загроз залежить від правильного налаштування шифрування. Атаки можливі на кінцеві точки VPN або через вразливі протоколи. При належній реалізації ймовірність успішного злому низька (менше 0,05%).

- Мережева архітектура та інфраструктурні вимоги: VPN будується на основі публічних мереж, зазвичай Інтернету, із шифруванням трафіку між кінцевими точками. Апаратне забезпечення зазвичай включає стандартні мережеві пристрої, але може вимагати спеціальних VPN-серверів і клієнтів. Програмне забезпечення використовує протоколи, такі як OpenVPN, IPsec, L2TP(Layer 2 Tunneling Protocol) або SSL/TLS, для створення захищених тунелів.

Супутникові захищені лінії забезпечують передачу даних через супутники, що особливо важливо для віддалених регіонів. Основні характеристики[12, 16-17, 19]:

- Пропускна здатність і швидкість передачі даних: Супутникові системи можуть забезпечувати швидкість передачі даних до 100 Мбіт/с або більше. Однак

через відстань між супутником та Землею часто виникають затримки до 600 мс, що може впливати на продуктивність.

- Надійність і стійкість до зовнішніх загроз: Супутникові канали вразливі до ризику перехоплення сигналу через широке покриття та відсутність фізичного захисту кабелів. Проте сучасні системи використовують передові методи шифрування, такі як AES-256, що значно знижує ризик. Урядові та військові супутникові мережі часто використовують додаткові методи безпеки, такі як квантова криптографія (QKD), щоб підвищити надійність.

- Мережева архітектура та інфраструктурні вимоги: Супутникові лінії включають супутники на орбіті, наземні станції, антени і супутникові термінали для підтримки зв'язку. Апаратне забезпечення включає супутникові модеми, антени та приймачі. Програмне забезпечення включає системи управління доступом і шифрування для захисту переданих даних. Підтримка супутникових ліній вимагає значних інвестицій у запуск та обслуговування супутників.

Мобільні захищені мережі (LTE/5G) забезпечують високошвидкісну передачу даних із застосуванням сучасних методів шифрування. Основні характеристики[3, 13, 17]:

- Пропускна здатність і швидкість передачі даних: 5G забезпечує швидкість передачі даних до 10 Гбіт/с, що робить його перспективним для мобільних комунікацій. LTE, попередник 5G, забезпечує швидкість до 1 Гбіт/с. Продуктивність може змінюватися залежно від мережевого покриття і завантаженості.

- Надійність і стійкість до зовнішніх загроз: LTE/5G використовують складні алгоритми шифрування (наприклад, AES), що забезпечує високий рівень захисту. Проте мобільні мережі можуть бути вразливі до атак, таких як "man-in-the-middle". 5G підвищує рівень безпеки порівняно з LTE, але кінцеві точки можуть залишатися вразливими до атак.

- Мережева архітектура та інфраструктурні вимоги: LTE і 5G покладаються на інфраструктуру мобільних операторів, що включає базові станції, антени та мобільні термінали. 5G вимагає складніших антен і новітніх мережевих

технологій для забезпечення високої пропускної здатності. Програмне забезпечення мобільних мереж підтримує шифрування даних і аутентифікацію через SIM-карти. Інфраструктура потребує значних інвестицій у розгортання базових станцій, особливо для 5G, який потребує щільнішого покриття для забезпечення стабільної швидкості передачі даних.

Отже, після розгляду деяких основних характеристик закритих каналів передачі даних, ми можемо підсумувати, що кожен вид каналів має свої сильні та слабкі сторони, що робить їх придатними для різних умов і завдань. Фізичні захищені лінії демонструють найвищу швидкість і надійність, але їхнє впровадження вимагає значних інвестицій в інфраструктуру. VPN надають хороший баланс між безпекою та гнучкістю, хоча можуть стикатися з проблемами затримок та налаштувань. Мобільні захищені мережі (LTE/5G) забезпечують високу продуктивність, але їх ефективність залежить від покриття та є ризик вразливості кінцевих точок. Супутникові лінії є незамінними для віддалених регіонів, проте вони мають суттєві затримки і вразливі до перехоплення. Лінії з шифруванням даних гарантують високий рівень захисту, але потребують ресурсів для підтримки швидкості. Кожен із цих каналів має свої специфічні переваги, що дозволяє вибирати оптимальний варіант залежно від конкретних вимог та умов експлуатації[3, 9-17, 19].

1.3 Будова закритого каналу передачі даних

Закритий канал передачі даних складається з наступних основних компонентів[8-13]:

1. Джерело даних — пристрій або система, що генерує або надає інформацію, яка потребує захисту.

2. Методи шифрування (необов'язкове) — технології, що використовуються для забезпечення конфіденційності даних. Наприклад, AES, IPsec або TLS.

3. Фізичний або віртуальний канал передачі — шлях, по якому передаються дані. Найчастіше він складається з інфраструктурного обладнання —

оптоволоконні кабелі, маршрутизатори, комутатори, супутникові антени, мобільні базові станції, сервери, VPN-тунелі, тощо.

4. Контроль доступу та автентифікація (необов'язкове) — забезпечують підтвердження, що до мережі підключаються лише авторизовані користувачі. Використовуються сертифікати, ключі або інші механізми.

5. Цільове призначення — отримувач даних, що приймає і обробляє захищену інформацію.

Будова кожного типу каналу[8-13]:

Фізичні захищені лінії починаються з пристроїв-джерел, які генерують або надають інформацію для передачі. Це можуть бути комп'ютери, сервери чи інші мережеві пристрої, які підключені до фізичних ліній зв'язку. Шифрування може бути застосоване для додаткового захисту даних, і часто використовуються такі методи, як AES або навіть квантове шифрування (QKD), що забезпечують найвищий рівень безпеки. Сам канал передачі представлений оптоволоконними кабелями або виділеними лініями зв'язку, що забезпечують фізичний захист від перехоплення даних завдяки відсутності електромагнітного випромінювання. Контроль доступу часто реалізується на фізичному рівні шляхом обмеження доступу до інфраструктури. Отримувачем даних можуть бути будь-які пристрої, які приймають інформацію через фізичний канал, наприклад інші сервери або комутатори.

Лінії з шифруванням даних передбачають, що дані генеруються або надаються серверами чи клієнтами, які ініціюють передачу. Дані шифруються перед відправкою за допомогою криптографічних протоколів, таких як TLS, SSL або IPsec, що забезпечують конфіденційність інформації навіть при передачі через загальнодоступні мережі, як-от Інтернет. Сам канал передачі — це публічна мережа, яка захищена за допомогою зазначених протоколів шифрування. Контроль доступу реалізується через сертифікати та ключі шифрування, які підтверджують автентичність користувачів або пристроїв. Отримувачем даних можуть бути сервери, клієнти або інші кінцеві пристрої, які використовують ті ж протоколи для дешифрування інформації.

VPN використовуються для створення захищених тунелів через Інтернет, забезпечуючи безпечний доступ до корпоративних мереж або ресурсів з віддалених місць. Джерелом даних можуть бути клієнти або сервери, які підключаються до VPN. Для шифрування даних використовуються сучасні алгоритми, такі як AES-256 або ChaCha20(швидкий потоковий шифр, створений Д. Бернштейном), які створюють зашифрований тунель для передачі даних. Сам канал передачі представлений віртуальними тунелями, створеними через загальнодоступну мережу, що дозволяє захистити інформацію під час її переміщення. Контроль доступу до VPN реалізується через багатофакторну автентифікацію, що мінімізує ризики несанкціонованого підключення. Дані приймаються віддаленими клієнтами або серверами, які є кінцевими точками VPN-з'єднання.

Супутникові лінії забезпечують передачу даних через супутники, що особливо важливо для віддалених районів або регіонів, де немає доступу до наземної інфраструктури. Дані генеруються наземними станціями або мобільними терміналами, які підключаються до супутникової мережі. Шифрування виконується за допомогою алгоритмів, таких як AES або TLS, що забезпечує захист трафіку під час його передачі через радіосигнали. Сам канал передачі реалізується за допомогою радіосигналів між супутниками та наземними станціями, що дозволяє обмінюватися інформацією на великі відстані. Контроль доступу реалізується за допомогою криптографічних ключів або автентифікації користувачів, щоб забезпечити безпечний доступ до мережі. Дані приймаються наземними станціями або мобільними терміналами, які обробляють сигнал, отриманий від супутника.

Мобільні захищені мережі (LTE/5G) використовуються для забезпечення захищеного доступу до мобільного Інтернету та корпоративних ресурсів. Джерелом даних можуть бути мобільні пристрої, такі як смартфони або IoT-пристрої(Інтернету речей), які генерують дані. Шифрування забезпечується за допомогою алгоритмів, таких як AES-256 або EPS(Evolved Packet System) Encryption, що гарантує конфіденційність переданої інформації. Канал передачі

реалізується за допомогою радіосигналів через мобільні мережі, зокрема LTE або 5G, що дозволяє швидко передавати великі обсяги даних. Контроль доступу до мобільних мереж здійснюється за допомогою автентифікації користувачів (EAP-AKA(Extensible Authentication Protocol - Authentication and Key Agreement), SIM-карти), що ускладнює підключення неавторизованих пристроїв. Отримувачами даних є базові станції, сервери або інші пристрої, що приймають інформацію від мобільних терміналів.

Для кожного з раніше згаданих закритих каналів передачі даних наведено відповідний компонент/пристрій/рішення в таблиці 1.1. У рис. 1.1 наведено узагальнену схематичну будову закритого каналу передачі даних.

Таблиця 1.1 — Узагальнена схема основних компонентів закритої лінії передачі даних

Вид каналу передачі	**Джерело даних**	**Метод шифрування**	**Фізичний або віртуальний канал**	**Контроль доступу та автентифікація**	**Отримувач даних**
Фізичні захищені лінії	Пристрої-джерела	AES, QKD	Оптоволоконні кабелі, виділені лінії	Фізичний доступ	Пристрої-отримувачі
Лінії з шифруванням даних	Сервери або клієнти	TLS, SSL, IPsec	Інтернет	Сертифікати, криптографічні ключі	Сервери або клієнти
VPN	Клієнти або сервери	AES-256, ChaCha20	Інтернет (віртуальні тунелі)	Багатофакторна аутентифікація	Віддалені клієнти або сервери
Супутникові лінії	Наземні станції або мобільні термінали	AES, TLS	Радіосигнали через супутники	Криптографічні ключі, автентифікація	Наземні станції або мобільні термінали
Мобільні захищені	Мобільні	AES-256, EPS	Радіосигнали, мобільні	EAP-AKA,	Базові станції або

мережі (LTE/5G)	пристрої	Encryption	мережі	SIM-карти	сервери

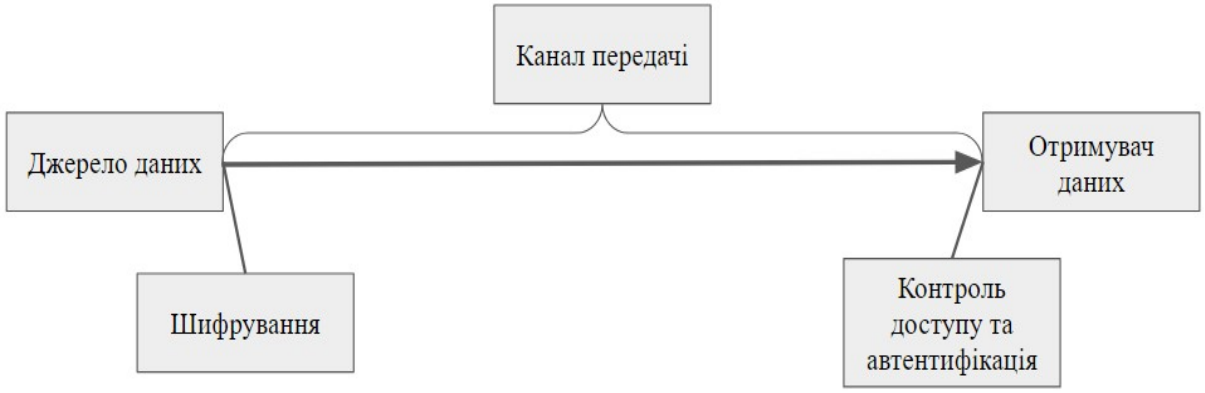


Рисунок 1.1 — Узагальнена схема будову закритого каналу передачі даних.

Кожен вид каналу передачі має свою специфіку в забезпеченні безпеки, що робить його більш ефективним для певних задач і умов використання[8-13].

1.4 Висновок до першого розділу

У першому розділі було здійснено детальний аналіз концепції закритих ліній передачі даних, які сьогодні є важливим елементом інформаційної безпеки для організацій різних рівнів. Закриті лінії передачі даних визначаються як спеціально розроблені канали зв'язку, що забезпечують захищену та конфіденційну передачу даних між двома або більше сторонами. Вони використовуються для мінімізації ризиків перехоплення чи несанкціонованого доступу до інформації завдяки використанню шифрування та інших технологій захисту.

Роль технологій захисту інформації стрімко зростає через постійне збільшення залежності сучасного світу від цифрових комунікацій. З кожним роком вимоги до безпеки інформації стають жорсткішими. Державні установи, банки, медичні заклади, енергетичні компанії та інші критичні інфраструктури працюють із величезними обсягами конфіденційних даних, що потребують надійного захисту. Закони та нормативні акти у сфері кібербезпеки постійно оновлюються, встановлюючи все більш суворі стандарти захисту інформації. Це

зумовлює потребу в постійному вдосконаленні засобів шифрування, фізичних систем захисту каналів передачі даних та управління доступом.

Закриті лінії передачі даних є одним із найважливіших елементів у забезпеченні інформаційної безпеки сучасних організацій. Їх основна роль полягає в тому, щоб мінімізувати ризики перехоплення інформації та забезпечити надійний канал для обміну конфіденційними даними. У той час як відкриті мережі, такі як Інтернет, можуть бути вразливими до різних типів атак, закриті лінії забезпечують фізичну або віртуальну ізоляцію каналів, що робить їх надзвичайно стійкими до зломів. Наприклад, оптоволоконні мережі є практично непроникними для несанкціонованого втручання завдяки своїй фізичній структурі, а VPN дозволяють шифрувати трафік навіть при використанні загальнодоступних мереж.

Закриті лінії передачі даних також забезпечують високу надійність зв'язку, що є критичним для організацій, які не можуть дозволити собі втрату даних або перебої у передачі інформації. Вони використовуються в державних установах, військових структурах, фінансових організаціях та інших сферах, де безпека і цілісність даних мають пріоритетне значення.

Розвиток технологій для захисту інформації є невід'ємною частиною сучасної кібербезпеки. Кожен новий крок у розвитку технологій, таких як квантове шифрування або захищені мобільні мережі, допомагає посилити захист від постійно еволюціонуючих кіберзагроз. Для організацій, що працюють із конфіденційною інформацією, це питання стає особливо важливим, оскільки від надійності захисту часто залежить їх успішне функціонування, а іноді й сама безпека національних структур.

Окремо було розглянуто будову закритих каналів передачі даних, яка передбачає використання таких елементів, як фізичні середовища (наприклад, мідні дроти або оптоволоконні кабелі), засоби шифрування, а також механізми автентифікації та контролю доступу. Сучасні закриті канали поєднують різні рівні захисту, включаючи фізичні бар'єри, криптографічні алгоритми та

програмні засоби захисту, що дозволяє досягти максимальної стійкості до кіберзагроз.

Закриті лінії передачі даних, як і інші захищені канали, є критично важливими для забезпечення безпеки у світі, де цифрова інформація стала однією з найцінніших речей. Вдосконалення цих технологій дозволяє не лише уникати загроз кіберзлочинців, а й забезпечувати надійний захист даних в умовах постійно зростаючих кіберризиків.

РОЗДІЛ 2 ДОСЛІДЖЕННЯ РОБОТИ ЗАКРИТОЇ ЛІНІЇ ПЕРЕДАЧІ ДАНИХ

2.1 Методи шифрування у закритих лініях зв'язку

У даному підрозділі ми будемо розглядати ключові методи шифрування, які застосовуються в закритих лініях зв'язку для забезпечення їхньої конфіденційності, цілісності та автентичності. Шифрування відіграє фундаментальну роль у захисті даних, особливо у контексті захищених каналів передачі інформації, таких як фізичні захищені лінії, VPN, супутникові канали та мобільні мережі. Оскільки різні методи шифрування мають свої особливості та сфери застосування, їх вибір залежить від вимог до рівня безпеки, продуктивності та надійності системи. У цьому підрозділі ми детально розглянемо два основні типи шифрування – симетричне та асиметричне, криптографічні протоколи, що забезпечують безпеку каналів зв'язку, а також апаратні й програмні рішення для шифрування даних.

2.1.1 Симетричні та асиметричні алгоритми шифрування

Симетричні та асиметричні алгоритми шифрування є двома основними підходами до захисту інформації в сучасних закритих лініях передачі даних, і кожен з них має свої переваги та недоліки.

Симетричне шифрування засноване на використанні одного і того ж ключа як для шифрування, так і для дешифрування даних. Цей тип алгоритмів характеризується високою швидкістю обробки інформації, оскільки процес шифрування і дешифрування є відносно простим з обчислювальної точки зору. Його головна перевага — висока швидкість і ефективність, що робить цей метод ідеальним для великих обсягів даних. Однак ключовий недолік полягає у складності безпечного обміну ключами: якщо ключ перехоплять, зловмисник отримає доступ до всієї інформації. Популярними симетричними алгоритмами є AES та DES (Data Encryption Standard), які широко використовуються для забезпечення конфіденційності даних.

Асиметричне шифрування, або криптографія з відкритим ключем, використовує пару ключів: відкритий — для шифрування, і приватний — для дешифрування. Асиметричне шифрування є більш безпечним для передачі ключів, оскільки немає необхідності в передачі приватного ключа. Однак цей метод значно повільніший за симетричне шифрування через складні математичні операції, які потребують більше обчислювальних ресурсів. До основних асиметричних алгоритмів відносяться RSA (Rivest-Shamir-Adleman) та ECC (Elliptic Curve Cryptography).

Порівнюючи ці два методи, можна виділити наступні ключові відмінності. Симетричне шифрування швидше та ефективніше, але потребує надійного механізму передачі ключів. Асиметричне, хоча й безпечніше для обміну ключами, є ресурсозатратнішим. Сучасні системи комбінують ці методи: асиметричне шифрування застосовують для передачі ключів, а симетричне — для захисту великих обсягів даних[3, 8].

У різних типах закритих ліній передачі даних застосовуються різні алгоритми шифрування, залежно від вимог до захисту і продуктивності.

У фізично захищених лініях шифрування виконує допоміжну роль, адже безпека забезпечується фізичним захистом. Тому симетричні алгоритми шифрування, такі як AES, часто є оптимальним вибором, оскільки вони забезпечують високу швидкість шифрування і дешифрування[18].

У лініях з шифруванням даних, де безпека є головним пріоритетом, зазвичай використовують як симетричні, так і асиметричні алгоритми. В лініях з шифруванням даних, де безпека є критично важливою, комбінують асиметричні (RSA, ECC) для обміну ключами та симетричні (AES) для шифрування, що дозволяє досягти балансу між швидкістю та захистом.

У VPN-з'єднаннях використовуються обидва типи шифрування. Під час ініціалізації з'єднання асиметричне шифрування (RSA або ECC) використовується для захищеного обміну ключами, а симетричне шифрування (AES) застосовується для передачі даних після встановлення захищеного каналу. Це дозволяє забезпечити високу продуктивність та безпеку.

У супутникових захищених лініях передачі також застосовуються симетричні та асиметричні алгоритми. Супутниковий зв'язок через високу вразливість до перехоплення використовує симетричні алгоритми (AES) для шифрування даних і асиметричні для обміну ключами, гарантучи конфіденційність[26].

У мобільних захищених мережах, таких як LTE та 5G, шифрування відіграє ключову роль. У мобільних мережах LTE і 5G симетричне шифрування (AES) забезпечує швидкість і захист радіоінтерфейсу, а асиметричні алгоритми підтримують автентифікацію і створення захищеного каналу між пристроєм і мережею [28].

AES, RSA та ECC[3, 8, 17-19]:

1. AES — симетричний алгоритм шифрування, розроблений у 1998 році Вінсентом Рейменом і Жоаном Дайменом, які перемогли в конкурсі NIST(The National Institute of Standards and Technology). У 2001 році AES став стандартом для захисту державної та комерційної інформації, замінивши DES.

Він підтримує ключі довжиною 128, 192 і 256 біт, причому AES-256 є найзахищенішим і широко використовується.

AES є блочним алгоритмом, де дані розбиваються на блоки по 128 біт і обробляються через кілька раундів. Ось докладніший опис кожного з етапів алгоритму[3, 8]:

Підстановка байтів (англ. SubBytes) — кожен байт блоку замінюється на новий за таблицею S-box для нелінійності, що підвищує стійкість до криптоаналізу.

Перемішування рядків (англ. ShiftRows) — байти матриці циклічно зміщуються вліво для розподілу даних, посилюючи дифузію.

Перестановка стовпців (англ. MixColumns) — стовпці матриці змішуються через матричне множення в скінченному полі для розсіювання даних.

Додавання раундового ключа (англ. AddRoundKey) — кожен байт матриці об’єднується з байтом раундового ключа за допомогою операції XOR (побітове додавання за модулем 2). Ключі для кожного раунду генеруються за допомогою спеціального алгоритму розширення ключа, що базується на початковому ключі шифрування.

Після цих чотирьох етапів дані проходять через ще кілька раундів (кількість раундів залежить від довжини ключа: 10 для AES-128, 12 для AES-192 і 14 для AES-256). Наприкінці останнього раунду виконується все, крім етапу перестановки стовпців, і результатом є зашифрований блок даних.

Більша кількість раундів забезпечує вищу безпеку, але при цьому трохи знижується продуктивність алгоритму через додаткові обчислення.

Основною особливістю AES є його висока швидкість і ефективність при використанні на різних платформах, зокрема на апаратних пристроях, де він може бути реалізований без значних ресурсних витрат. AES також вважається стійким до відомих атак, таких як атака грубою силою, оскільки кількість можливих ключів надзвичайно велика. AES-256 має 2^{256} можливих комбінацій

ключів, що робить його практично незламним для сучасних обчислювальних потужностей[17-18].

2. RSA — асиметричний алгоритм шифрування, створений у 1977 році Рональдом Рівестом, Аді Шаміром і Леонардом Адлеманом. Це один із найстаріших і найпоширеніших методів криптографії з відкритим ключем, що забезпечує безпечний обмін даними.

RSA– використовує пару ключів: відкритий — для шифрування, і приватний — для дешифрування. Відкритий ключ може бути доступним публічно, але тільки власник приватного ключа може розшифрувати інформацію. Сучасні реалізації застосовують ключі довжиною щонайменше 2048 біт, а ключі у 4096 біт вважаються найзахищенішими.

Математична основа RSA

RSA базується на труднощі факторизації дуже великих чисел. Алгоритм працює наступним чином[17-18, 28]:

1. Генерація ключів:

Обираються два великі прості числа p і q.

Обчислюється модуль $N = p \cdot q$, який буде використовуватися як частина публічного і приватного ключів.

Також обчислюється значення функції Ейлера $\varphi(N) = (p-1)(q-1)$, яке використовується для генерації відкритого і закритого ключів.

Обирається відкрите значення e, яке є цілим числом, взаємно простим з $\varphi(N)$. Часто використовують значення $e = 65537$, яке забезпечує високу ефективність і безпеку.

Приватний ключ d обчислюється за допомогою розв'язку рівняння $e \cdot d \equiv 1 \, mod \varphi(N)$(тобто d є мультиплікативною оберненою до e за модулем $\varphi(N)$).

2. Шифрування:

Повідомлення M (що представляє собою число, менше ніж N) шифрується відкритим ключем e та модулем N за формулою 2.1:

$$C = M^e \, mod N \tag{2.1}$$

де C – це зашифрований текст.

3. Дешифрування:

Для відновлення початкового повідомлення M, зашифрований текст C обчислюється за допомогою приватного ключа d за формулою 2.2:

$$M = C^d \, mod N \tag{2.2}$$

RSA забезпечує високу безпеку завдяки використанню двох ключів і складності факторизації великих чисел. Сучасні комп'ютери не можуть ефективно розкласти великі числа на множники, що робить RSA стійким до атак. Однак, для забезпечення високої безпеки, ключі RSA повинні бути достатньо довгими (найменша рекомендована довжина ключа – 2048 біт, хоча 4096-бітні ключі забезпечують ще вищий рівень безпеки).

Головний недолік RSA — низька ефективність при роботі з великими обсягами даних, адже шифрування і дешифрування потребують значних обчислювальних ресурсів. Тому RSA зазвичай застосовується для шифрування симетричних ключів (наприклад, у протоколах TLS), а не для великих файлів.

3. ECC – це асиметричний алгоритм шифрування, заснований на властивостях еліптичних кривих над скінченими полями. Розроблений у 1980-х роках Віктором Міллером і Нейлом Кобліцем, він став популярним завдяки ефективності та високій безпеці при використанні коротких ключів.

ECC використовує точки на еліптичних кривих і операції з ними для шифрування, забезпечуючи високу криптографічну стійкість при значно меншому розмірі ключів порівняно з іншими методами. Це робить ECC ефективним і перспективним у сучасних системах безпеки.

Математична основа ECC: Еліптична крива в контексті ECC задається рівнянням виду 2.3:

$$y^2 = x^3 + ax + b \, mod p \tag{2.3},$$

де a і b – це константи, які визначають форму кривої, а p – це просте число, що задає модульне поле. Точки на цій кривій, які задовольняють це рівняння, використовуються для криптографічних операцій.

Основним принципом ECC є проблема дискретного логарифма на еліптичній кривій (ECDLP), яка полягає в тому, що при заданій точці P на кривій

та її кратній точці $Q = kP$, де k – скаляр, дуже важко знайти значення k, навіть якщо P і Q відомі. Це робить ECC надзвичайно стійким до зламів, оскільки обчислювальна складність цієї проблеми зростає експоненціально зі збільшенням розміру ключа.

ECC забезпечує високу безпеку з коротшими ключами, ніж RSA: 256-бітний ECC еквівалентний 3072-бітному RSA. Це робить його ідеальним для пристроїв з обмеженими ресурсами. Завдяки меншому розміру ключів, ECC підвищує продуктивність у мережах з високими вимогами та зменшує обсяг даних для шифрування, що важливо для середовищ із низькою пропускною здатністю. Алгоритм стійкий до грубої сили й квантових атак.

ECC широко використовується у цифрових підписах (ECDSA), обміні ключами (ECDH) і протоколах безпеки (TLS). Його ефективність робить ECC оптимальним для мобільних мереж, VPN і захищених каналів, де важливі економія ресурсів і швидкість[3, 17-19, 26].

2.1.2 Криптографічні протоколи для захищених каналів (SSL/TLS, IPsec)

Криптографічні протоколи є основними механізмами, що забезпечують безпеку даних під час їх передачі через різні мережі. Вони включають в себе алгоритми шифрування, аутентифікації та механізми захисту цілісності даних. Основна мета криптографічних протоколів – захистити інформацію від несанкціонованого доступу, зламу або модифікації під час її передачі. Протоколи визначають правила шифрування даних, керування ключами та створення безпечних каналів для обміну інформацією. Найбільш популярні криптографічні протоколи включають SSL/TLS, IPsec та інші, які застосовуються для захисту конфіденційності, автентифікації користувачів та забезпечення цілісності даних у різних мережевих середовищах.

У фізично захищених лініях передачі даних безпека забезпечується самим середовищем, наприклад, оптоволоконними кабелями, які важко перехопити. Однак у деяких випадках для додаткового захисту застосовуються протоколи типу IPsec, щоб зашифрувати дані на випадок порушення лінії.

У лініях з шифруванням безпека базується на криптографічних протоколах. SSL/TLS забезпечує шифрування інтернет-трафіку та автентифікацію між серверами та клієнтами, тоді як IPsec використовується для захисту IP-пакетів у складних мережах.

VPN використовують IPsec або SSL/TLS для створення тунелів, через які передаються зашифровані дані. IPsec забезпечує шифрування на рівні мережевих пакетів, що дозволяє захищати передачу між двома точками в мережі. SSL/TLS VPN зазвичай використовуються для захисту віддаленого доступу до ресурсів, де клієнт встановлює захищений канал з сервером через браузер або спеціальне програмне забезпечення.

Супутникові лінії особливо вразливі до перехоплення через відкриту природу сигналу. Для захисту застосовують AES для шифрування даних і IPsec для забезпечення конфіденційності трафіку між наземними станціями й супутниками.

У мобільних захищених мережах, таких як LTE та 5G, використовуються спеціалізовані криптографічні протоколи для шифрування та автентифікації трафіку між пристроями і базовими станціями. Протоколи, такі як EPS-AKA для LTE і 5G-AKA(5G Authentication and Key Agreement) для 5G, забезпечують автентифікацію та захист від атак на рівні доступу. Ці протоколи підтримують симетричне шифрування, яке дозволяє ефективно захищати трафік при високій швидкості передачі даних, що є важливим для мобільних мереж.

Таким чином, криптографічні протоколи адаптуються до потреб конкретної мережі або середовища, забезпечуючи належний рівень захисту на кожному рівні комунікації [3, 10-11, 19-21].

IPsec, SSL/TLS, EPS-AKA і 5G-AKA[10-13, 19-23]**:**

IPsec, створений Інженерною радою Інтернету (IETF), забезпечує безпеку на рівні мережевих протоколів через шифрування та аутентифікацію IP-пакетів. Він працює у двох режимах: тунелювання, що шифрує весь трафік між вузлами, і транспорту, який захищає окремі пакети. Основні компоненти IPsec включають Authentication Header (AH) для аутентифікації та перевірки цілісності даних і

Encapsulating Security Payload (ESP) для шифрування. Обмін ключами здійснюється через протокол IKE(Internet Key Exchange), який забезпечує конфіденційність і взаємну автентифікацію. IPsec широко використовується в корпоративних VPN і для захисту мережевих шлюзів, оскільки забезпечує шифрування та аутентифікацію всього трафіку незалежно від його типу[11, 19-21].

SSL/TLS, створений Netscape, став стандартом для захисту інтернет-комунікацій. Його основна функція — шифрування трафіку між клієнтами та серверами для забезпечення безпечної передачі даних. Працюючи на транспортному рівні моделі OSI(Open Systems Interconnection), SSL/TLS створює захищений канал після взаємної автентифікації через процес "handshake". Під час "handshake" узгоджуються криптографічні алгоритми, генерується сесійний ключ і перевіряються цифрові сертифікати. Після цього дані шифруються симетричними ключами. SSL/TLS широко застосовується в протоколі HTTPS(HyperText Transfer Protocol Secure) для захисту користувацьких даних і є популярним завдяки простій інтеграції та високій надійності[10, 21].

EPS-AKA є криптографічним протоколом автентифікації, який був розроблений для мереж LTE. Він працює на рівні мобільної інфраструктури, забезпечуючи безпечну автентифікацію користувачів та передачу даних між мобільними пристроями і базовими станціями. Протокол працює через обмін викликами: мережа надсилає випадковий номер, а мобільний пристрій відповідає, використовуючи ключ K із SIM-карти. Після перевірки автентичності встановлюється захищений канал. EPS-AKA також шифрує дані, забезпечуючи конфіденційність зв’язку. Цей протокол обрано для LTE завдяки високій продуктивності, низьким затримкам і надійному захисту трафіку в умовах великої кількості користувачів[12].

5G-AKA є наступником EPS-AKA і розроблений спеціально для мереж 5G. Він працює за схожою схемою, однак з покращеними можливостями захисту, оскільки мережі 5G пропонують більше можливостей для нових видів атак через свою більшу складність і швидкість. Як і EPS-AKA, він базується на

автентифікації через виклики та підписані відповіді, але включає покращений захист різних типів трафіку і взаємодії між компонентами мережі. 5G-AKA підтримує розподілені та віртуалізовані інфраструктури, що робить його важливим для IoT та автономних систем. Протокол обраний для 5G через здатність забезпечувати безпеку в умовах високих швидкостей передачі даних і великої кількості одночасних підключень[13, 23].

Кожен із цих протоколів був розроблений з урахуванням специфіки відповідних технологій і середовищ, в яких вони використовуються. IPsec є незамінним для захисту мережевих тунелів і корпоративних VPN, SSL/TLS – для безпечної передачі даних у веб-просторі, тоді як EPS-AKA і 5G-AKA пристосовані до потреб мобільних мереж, забезпечуючи швидку та безпечну автентифікацію користувачів у високонавантажених мобільних інфраструктурах.

2.1.3 Апаратне та програмне забезпечення для шифрування

Апаратне, програмне та програмно-апаратне забезпечення для шифрування виконують критичні функції в сучасних системах захисту даних, забезпечуючи конфіденційність і цілісність переданих даних. Апаратне забезпечення для шифрування зазвичай включає спеціалізовані пристрої, такі як криптографічні модулі, маршрутизатори з підтримкою шифрування та апаратні VPN-шлюзи. Програмне забезпечення, у свою чергу, реалізується на загальнодоступних обчислювальних системах і включає різноманітні програми та утиліти для шифрування, такі як OpenVPN або OpenPGP. Програмно-апаратне забезпечення об'єднує переваги обох підходів, забезпечуючи ефективне використання апаратних ресурсів і гнучкість програмного рішення.

Основна відмінність між апаратним і програмним шифруванням полягає в тому, що апаратні рішення надають вищу продуктивність завдяки оптимізованим процесорам та спеціалізованим схемам, які швидко виконують криптографічні обчислення. Вони також пропонують кращу стійкість до

фізичних атак, оскільки більшість таких пристроїв включають механізми захисту від спроб несанкціонованого доступу. Проте апаратні рішення зазвичай дорожчі, оскільки вимагають розробки та виробництва спеціалізованих компонентів.

Програмне забезпечення для шифрування є більш гнучким і доступним, адже не вимагає спеціальних пристроїв. Вартість такого рішення, зазвичай, є нижчою, але продуктивність може страждати через залежність від загального процесора комп'ютера. Також, у випадку атак на саму операційну систему або програмні баги, програмне забезпечення може бути вразливішим до атак, особливо якщо не було проведено належних оновлень безпеки.

Програмно-апаратні рішення намагаються досягти компромісу між високою продуктивністю апаратного забезпечення та гнучкістю програмного. Ці рішення дозволяють гнучко змінювати криптографічні алгоритми і параметри, інтегруючи їх в апаратну частину для досягнення максимальної ефективності. Це може бути вигідно для складних або спеціалізованих середовищ, таких як корпоративні мережі або високозахищені системи, що потребують постійного оновлення[3, 6-7].

У закритих лініях передачі даних використовуються різні типи шифрувального забезпечення залежно від специфіки та вимог мережі. У фізичних захищених лініях передачі, таких як виділені оптоволоконні канали, часто використовуються апаратні пристрої для шифрування, такі як мережеві шифратори, що інтегруються в маршрутизатори або комутатори. Наприклад, пристрої Cisco Catalyst, приклад якого можна побачити на рис. 2.1, або продукти компанії Thales є популярними варіантами для забезпечення надійного апаратного шифрування на високих швидкостях без значних затримок[9].

Рисунок 2.1 — Cisco Catalyst 9300 series

У лініях із шифруванням даних часто використовуються як апаратні, так і програмні рішення. У випадку шифрування на рівні транспортного протоколу (наприклад, IPsec), використовуються апаратні VPN-шлюзи або маршрутизатори з підтримкою криптографічних протоколів. Програмні рішення, такі як OpenVPN або IPsec вбудований в операційні системи, також використовуються для забезпечення шифрування даних при використанні менших обчислювальних ресурсів[8, 10].

Для VPN-з'єднань також існують апаратні та програмні рішення. Апаратні VPN-шлюзи, такі як продукти Cisco ASA (Adaptive Security Appliance) або Fortinet, забезпечують швидке і безпечне шифрування даних через публічні мережі. Вони пропонують високу пропускну здатність і можуть працювати з великими об'ємами трафіку. Програмні рішення для VPN, такі як OpenVPN або WireGuard, є більш доступними, але залежать від потужності обчислювальної системи[11, 15].

У супутникових захищених лініях передачі даних шифрування зазвичай забезпечується апаратними криптографічними модулями, оскільки високі вимоги до безпеки і продуктивності роблять апаратні рішення найбільш придатними. Пристрої, такі як модулі шифрування на базі HSM (Hardware Security Module), дозволяють забезпечувати захищене передавання даних навіть у складних умовах супутникового зв'язку. Компанії, що займаються супутниковим зв'язком, як-от SES або Inmarsat, інтегрують криптографічні рішення безпосередньо у свої інфраструктури[12, 14].

У мобільних захищених мережах, таких як LTE і 5G, для забезпечення захищеності використовуються програмно-апаратні рішення. Високий рівень безпеки досягається завдяки поєднанню апаратних криптографічних модулів на рівні базових станцій та програмних протоколів шифрування, таких як EPS-AKA для LTE або 5G-AKA для 5G. Це дозволяє ефективно керувати шифруванням на рівні передачі даних і з'єднання абонентів, забезпечуючи одночасно високу пропускну здатність і захищеність від атак[13].

Таким чином, у різних закритих лініях передачі даних вибір апаратного, програмного або програмно-апаратного забезпечення для шифрування залежить від балансу між необхідною продуктивністю, безпекою та вартістю. Апаратні рішення є більш продуктивними та захищеними, але дорогими. Програмні рішення є доступнішими, але менш стійкими до фізичних атак і можуть вимагати значних обчислювальних ресурсів. Програмно-апаратні рішення пропонують компроміс між гнучкістю і продуктивністю, що робить їх ідеальними для середовищ з підвищеними вимогами до безпеки [3, 6-15].

2.2 Вплив атак на захищеність ліній зв'язку та способи їх запобігання

У сучасних закритих каналах передачі даних забезпечення їхньої стійкості до різних видів атак стає ключовим завданням для підтримки безпеки інформаційних систем. Такі канали, як фізичні захищені лінії передачі, лінії з шифруванням даних, VPN, супутникові та мобільні захищені мережі, часто використовуються для обміну чутливими даними, що робить їх привабливими цілями для зловмисників. Атаки можуть бути різноманітними: від простого перехоплення інформації до складних сценаріїв модифікації даних або порушення їхньої конфіденційності. Нападники намагаються отримати несанкціонований доступ до переданих даних або навіть змінити їх, що може призвести до значних збитків і порушення роботи важливих систем.

Кожен із цих типів атак має свої особливості та специфіку, що вимагає застосування відповідних методів захисту. Дослідження природи цих загроз дозволяє краще розуміти, які саме вразливості можуть бути використані

зловмисниками у конкретному типі лінії передачі. На основі цього можна визначити найбільш ефективні заходи для забезпечення захищеності — від впровадження криптографічних протоколів і шифрування даних до використання систем автентифікації та методів контролю доступу. Вивчення взаємодії між типами атак і методами захисту є важливим етапом для розробки стійких і надійних рішень у сфері кібербезпеки.

Так же слід згадати про найосновніші проблеми, які виникають при використання закритих ліній передачі даних для захисту передаваємої інформації. Це проблемами сумісності, витрат і безпеки. Інтеграція різних систем і стандартів часто ускладнює забезпечення єдиної політики безпеки, особливо в мультивендорних середовищах. Високі витрати на впровадження, підтримку та модернізацію таких каналів вимагають значних інвестицій. Крім того, ризик компрометації залишається, навіть при застосуванні сучасних методів шифрування, що потребує постійного вдосконалення засобів захисту для протидії новим загрозам.

2.2.1 Типи атак: перехоплення даних, модифікація повідомлень, атаки на конфіденційність

Атаки на закриті лінії передачі даних є однією з основних загроз у сфері інформаційної безпеки, і їх класифікація дозволяє краще розуміти, як зловмисники намагаються скомпрометувати конфіденційність, цілісність і доступність інформації. Розглянемо три основні типи атак: перехоплення даних, модифікація повідомлень та атаки на конфіденційність.

Перехоплення даних є однією з найпоширеніших атак на лінії зв’язку, під час якої зловмисник отримує доступ до переданих даних без їхнього модифікування. До підвидів перехоплення належать атаки типу "людина посередині" (MITM), прослуховування (eavesdropping), а також пасивний моніторинг трафіку. Схеми даних атак можна побачити на рис. 2.2-2.4. Зазвичай такі атаки реалізуються за допомогою вразливостей у фізичному середовищі передачі або слабких методів шифрування. Наприклад, у бездротових мережах зловмисники можуть

використовувати спеціальне обладнання для перехоплення радіосигналів, або ж можуть підключатися до нешифрованих комунікаційних каналів у випадку неправильного налаштування безпеки[1-5].

Рисунок 2.2 — Атаки MITM

Рисунок 2.3 — Прослуховування (eavesdropping)

Рисунок 2.4 — Пасивний моніторинг трафіку

Модифікація повідомлень передбачає зміну даних під час їх передачі між відправником і отримувачем. Це може включати вставку нових даних, видалення

частини інформації або її коригування. Атаки типу модифікації також можуть бути частиною складніших атак MITM, де зловмисник не лише перехоплює, а й змінює інформацію. Підвиди таких атак включають фальсифікацію повідомлень, атаки на цілісність даних, а також атаки на контрольні суми. Ці атаки часто реалізуються шляхом використання недостатньо захищених протоколів або застарілих механізмів верифікації даних.

Атаки на конфіденційність спрямовані на несанкціонований доступ до чутливої інформації. Основна їхня мета — розкрити захищену інформацію або навіть анонімність користувачів. Це можуть бути як атаки на алгоритми шифрування, так і розкриття метаданих про користувачів. Підвиди цих атак включають аналіз трафіку, атаки на слабкі ключі шифрування та атаки на протоколи анонімності. Атаки на конфіденційність часто використовуються для отримання доступу до інформації, що передається через захищені канали, з метою подальшого використання її в шкідливих цілях.

Перехоплення даних та атаки на конфіденційність, попри власну схожість мають різну мету і механізми. Перехоплення даних спрямоване на отримання доступу до інформації під час її передачі між двома сторонами без їх відома. Найчастіше такий тип атаки реалізується через фізичні аспекти середовища і не завжди націлений на захищену інформацію. В даному випадку зловмисник не обов'язково націлений на те, щоб самому отримати певну інформацію, тобто йому не обов'язково цікавить зміст інформації, метою є її отримання. Натомість атаки на конфіденційність спрямовані на розкриття захищеної або прихованої інформації. Атаки на кофіденційність з самого початку мають на меті отримання доступу до конфіденційної/захищеної інормації з метою пізнішого її використання на власну користь[1-5, 24-26].

Фізичні захищені лінії передачі даних забезпечують високий рівень безпеки за рахунок захисту на фізичному рівні, проте залишаються вразливими до атак перехоплення у випадку доступу до кабельної інфраструктури. Наприклад, зловмисник може встановити фізичні пристрої перехоплення, такі як "крани" або "промислові шпигунські інструменти", для збору даних з

оптоволоконних або мідних ліній. Також можуть використовуватися атаки типу прослуховування, якщо фізичний захист був недостатнім.

Лінії з шифруванням даних вразливі до атак на ключі шифрування, а також до модифікації даних у випадках використання застарілих або слабких алгоритмів шифрування. Наприклад, атаки на слабкі ключі або підбір ключів (brute force) можуть призводити до розшифрування даних. Перехоплення також може бути ефективним у разі відсутності належної автентифікації сторін, що обмінюються інформацією.

VPN часто стають цілями атак MITM, де зловмисник може перехопити зашифрований трафік і спробувати розшифрувати його. Крім того, атаки на конфіденційність можуть бути реалізовані шляхом аналізу метаданих або ідентифікації кінцевих точок VPN. Для модифікації повідомлень зловмисники можуть намагатися втрутитися в трафік між клієнтськими пристроями та VPN-сервером, змінюючи або фальсифікуючи дані.

Супутникові захищені лінії передачі часто вразливі до атак на перехоплення сигналу, особливо в випадках недостатнього шифрування переданих даних. Оскільки супутникові сигнали поширюються на великі відстані, зловмисники можуть використовувати спеціальне обладнання для перехоплення супутникового зв'язку, що створює ризик для конфіденційності інформації. Атаки на модифікацію супутникових сигналів є складнішими, але можуть реалізовуватися шляхом спотворення або блокування сигналу.

Мобільні захищені мережі (LTE/5G) є об'єктами складних атак на перехоплення і модифікацію, оскільки ці мережі використовують широкий спектр протоколів захисту. Проте атаки на конфіденційність все ще можливі через аналіз трафіку або уразливості у старіших версіях стандартів шифрування, таких як 4G/LTE. Наприклад, атаки на системи аутентифікації користувачів можуть призвести до компрометації конфіденційної інформації.

Таким чином, кожен тип закритої лінії передачі даних має свої вразливості до певних типів атак, і ефективність атак залежить від того, як захищена система і які саме методи захисту застосовуються[10-13, 24-26].

2.2.2 Методи захисту від атак: шифрування, VPN, методи автентифікації та авторизації

У попередніх розділах вже було детально розглянуто метод шифрування як один із основних способів захисту даних, а також були описані різні криптографічні протоколи, що забезпечують надійність цього процесу. Шифрування дозволяє забезпечити конфіденційність і цілісність інформації, перетворюючи її в незрозумілий для зловмисників вигляд. Крім того, у роботі вже згадувався VPN — віртуальна приватна мережа, яка не тільки виконує роль окремого закритого каналу передачі даних, але й використовує шифрування для захисту трафіку. Це особливо важливо при передачі даних через публічні мережі, такі як Інтернет, де забезпечується приватність і захищеність інформації від перехоплення або несанкціонованого доступу.

Методи автентифікації, аутентифікації та авторизації є складовими частинами комплексної системи захисту даних, що забезпечують різні рівні перевірки користувачів і контроль доступу до системи або ресурсів. Ці процеси не тільки знижують ризик несанкціонованого доступу, але й допомагають мінімізувати наслідки потенційних атак.

Автентифікація є першим кроком у забезпеченні безпеки. Вона відповідає за перевірку особи користувача або пристрою, підтверджуючи, що цей суб'єкт є тим, за кого себе видає. Найбільш простим і розповсюдженим методом автентифікації є введення логіна і пароля. Однак цей спосіб має серйозні вразливості: паролі можуть бути викрадені або зламані. Для підвищення безпеки використовуються більш складні методи автентифікації, наприклад, одноразові паролі, що надсилаються на мобільний телефон, або біометричні методи, такі як відбитки пальців, сканування райдужки ока або розпізнавання обличчя. В апаратно-програмних рішеннях часто застосовуються токени або смарт-карти, які зберігають унікальні ключі доступу, забезпечуючи додатковий рівень захисту.

Автентифікація є критично важливою для всіх закритих каналів передачі даних. У VPN автентифікація використовується для встановлення захищеного з'єднання між користувачем і віддаленим сервером, де аутентичність обох сторін підтверджується перед передачею будь-яких даних. У мобільних захищених мережах (LTE/5G) автентифікація також є ключовим механізмом, оскільки мобільні оператори повинні гарантувати, що кожен пристрій, підключений до мережі, дійсно належить легітимному користувачеві.

Авторизація — це процес, який визначає, які дії дозволені користувачеві після успішної аутентифікації. Іншими словами, авторизація вирішує, які ресурси доступні користувачу. Наприклад, після того як користувач пройшов автентифікацію в мережі, авторизація визначить, чи може він переглядати певні файли, редагувати їх або просто читати. У сучасних системах авторизація часто ґрунтується на ролях (RBAC англ. Role-Based Access Control), коли кожному користувачеві надається відповідний рівень доступу на основі його ролі в організації. Наприклад, адміністратору може бути дозволено змінювати конфігурації системи, тоді як звичайному співробітнику — лише переглядати певні дані. Для кращого розуміння даної системи є рис. 2.5.

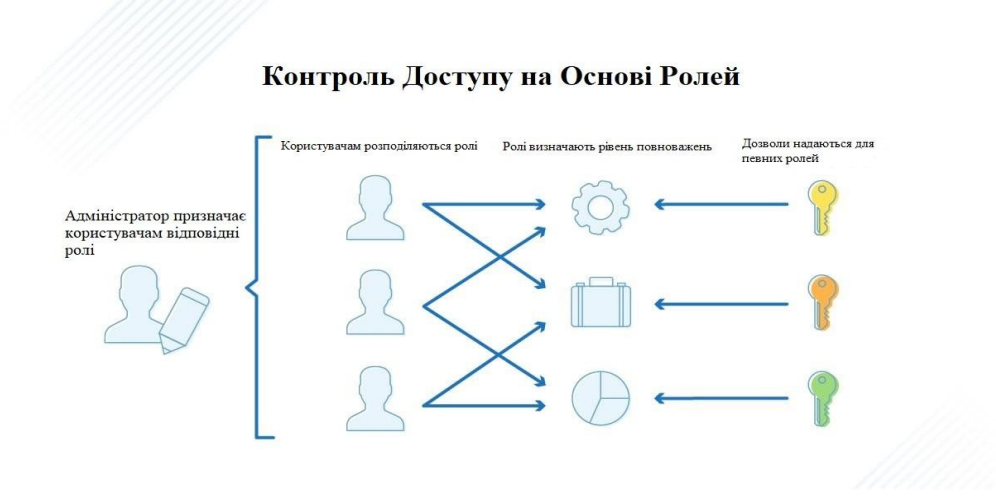


Рисунок 2.5 — Контроль доступу на основі ролей

У VPN і лініях з шифруванням даних авторизація грає критичну роль, оскільки необхідно контролювати, хто має доступ до чутливих файлів або систем, особливо при віддаленому доступі. У супутникових і мобільних мережах авторизація використовується для визначення, які ресурси доступні

користувачам на основі їхнього місцезнаходження або типу підключення. Це важливо для забезпечення того, щоб лише уповноважені користувачі могли отримати доступ до стратегічних або конфіденційних даних [2, 10-13, 16-21].

2.2.3 Використання брандмауерів, системи контролю доступу, систем виявлення та запобігання вторгнень (IDS(Intrusion Detection System)/IPS(Intrusion Prevention System))

Брандмауери (Firewall) є основним інструментом для захисту мереж від несанкціонованого доступу. Вони фільтрують мережевий трафік на основі попередньо встановлених правил, що дозволяє блокувати небажані підключення або атаки. Це рішення використовується в усіх типах закритих ліній передачі даних: фізичних захищених лініях, лініях з шифруванням, VPN, супутникових та мобільних захищених мережах. У фізичних лініях брандмауери контролюють доступ до критичних точок, у VPN та шифрованих лініях – захищають трафік на вході й виході з каналів, у супутникових мережах – захищають наземні станції, а в мобільних мережах LTE і 5G – базові станції й пристрої.

Переваги брандмауерів включають швидку фільтрацію трафіку та гнучке налаштування політик. Недоліком є відсутність глибокого аналізу трафіку або захисту від складних атак, наприклад, всередині зашифрованих каналів. Прикладом ефективного рішення є Cisco ASA Firewall для фізичних, рис. 2.6, і VPN-мереж, який забезпечує як апаратну, так і програмну безпеку.

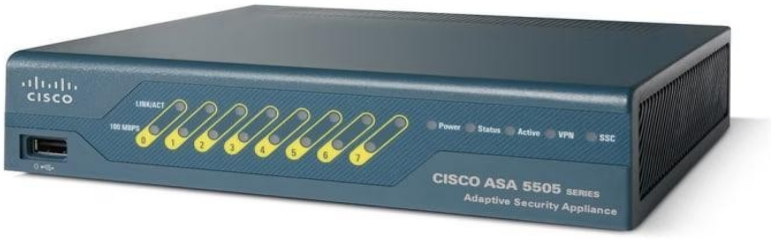


Рисунок 2.6 — Cisco ASA 5500-X Series Firewalls

Системи контролю доступу (Access Control Systems, ACS) використовуються для забезпечення того, що лише авторизовані користувачі можуть отримати доступ до критичних ресурсів у закритих лініях передачі

даних. Вони застосовуються в шифрованих лініях, VPN та мобільних мережах для захисту конфіденційної інформації, у фізичних лініях – для контролю доступу до серверів і вузлів мережі, а в супутникових лініях – для захисту наземних станцій. У VPN і мобільних мережах ACS забезпечують аутентифікацію користувачів, запобігаючи несанкціонованому доступу. Наприклад, система Microsoft Active Directory дозволяє централізовано керувати політиками доступу в корпоративних VPN і мобільних мережах.

Перевагами ACS є їхня гнучкість і можливість налаштування різнорівневого доступу, що дозволяє ефективно керувати правами користувачів. Однак, у разі слабкої конфігурації або ненадійної автентифікації (наприклад, без багатофакторної автентифікації), існує ризик злому системи, що може призвести до отримання несанкціонованого доступу.

Системи виявлення та запобігання вторгнень (IDS/IPS) моніторять мережеву активність і виявляють аномалії, що можуть вказувати на спробу вторгнення. IDS (система виявлення) лише сповіщає про підозрілу активність, а IPS (система запобігання) може автоматично блокувати шкідливі дії. IDS/IPS системи застосовуються в усіх типах закритих ліній: у фізичних – для захисту ключових вузлів, у VPN і шифрованих лініях – для аналізу трафіку в зашифрованих каналах, у супутникових – для захисту наземних станцій від DDoS(Distributed Denial of Service)-атак, у мобільних мережах – для запобігання атакам на базові станції та пристрої.

IDS/IPS забезпечують швидке виявлення та реагування на загрози, проте можливі помилкові спрацювання, що можуть блокувати легітимний трафік. Прикладом такого рішення є Snort (програмний IDS), який використовується для виявлення вторгнень у VPN або зашифрованих каналах, або Palo Alto Networks (апаратне IPS) для забезпечення проактивного захисту у фізичних та мобільних мережах[2, 9-15, 19-20].

2.2.4 Проблеми, з якими стикаються організації при використанні закритих ліній

Закриті лінії передачі даних відіграють ключову роль у забезпеченні безпеки інформації в організаціях, проте їх використання супроводжується певними проблемами. Однією з головних є ризик перехоплення чи зміни даних під час передачі, навіть у захищених лініях. Це вимагає додаткових методів шифрування і моніторингу. Організаціям необхідно постійно інвестувати в безпеку, щоб захистити дані від зовнішніх загроз і атак, що може стати складним завданням через постійно еволюціонуючі кіберзагрози.

Іншою проблемою є високі витрати на впровадження та підтримку закритих ліній. Потрібне спеціальне обладнання, програмне забезпечення та кваліфікований персонал. Постійне оновлення технологій для підтримки високого рівня безпеки ще більше підвищує фінансові витрати.

Крім того, сумісність і масштабованість є значним викликом. Закриті лінії часто важко інтегрувати з різними системами, особливо в мультивендорних середовищах, що ускладнює комунікацію між філіями або підрозділами. Масштабування таких ліній може бути технічно складним і дорогим, обмежуючи розширення інфраструктури організації[2].

1. Фізичні захищені лінії передачі мають власні переваги, але стикаються з низкою викликів[2, 9]:

Забезпечення конфіденційності: Оптоволокно забезпечує фізичний захист від втручання, але можливі ризики через фізичний доступ до кабелів, тому потрібні додаткові шифрувальні методи.

Цілісність та захист від перехоплення: Оптоволоконні лінії стійкі до електромагнітних перешкод і втручання в них легко виявити, проте фізичний доступ залишається загрозою.

Витрати: Висока вартість прокладання, обслуговування та моніторингу, особливо в складних географічних умовах, є суттєвою проблемою.

Сумісність і масштабованість: Труднощі інтеграції з різними стандартами й протоколами та фінансово складне масштабування обмежують можливості розширення інфраструктури.

2. Лінії з шифруванням даних забезпечують високий рівень захисту, але їх використання пов'язане з власними певними викликами[3, 10, 21]:

Забезпечення конфіденційності: Ці лінії шифрують всі передані дані, роблячи їх недоступними для сторонніх осіб. Однак проблеми можуть виникати з вибором алгоритмів шифрування та їхньою ефективністю проти нових загроз. Старі алгоритми і застарілі версії нових мають відомі вразливості, які легко використати.

Цілісність та захист від перехоплення: Криптографічні протоколи гарантують цілісність даних, але помилки в налаштуваннях або використання старих протоколів створюють ризики.

Витрати: Вимагають значних витрат на ліцензії, обладнання та регулярні оновлення для протидії новим загрозам.

Сумісність і масштабованість: Інтеграція із застарілими системами є складною та вимагає додаткових рішень, тоді як масштабування потребує потужного обладнання для обробки великих обсягів даних.

3. VPN надає високий рівень захисту, але має власні проблеми з налаштуванням роботи з'єднань[11, 15, 19]:

Забезпечення конфіденційності: Забезпечується створенням захищеного каналу та багатофакторною автентифікацією. Проблеми можуть виникати через неправильні конфігурації налаштувань або використання застарілих протоколів.

Цілісність та захист від перехоплення: Аутентифікація пакетів і криптографічні хеші, такі як HMAC, гарантують цілісність даних, а шифрування тунелю робить перехоплення марним без ключів.

Витрати: Витрати на VPN включають налаштування серверів, придбання програмного забезпечення (наприклад, OpenVPN, Cisco AnyConnect) і підтримку інфраструктури, зокрема хостинг серверів. Додаткові витрати включають автентифікацію користувачів, захист серверів і стабільність з'єднання, а також інвестиції в апаратні VPN-шлюзи для шифрованого трафіку.

Сумісність і масштабованість: VPN, як правило, добре інтегрується в різні мережеві середовища, але проблеми сумісності виникають, коли різні

організації використовують різні протоколи VPN (наприклад, OpenVPN, L2TP/IPsec, PPTP). Під час масштабування VPN для великої кількості користувачів виникають проблеми з продуктивністю, якщо існуюче обладнання не розраховане на високі навантаження або підтримку великих обсягів шифрованого трафіку.

4. Супутникові захищені лінії мають великі перспективи як закритий канал передачі даних, але мають складнощі з витратами, сумісністю та масштабованістю[12]:

Забезпечення конфіденційності: Під час передачі даних через супутники дані можуть бути вразливими до перехоплення через відкритий характер супутникового зв’язку. Хоч шифрування значно знижує даний ризик, але не являється ідеальним рішенням.

Цілісність: Для забезпечення цілісності даних у супутникових каналах використовуються механізми перевірки CRC (Cyclic Redundancy Check) або інші хеш-функції, що виявляють помилки та зміни під час передачі даних.

Витрати: Супутникові захищені лінії потребують значних початкових інвестицій у антени, наземні станції та послуги провайдерів. Постійні витрати включають оренду супутникового каналу, а також підтримку і моніторинг системи. Найбільші витрати пов'язані з використанням високошвидкісних каналів, що залежать від обсягу даних та віддаленості регіону. Супутникові лінії для військових значно дорожчі через витрати на розробку, запуск та обслуговування супутників. Додаткові витрати включають захищені наземні станції, мобільні термінали та системи шифрування. Витрати збільшуються при заміні супутників або підтримці резервних систем для безперебійного зв’язку.

Сумісність і масштабованість: Якщо кількість користувачів або обсяг даних, що передаються значно зростає відбувається зниження якості зв'язку або відмова у обслуговуванні. Сумісність супутникових ліній з наземними мережами проблематична через різницю у швидкості передачі даних і високі затримки, характерні для супутникового зв'язку.

5. Мобільні захищені мережі перспективні завдяки зручності використання, але забезпечення високого рівня безпеки є складним завданням[13, 23]:

Забезпечення конфіденційності: Сучасні мобільні мережі використовують більш удосконалені алгоритми шифрування в порівнянні з попередніми поколіннями мобільного зв’язку.

Цілісність та захист від перехоплення: Інтегровані механізми перевірки забезпечують цілісність даних, а шифрування (AES-256) захищає трафік між пристроями та базовими станціями.

Витрати: Включають доступ до операторів, налаштування приватних каналів, придбання обладнання для шифрування та підтримку політик безпеки. Додаткові витрати виникають при оновленні захисту, розширенні мережі та підвищенні пропускної здатності.

Сумісність і масштабованість: Мобільні захищені мережі (LTE/5G) стикаються з проблемами сумісності через різні стандарти зв'язку і нерівномірний розвиток 5G-інфраструктури в різних регіонах. Масштабування мереж ускладнюється збільшенням кількості підключень, що знижує швидкість передачі. Крім того, різні оператори можуть використовувати різні протоколи шифрування, що ускладнює інтеграцію з корпоративними мережами.

Закриті лінії передачі даних використовують різні підходи для забезпечення конфіденційності, цілісності та захисту від перехоплення даних. Фізичні лінії забезпечують захист завдяки контролю фізичного доступу, але залишаються вразливими при прямому втручанні. Лінії з шифруванням, VPN і супутникові канали покладаються на криптографічні протоколи для захисту, хоча вони можуть потребувати складної інтеграції та налаштувань у різних середовищах. Мобільні мережі LTE/5G використовують сучасні технології шифрування, проте стикаються з проблемами сумісності через різні стандарти та географічні обмеження.

Кожен тип закритих ліній має свої виклики з точки зору сумісності, масштабованості та витрат на впровадження. Фізичні лінії потребують великих

інвестицій в інфраструктуру, а супутникові і мобільні мережі — в обладнання та підтримку. Додаткові витрати виникають при масштабуванні або модернізації мереж. Проблеми з інтеграцією різних технологій і протоколів, а також нерівномірний розвиток інфраструктури в різних регіонах, часто ускладнюють налаштування єдиних стандартів безпеки і підвищують вимоги до інвестицій в інфраструктуру [10-13, 20-23].

2.3 Огляд сучасних рішень для захисту закритих ліній передачі

Закриті лінії передачі даних є фундаментом для безпечного обміну конфіденційною інформацією між користувачами, мережами та системами. В умовах зростання кіберзагроз сучасні технології захисту цих ліній стали критично важливими для великих компаній, урядових установ та військових. Ці рішення охоплюють широкий спектр новітніх підходів, зокрема шифрування, багаторівневий контроль доступу та їх інтеграцію в програмно-апаратних засобів. Шифрування є основним методом захисту, що гарантує недоступність перехоплених даних для зловмисників. Багаторівневий контроль доступу додає додатковий рівень безпеки, надаючи доступ лише авторизованим користувачам. Водночас використання сучасних програмно-апаратних рішень, таких як брандмауери, криптографічні модулі та захищені комунікаційні пристрої, підвищує захист як на фізичному, так і на мережевому рівнях.

Однак сучасні рішення не позбавлені проблем. Одним з основних прикладів таких проблем є зниження пропускної здатності через використання складних алгоритмів шифрування. Також складність управління шифрувальними ключами та дотримання високих стандартів безпеки може бути викликом для великих мережевих систем.

Є великі перспективи розвитку технологій захищених ліній передачі даних і вони пов’язані з інтеграцією квантового шифрування та штучного інтелекту для автоматизації безпеки. Такі технології можуть підвищити рівень захисту і зменшити вплив людського фактора.

Технології на кшталт квантового шифрування та використання штучного інтелекту для аналізу та прогнозування загроз вже демонструють свій потенціал. Вони можуть стати наступним кроком у забезпеченні безпеки закритих ліній передачі даних, забезпечуючи ще більш надійний захист від сучасних кіберзагроз[24-26].

2.3.1 Сучасні програмні, апаратні та програмно-апаратні засоби захисту/рішення в закритих ліній передачі

Використання новітніх технологій є ключовим фактором у забезпеченні безпеки закритих каналів передачі даних. Для кожного типу таких каналів (мобільні захищені мережі, супутникові лінії, VPN, фізичні та шифровані лінії) застосовуються сучасні рішення, що включають передові методи шифрування, багаторівневий контроль доступу та інші новітні механізми захисту, оптимізовані під конкретні потреби мережі.

Сучасні програмні, апаратні та програмно-апаратні рішення відіграють критичну роль у захисті цих каналів. Вони поєднують інноваційне апаратне обладнання з новітнім програмним забезпеченням, яке забезпечує надійний криптографічний захист, автентифікацію користувачів, контроль доступу та моніторинг мережевої активності. Це поєднання новітніх засобів гарантує високу стійкість до кіберзагроз і забезпечує безпечну передачу даних у сучасних умовах.

Далі розглянемо поєднання сучасних програмних, апаратних і програмно-апаратних рішень в закритих лініях передачі даних[24-26]:

1. Фізичні захищені лінії передачі: Фізично захищені лінії передачі, такі як оптоволоконні кабелі, забезпечують високий рівень безпеки від фізичних атак. Основні методи захисту включають використання сучасних алгоритмів шифрування (AES-256, IPsec) або квантового шифрування (QKD) гарантує конфіденційність даних навіть у разі фізичного втручання. Програмно-апаратні рішення, такі як комутатори та маршрутизатори з інтегрованими криптографічними модулями, доповнюють цю безпеку, забезпечують швидке та

надійне шифрування трафіку на фізичному рівні, що робить фізичні лінії стійкими до перехоплення та фізичного втручання.

2. Лінії з шифруванням даних: Лінії з шифруванням даних використовують алгоритми, такі як AES-256 і IPsec, для забезпечення надійного шифрування трафіку на рівні мережевого протоколу. Це гарантує безпечну передачу даних між організаціями або державними установами. Програмні рішення, такі як AES-GCM, забезпечують не лише шифрування, але й автентифікацію даних, підвищуючи захист від атак MITM. Апаратні криптографічні модулі, як-от Intel QAT, прискорюють операції шифрування, що робить лінії з шифруванням даних ефективними та безпечними для великих обсягів інформації.

3. VPN: VPN забезпечують захищену передачу даних через незахищені мережі, такі як Інтернет, завдяки протоколам шифрування, як-от AES-256 і ChaCha20. Основними протоколами є OpenVPN і WireGuard, що поєднують шифрування з автентифікацією для захисту даних від перехоплення. Програмно-апаратні засоби, такі як маршрутизатори Cisco ASA або Fortinet FortiGate, прискорюють обробку трафіку, використовуючи апаратні криптографічні модулі. Це дозволяє підвищити продуктивність і гарантує безпечну передачу даних через VPN навіть для великих організацій і віддалених офісів.

4. Супутникові захищені лінії: Супутникові захищені лінії використовуються для передачі даних на великі відстані, зокрема у віддалених регіонах. Для захисту використовуються шифрувальні алгоритми, такі як AES-256 і TLS/SSL, що гарантують безпеку трафіку. Програмно-апаратні рішення, як-от системи O3b mPOWER(система супутників компанії SES), поєднують шифрування з апаратними модулями, такими як Thales HSM, для забезпечення безпеки на фізичному рівні. Технології на кшталт Beam Hopping дозволяють динамічно змінювати напрям сигналу, зменшуючи ризик перехоплення даних, що підвищує безпеку супутникового зв’язку.

5. Мобільні захищені мережі (LTE/5G): У мобільних мережах LTE/5G захист забезпечується за допомогою шифрування даних на рівні

радіоінтерфейсу, таких як AES-256 і протокол EPS Encryption. Важливу роль відіграють багаторівневі протоколи автентифікації, як-от EAP-AKA, що забезпечують контроль доступу. Програмно-апаратні засоби, наприклад маршрутизатори Cisco з інтегрованими криптографічними модулями, забезпечують швидке шифрування трафіку. У мережах 5G використовуються інноваційні технології, такі як квантове розподілення ключів (QKD), що гарантують додатковий захист від перехоплення, підвищуючи загальний рівень безпеки мереж.

Сучасні закриті лінії передачі даних забезпечуються комплексними рішеннями, що поєднують новітні програмні, апаратні та програмно-апаратні засоби захисту. Використання передових технологій шифрування, таких як AES-256 та квантова криптографія, гарантує надійний захист даних, навіть у разі їх перехоплення. Багаторівневі протоколи автентифікації та контроль доступу додають додаткові шари безпеки, забезпечуючи захист від несанкціонованого доступу.

Програмно-апаратні рішення, включаючи криптографічні модулі, захищені комунікаційні пристрої та інноваційні протоколи VPN, забезпечують стійкість до загроз на фізичному та мережевому рівнях. Ці технології гарантують надійний захист у різних умовах — від мобільних мереж до супутникових і фізичних ліній передачі, дозволяючи організаціям безпечно передавати конфіденційну інформацію та залишатися стійкими до сучасних кіберзагроз.

2.3.2 Проблеми та перспективи розвитку технологій закритих ліній передачі даних

Технології захищених ліній передачі даних постійно еволюціонують, оскільки нові загрози та вимоги до безпеки виникають з розвитком технологій. Проблеми з безпекою стають дедалі складнішими, але водночас з'являються нові перспективні рішення, що можуть значно підвищити захист закритих каналів передачі. Далі наведені деякі найочевидніші проблеми і перспективи розвитку технологій закритих ліній передачі даних[25-27].

Проблеми:

1. Квантові обчислення і загроза шифруванню. Традиційні криптографічні алгоритми, як-от AES та RSA, можуть стати вразливими до квантових обчислень. Алгоритми квантового зламування здатні ефективно розв'язувати завдання факторизації та дискретного логарифму, на яких базується сучасна криптографія. Це робить майбутні квантові комп'ютери великою загрозою для безпеки даних.

2.1 Широкий масштаб атак. Зі зростанням числа підключених пристроїв і складністю мереж (особливо у 5G і IoT середовищах), закриті канали передачі даних стають дедалі вразливішими до атак типу MITM, DDoS, та інших кіберзагроз. Наприклад, у мобільних мережах, таких як 5G, зростає ризик атак на ключову інфраструктуру і компрометації критично важливих комунікацій.

2.2 Зростання складності атак. Сучасні кібератаки стають дедалі складнішими та багаторівневими. Ті ж самі атаки на рівні інфраструктури мереж включають складні сценарії компрометації мережевих пристроїв, маніпуляції з трафіком та впровадження шкідливого коду. Це вимагає від захищених каналів передачі даних вдосконалення систем виявлення загроз та миттєвого реагування на них.

3. Обмеження апаратних рішень. Хоча апаратні криптографічні модулі, як-от HSM, забезпечують високий рівень безпеки, вони також мають обмежену продуктивність і масштабованість. Захищені канали передачі даних потребують серйозних інвестицій в апаратні засоби захисту, програмне забезпечення та інфраструктуру. Наприклад, впровадження квантової криптографії або новітніх криптографічних модулів, як-от HSM, є дорогим, що стає бар'єром для багатьох організацій і державних установ.

4. Затримки та пропускна здатність. Використання апаратних рішень для шифрування часто впливає на пропускну здатність мереж і створює додаткові затримки. Використання шифрування та апаратних рішень для безпеки також призводить до збільшення затримок у передачі даних, особливо у супутникових і віддалених мережах. Це є важливою проблемою для супутникових мереж, де затримки вже великі через значні відстані, які сигнал долає до супутників і назад.

Масштабованість захищених каналів також обмежена технічними можливостями сучасних криптографічних пристроїв.

5. Інтеграція старих і нових технологій. Підтримка зворотної сумісності з більш старими протоколами шифрування та безпеки є викликом. Багато організацій використовують застарілі системи, які можуть бути вразливими до сучасних атак, що ускладнює перехід на нові, більш захищені технології.

Перспективи:

1. Квантова криптографія: Однією з головних перспектив є впровадження квантової криптографії. Технологія QKD дає змогу передавати шифрувальні ключі через квантові канали, що унеможливлює несанкціоноване перехоплення або підміну даних. Це є проривним рішенням у сфері захисту критично важливої інформації.

2. Автоматизація безпеки: Штучний інтелект (ШІ) та машинне навчання можуть бути використані для автоматизації процесів виявлення загроз та реагування на них у режимі реального часу. Це дозволить зменшити вплив людського фактора та значно підвищити ефективність захисту мереж.

3. Покращення пропускної здатності: Нові рішення в сфері шифрування, як-от оптимізовані криптографічні алгоритми та новітні процесори для шифрування, зменшують затримки та підвищують пропускну здатність мереж. Наприклад, апаратні модулі, такі як Nitrox V або Intel QAT, дають змогу швидше обробляти великий обсяг зашифрованого трафіку.

4. Розвиток хмарних і гібридних рішень: Інтеграція захищених каналів передачі даних з хмарними рішеннями дозволяє підвищити гнучкість та ефективність управління безпекою. Це особливо важливо для глобальних корпорацій, які використовують захищені канали для зв'язку між офісами в різних частинах світу.

2.4 Методи дослідження закритих ліній передачі даних

У цьому підрозділі розглядаються методи, які можуть бути використані для дослідження закритих ліній передачі даних, зокрема фізичних захищених

ліній, ліній з шифруванням даних, VPN, супутникових ліній передачі та мобільних захищених мереж. Існує багато підходів для оцінки надійності та безпеки таких каналів, однак ми зосередимося на основних методах, які найкраще відображають різні аспекти роботи закритих каналів передачі.

В даному підрозділі будуть описані п’ять ключових методів: порівняльний аналіз різних технологій закритих каналів, криптографічний аналіз захищеності каналів зв'язку, оцінка ефективності методів захисту від несанкціонованого доступу, моделювання ризиків, аналіз продуктивності. Ці методи дозволяють детально дослідити основні характеристики закритих каналів передачі даних, а також виявити їх переваги і недоліки у сфері забезпечення інформаційної безпеки.

Далі детальніше розглянемо, що представляють собою кожен з цих методів, та як вони застосовуються для дослідження закритих ліній передачі даних.

2.4.1 Порівняльний аналіз різних технологій закритих каналів

Порівняльний аналіз є важливим методом дослідження різних технологій закритих каналів передачі даних, що дозволяє оцінити ефективність і надійність кожної з них в умовах, які відрізняються за своїми вимогами до безпеки, продуктивності та надійності. Суть методу полягає в детальному вивченні основних технічних характеристик, можливостей і обмежень кожної технології, а також її здатності забезпечити захист даних в різних умовах використання. Цей метод дозволяє порівняти такі показники, як пропускна здатність, рівень безпеки, стійкість до зовнішніх загроз, швидкість передачі даних, затримки, рівень доступності та надійність. Раніше вже були наведені певні характеристики досліджуваних закритих ліній передачі даних, але в майбутньому параметри ліній будуть розглянуті більш детально.

Одним із ключових завдань порівняльного аналізу є визначення сильних і слабких сторін кожної технології, що дозволяє зробити обґрунтований вибір на користь тієї або іншої лінії передачі даних. Наприклад, у деяких ситуаціях можуть бути пріоритетними такі параметри, як висока пропускна здатність і низька затримка, тоді як в інших випадках на першому місці стоїть безпека і стійкість до атак. Порівняльний аналіз дозволяє отримати загальну картину щодо того, яка технологія краще підходить для тих чи інших потреб. Для закритих ліній передачі найважливішою характеристикою є безпека передачі даних, але через ситуаційність потреб визначення найкращого варіанту складне.

У дослідженні закритих ліній передачі даних цей метод є особливо важливим, оскільки кожна з технологій, що використовується для створення захищених каналів, має свої унікальні характеристики. Наприклад, фізичні захищені лінії передачі мають високий рівень фізичної безпеки, але можуть бути менш гнучкими в умовах швидких змін в інфраструктурі, тоді як VPN забезпечують мобільність і шифрування, але залежать від безпеки самого Інтернету[9-13].

Основними етапами порівняльного аналізу є[22-24]:

1. Визначення критеріїв порівняння, які включають технічні параметри, рівень безпеки та особливості експлуатації;

2. Збір інформації про кожну технологію, включаючи її архітектуру, способи шифрування та захисту даних, вимоги до обладнання;

3. Аналіз результатів і побудова порівняльної таблиці для візуалізації переваг і недоліків кожної технології;

4. Висновки про те, які технології найкраще підходять для конкретних сценаріїв використання або умов експлуатації.

Метод порівняльного аналізу застосовується до різних технологій закритих каналів передачі даних для того, щоб знайти найкраще рішення для певної інфраструктури, враховуючи потреби в безпеці, продуктивності та доступності. У подальшому ми детально розглянемо кожну з цих технологій у контексті порівняння їх переваг та недоліків [18].

2.4.2 Криптографічний аналіз захищеності каналів зв'язку

Криптографічний аналіз захищеності каналів зв'язку є методом дослідження, спрямованим на перевірку надійності криптографічних механізмів, які забезпечують конфіденційність, цілісність та автентичність даних під час їх передачі. Цей підхід полягає в детальному вивченні криптографічних протоколів і алгоритмів, які використовуються для захисту інформації, а також в аналізі стійкості системи до різних атак, таких як перехоплення, дешифрування та модифікація даних. Основна мета криптографічного аналізу — виявити потенційні вразливості, які можуть бути використані зловмисниками для порушення захисту системи, і запропонувати шляхи їх усунення.

Криптографічний аналіз включає в себе перевірку таких компонентів захищеності, як симетричне та асиметричне шифрування, протоколи для захищеної передачі ключів, цифрові підписи та методи автентифікації. Наприклад, використовуються різні алгоритми шифрування, такі як AES, RSA, ECC, які аналізуються на предмет їхньої стійкості до атак (сила ключа, ймовірність зламування). У рамках криптоаналізу також оцінюються специфічні методи атак на криптографічні системи, включаючи атаки грубої сили, диференційний криптоаналіз, криптоаналіз за сторонніми каналами та атаки MITM.

Одним з основних аспектів криптографічного аналізу є оцінка надійності системи автентифікації, що забезпечує ідентифікацію користувачів та захист від спроб несанкціонованого доступу до закритих каналів передачі. Метод перевіряє, чи можна використовувати прогалини в автентифікаційних процесах для компрометації системи, наприклад, шляхом відтворення сеансів зв'язку або підробки цифрових підписів. Окрім цього, криптографічний аналіз враховує фактори, пов'язані з управлінням ключами: їх зберігання, передача та використання в межах різних типів мереж.

Цей метод є важливим інструментом для оцінки стійкості сучасних систем захисту даних, оскільки дає можливість не лише виявити слабкі місця в існуючих

криптографічних алгоритмах, але й сприяє розробці нових, більш надійних методів захисту. Криптографічний аналіз також дозволяє оптимізувати вибір криптографічних протоколів залежно від специфіки мережі або середовища, в якому функціонують закриті лінії передачі, підвищуючи таким чином загальний рівень безпеки [3, 8, 26].

2.4.3 Оцінка ефективності методів захисту від несанкціонованого доступу

Оцінка ефективності методів захисту від несанкціонованого доступу є важливим етапом дослідження закритих ліній передачі даних. Вона спрямована на перевірку здатності захисних механізмів, таких як брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS) і системи контролю доступу, виконувати свої функції. Цей процес включає в себе тестування їхньої реакції на потенційні загрози, спроби несанкціонованого проникнення та перевірку можливостей блокування або фільтрації шкідливого трафіку. У ході цього дослідження також перевіряється, наскільки точно системи можуть розпізнавати легітимний трафік, не створюючи перешкод для звичайної роботи мережі.

Основна мета оцінки ефективності полягає в тому, щоб переконатися, що використовувані захисні механізми забезпечують необхідний рівень безпеки, захищаючи канали передачі від різних типів атак, зокрема від атак типу "відмова в обслуговуванні" (DoS), спроб обману систем автентифікації, перехоплення або модифікації даних. Важливим аспектом є також перевірка на можливість витоку інформації через так звані "зворотні двері", коли зловмисники можуть обходити встановлені правила безпеки через приховані уразливості.

Метод оцінки ефективності передбачає проведення серії тестів і симуляцій атак для того, щоб побачити, як захисні механізми реагують на них у реальних умовах. Цей процес може включати аналіз журналів подій, тестування здатності систем до самовідновлення після атак, а також вимірювання часу реакції на загрози. Крім цього, проводиться оптимізація налаштувань безпеки на основі отриманих результатів, щоб підвищити загальну продуктивність системи безпеки.

Додатковим важливим аспектом оцінки є врахування специфічних вимог до захисту кожного типу мережі. Наприклад, захист фізичних ліній передачі більше фокусується на фізичному доступі до кабелів, тоді як для мобільних і супутникових мереж велике значення має захист від перехоплення сигналу або атак на автентифікаційні протоколи [16-19, 23-27].

2.4.4 Моделювання ризиків

Моделювання ризиків (англ. Risk Modeling) є важливим методом, який використовується для оцінки ймовірності виникнення загроз і потенційних наслідків їх реалізації у закритих лініях передачі даних. Цей підхід дозволяє на основі низки факторів, таких як характеристики мережі, рівень захисту, використовувані методи шифрування та автентифікації, оцінити рівень ризиків, з якими може стикнутися система під час експлуатації. Моделювання ризиків базується на створенні моделей ймовірностей різних загроз і аналізі їх впливу на мережу або систему в цілому.

Основною метою моделювання ризиків є ідентифікація найбільш вразливих місць у мережі та оцінка ймовірності успішного здійснення атаки. Це дозволяє пріоритизувати зусилля з покращення захисту саме в тих точках, де ризик найбільший. Крім того, моделювання ризиків дозволяє оцінити потенційні наслідки успішної атаки, що допомагає визначити найбільш ефективні методи захисту для зменшення або повного усунення ризиків.

Метод передбачає врахування різних видів загроз, таких як атаки типу DoS, спроби зламу шифрування, атаки на автентифікацію або несанкціонований доступ до конфіденційних даних. Крім того, він враховує внутрішні фактори, наприклад, надійність апаратних та програмних рішень, використаних для захисту закритих ліній передачі[3, 24].

Основними етапами моделювання ризиків є[6-7]:

1. Ідентифікація можливих загроз, які можуть виникнути в системі або мережі.

2. Оцінка ймовірності реалізації цих загроз на основі історичних даних, відомих атак або аналізу вразливостей мережевих компонентів.

3. Оцінка потенційних наслідків, що виникають у результаті успішного здійснення атаки або проникнення в систему.

4. Пріоритизація заходів безпеки на основі отриманих даних, що дозволяє зосередити ресурси на найбільш критичних аспектах захисту.

Моделювання ризиків є невід'ємною частиною стратегії забезпечення безпеки, оскільки воно дозволяє систематизовано оцінювати, де і яким чином захист слід посилити. Завдяки цьому методу можливо уникнути серйозних порушень в роботі закритих ліній передачі даних шляхом впровадження запобіжних заходів[18].

2.4.5 Аналіз продуктивності

Аналіз продуктивності (англ. Performance Analysis) є одним із ключових методів дослідження ефективності закритих ліній передачі даних, який дозволяє оцінити, наскільки обрана технологія захисту впливає на швидкість передачі інформації, рівень затримок та пропускну здатність мережі. Цей метод націлений на вивчення технічних характеристик системи у реальних або змодельованих умовах експлуатації для визначення її оптимальності та продуктивності в різних сценаріях використання. Основною метою аналізу продуктивності є забезпечення балансу між безпекою та ефективністю передачі даних.

Метод дозволяє проводити кількісне вимірювання таких показників, як затримка в передачі даних (англ. latency), що є критичним фактором для систем, які працюють у режимі реального часу, пропускна здатність мережі (англ. bandwidth), яка визначає, який обсяг даних можна передати за одиницю часу, а також швидкість передачі, що залежить від складності шифрування або додаткових процедур захисту даних. Аналіз продуктивності дозволяє виявити, наскільки вибрані методи шифрування або засоби захисту впливають на загальну ефективність передачі даних, і чи виправдані обрані рішення з точки зору забезпечення балансу між безпекою та швидкістю.

Аналіз продуктивності дозволяє визначити, як різні технології захисту впливають на продуктивність закритих ліній передачі даних, особливо в умовах високого навантаження або під час передачі великих обсягів інформації. Наприклад, деякі алгоритми шифрування можуть значно збільшувати затримки через свою обчислювальну складність, що може бути неприйнятним у критичних системах, таких як мобільні мережі або системи реального часу. Водночас, більш прості алгоритми можуть мати недостатню стійкість до атак, що знижує загальну безпеку системи[3].

Основними етапами аналізу продуктивності є[3, 18]:

1. Визначення ключових показників продуктивності, які будуть вимірюватися, таких як швидкість передачі, затримки, пропускна здатність тощо.

2. Вимірювання продуктивності системи в різних сценаріях роботи, наприклад, під час нормального навантаження або в умовах підвищених вимог до безпеки.

3. Аналіз впливу технологій захисту на продуктивність, зокрема, як різні методи шифрування впливають на швидкість передачі або затримки в мережі.

4. Порівняння результатів з іншими технологіями, що дозволяє виявити найбільш оптимальне рішення для забезпечення захисту без значних втрат продуктивності.

Цей метод дозволяє не лише оцінити ефективність функціонування існуючих технологій, але й використовувати результати для їх оптимізації. Аналіз продуктивності є важливим для тих систем, де критичним є забезпечення як високого рівня захисту, так і стабільної швидкості передачі даних, таких як VPN, мобільні та супутникові мережі, а також фізичні захищені лінії.

Метод аналізу продуктивності є важливим інструментом для вибору та налаштування технологій захисту закритих ліній передачі даних, оскільки він дозволяє враховувати вплив різних заходів безпеки на реальну продуктивність мережі[18].

2.5 Висновок до другого розділу

У другому розділі було розглянуто основні аспекти захисту закритих ліній передачі даних. Детально досліджено методи шифрування, зокрема симетричні та асиметричні алгоритми, а також криптографічні протоколи, що використовуються для забезпечення безпеки інформації. Було детально проаналізовано суть цих алгоритмів, зокрема теоретичні основи, на яких вони засновані, та їхні принципи роботи. Окрему увагу приділено ролі алгоритмів шифрування, таких як AES, RSA та ECC, у забезпеченні безпеки, а також криптографічним протоколам, таким як TLS/SSL та IPsec, які захищають передані дані. Було розглянуто не лише алгоритми та протоколи, але й те, як програмне і апаратне забезпечення застосовується для реалізації захисту. Зокрема, досліджено роль апаратних пристроїв, таких як брандмауери та системи контролю доступу, а також програмних рішень для шифрування та автентифікації, що забезпечують цілісність і конфіденційність інформації під час її передачі.

Розділ також охоплює детальний аналіз загроз, які можуть впливати на захищеність закритих ліній передачі даних. Зокрема, розглянуто різні типи атак, такі як перехоплення даних, що передбачає несанкціоноване отримання інформації під час її передачі; модифікація повідомлень, коли зловмисник змінює або підробляє передані дані; та атаки на конфіденційність, спрямовані на розкриття захищеної інформації або доступ до неї без дозволу. Для кожного типу атак були розглянуті відповідні методи захисту, такі як шифрування для забезпечення конфіденційності, VPN для захисту трафіку під час передачі через незахищені мережі, а також методи автентифікації, аутентифікації та авторизації, які запобігають доступу несанкціонованих користувачів до системи.

Було також проаналізовано проблеми, з якими стикаються організації при використанні закритих ліній передачі даних. Серед них – висока вартість впровадження та підтримки захищених каналів, складнощі з інтеграцією нових технологій у вже існуючу інфраструктуру, а також необхідність постійного оновлення систем захисту для відповідності сучасним стандартам кібербезпеки.

Ці проблеми вимагають значних ресурсів та зусиль для їх подолання, що може бути складним для організацій з обмеженими бюджетами або технічними можливостями.

У відповідь на ці виклики було розглянуто сучасні рішення для захисту закритих ліній передачі даних, які поєднують програмні, апаратні та програмно-апаратні засоби. До них відносяться новітні криптографічні алгоритми, системи багатофакторної автентифікації, а також інтегровані платформи захисту, які автоматизують процеси виявлення та запобігання кіберзагрозам. Зокрема, сучасні засоби шифрування та виявлення вторгнень можуть забезпечити високий рівень захисту навіть у складних мережевих умовах, а програмно-апаратні рішення, такі як HSM, підвищують рівень безпеки ключових даних.

У завершальній частині розділу було приділено увагу методам дослідження ефективності закритих ліній передачі даних. Серед них — порівняльний аналіз різних технологій закритих каналів, що дозволяє оцінити переваги і недоліки кожної технології у різних умовах експлуатації. Криптографічний аналіз досліджує стійкість шифрувальних протоколів до атак, а також вразливості, які можуть бути використані зловмисниками. Оцінка ефективності методів захисту від несанкціонованого доступу дозволяє визначити рівень захисту системи та виявити потенційні загрози. Моделювання ризиків, яке оцінює ймовірність виникнення загроз, їх наслідки та визначає вразливі місця мережі для покращення захисту. Аналіз продуктивності досліджує вплив захисних технологій на швидкість передачі даних, затримку та пропускну здатність для забезпечення балансу між безпекою і ефективністю. Кожен із цих методів вносить вагомий внесок у забезпечення надійності та безпеки при розробці і побудові закритих ліній передачі даних.

РОЗДІЛ 3 РОЗРОБЛЕНИЙ ЗАКРИТИЙ КАНАЛ ПЕРЕДАЧІ ДАНИХ

3.1 Опис ідеї закритого каналу передачі даних

Цей розділ присвячений розробці нового підходу до створення закритого каналу передачі даних, що базується на модифікації існуючих VPN-технологій. Основна концепція полягає у забезпеченні високого рівня захисту за рахунок поділу інформаційного потоку на кілька паралельних каналів з меншою пропускною здатністю. На відміну від традиційного VPN, який використовує один канал для передачі всіх даних, ця модель передбачає одночасну роботу

кількох каналів, що посилює безпеку й ускладнює спроби перехоплення даних[6, 18].

Перед відправкою дані поділяються на блоки, які шифруються за допомогою надійного алгоритму шифрування AES-256, що забезпечує захист від несанкціонованого доступу. Шифрування виконується за допомогою апаратних VPN-шлюзів, що допомагає знизити час обробки й навантаження на пристрій. Кожен блок після шифрування передається через один із паралельних каналів у випадковому порядку. Це означає, що послідовність блоків під час передачі не зберігається, а кожен блок може передаватися через різні канали, що додатково ускладнює перехоплення всієї інформації[3, 36].

Особливістю даного підходу є те, що кожен канал передає лише частину даних, тому зловмиснику необхідно контролювати всі канали одночасно для перехоплення всієї інформації. Таким чином, поєднання кількох захищених каналів і криптографічного захисту забезпечує додатковий рівень безпеки.

Під час встановлення з'єднання здійснюється автентифікація через криптографічне рукостискання, яке гарантує підтвердження обох сторін з'єднання. Після успішної автентифікації система домовляється про використання кількох каналів для передачі даних. На приймальній стороні блоки збираються за допомогою хешів, вбудованих у кожен блок даних. Ця технологія була заснована на основі блокчейну для забезпечення цілісність і автентичність отриманих даних, адже кожен блок містить хеш попереднього і наступного блоків.

Слід зазначити, що хоча блоки збираються в правильній послідовності за допомогою хешів, на них усе ще присутні порядкові мітки для перевірки втрат блоків даних під час передачі. Однак ці мітки не відповідають правильній послідовності збору.

У результаті, запропонований метод забезпечує високий рівень захисту інформації, зберігаючи її цілісність і захищаючи від несанкціонованого доступу на всіх етапах передачі[6, 18].

3.2 Будова каналу

Будова каналу передачі даних у запропонованій концепції побудована на основі стандартної архітектури VPN, але має низку розширень, що робить її більш захищеною та надійною. Основні компоненти нового закритого каналу передачі даних такі ж, як у базових п'яти елементів, які використовуються в стандартних закритих каналах передачі інформації. Канал побудовано на основі принципів VPN-технологій, що дозволяє ефективно інтегрувати елементи шифрування та контроль доступу, забезпечуючи захищену передачу даних через Інтернет. Внаслідок такої побудови він має деякі специфічні особливості, характерні для VPN-систем, проте з додатковими удосконаленнями для покращення безпеки і надійності передачі.

Основні компоненти системи включають кінцеві точки — джерело та отримувача даних, які можуть функціонувати як взаємозамінні. У рамках цієї концепції кожен кінцевий пристрій може як надсилати, так і приймати дані, залежно від поточної задачі. Це дозволяє реалізувати гнучкість у використанні каналу, зокрема в сценаріях обміну даними між двома рівноправними пристроями. Далі йде канал передачі, який в даному випадку є багатоканальним і забезпечує додатковий захист через використання шифрування та розподілу трафіку між VPN-тунелями.

Процеси шифрування в новій архітектурі виконуються на апаратних VPN-шлюзах, що використовують алгоритм AES-256, які забезпечують високий рівень конфіденційності і алгоритм шифрування SHA-256 для забезпечення цілісності. Кожен блок даних розподіляється через декілька незалежних VPN-тунелів, що забезпечує випадковий розподіл та ускладнює перехоплення інформації. Контроль доступу також реалізовано через протоколи EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) та IPsec IKEv2(Internet Key Exchange version 2), які додають до автентифікації багаторівневий підхід, що включає перевірку сертифікатів і генерацію сесійних ключів.

Далі, будова каналу розглядатиметься детальніше, де будуть описані методи шифрування, контроль доступу, особливості маршрутизації та збирання даних на боці отримувача[18, 34].

3.2.1 Джерело даних і Отримувач даних

Кінцеві точки в даній системі — це комп’ютери або інші пристрої, що можуть як передавати, так і приймати зашифровані дані, а також наступний маршрутизатор, що виступає апаратним VPN-шлюзом. Ці компоненти можуть працювати як Джерело або Отримувач зашифрованих даних залежно від поточної задачі. У розглянутій моделі найпростішим варіантом кінцевої точки є комп’ютер[18, 29].

Функції Джерела даних[18, 29]:

Встановлення з'єднання та завершення: передача ініціюється шляхом надсилання запиту Отримувачу і завершується після передачі всіх файлів.

Розподіл інформації на блоки: VPN-шлюз розподіляє інформацію на окремі блоки даних.

Шифрування та хешування: VPN-шлюз шифрує кожен блок і додає хеші попереднього та наступного блоків для забезпечення цілісності та автентичності.

Функції Отримувача даних[18, 29]:

Автентифікація та контроль доступу: Під час з'єднання здійснюється обмін ключами шифрування. Після авторизації встановлюються параметри каналів передачі.

Прийом і дешифрування блоків: Отримані через канали блоки дешифруються та перевіряються за хешами.

Відновлення порядку блоків: Інформація збирається у вихідний вигляд за допомогою хеш-ідентифікаторів.

Для належного функціонування VPN-шлюзам потрібен спеціальний драйвер, що забезпечуватиме виконання всіх функцій шифрування й управління каналами.

Далі поетапно проведемо розрахунки для визначення мінімальних параметрів апаратного забезпечення, зокрема для оперативної пам'яті (RAM), процесорів, та пропускної здатності VPN-шлюзів, щоб вони дійсно відповідали потребам роботи з блоками даних і виконання основних функцій запропонованого закритого каналу без впливу на інші завдання користувача[18, 29].

VPN-шлюзи повинні мати наступні параметри для підтримки безперебійної роботи[18, 29]:

Процесор: Спеціалізовані процесори, як-от ARM(Advanced RISC Machines) або ASIC (Application-Specific Integrated Circuit) для швидкого шифрування, щоб знизити навантаження на основний процесор. Повинен підтримувати швидкість шифрування AES-256 мінімум 50 МБ/с. Для підтримки такої швидкості потрібен спеціалізований чип, який підтримує апаратне шифрування AES-256 (наприклад, ASIC або ARM із вбудованими криптографічними інструкціями).

RAM: 2 ГБ достатньо для обробки одночасних операцій шифрування/дешифрування, буферизації, контролю за каналами, розподілу блоків перед передачею та підтримки 5 паралельних тунелів.

Пропускна здатність: 1 Гбіт/с для обробки трафіку без затримок.

Розглянемо, як саме використовується RAM для кожної з основних функцій шлюза для обґрунтування потреб[18, 29]:

1. Буферизація блоків

Кожен тунель обробляє пакети розміром 1432 байти: Для 5 тунелів, кожен з яких обробляє до 10 блоків одночасно (розподіл і збереження перед передачею) розраховується добутком розміру блоків на кількість блоків помножити на кількість каналів: $RAM_{буфер} = 1432 \times 10 \times 5 = 71600\,байт \approx 70\,КБ$.

2. Пам’ять для шифрування/дешифрування

Для AES-256 обробляється блок у пам’яті до 16 байтів за цикл. Якщо одночасно шифрується/дешифрується 10 блоків для кожного з 5 тунелів, то

розмір пам’яті розраховується добутком розміру блоків на кількість блоків помножити на кількість каналів: $RAM_{AES} = 1432 \times 10 \times 5 = 71600\,байт$.

Потреби RAM для шифрувального процесу залишаються такими ж, як для буферизації, оскільки пакети обробляються послідовно. Разом на буферизацію та шифрування необхідно ~140 КБ.

3. Контроль каналів

Пам'ять використовується для зберігання метаданих про кожен тунель. Таблицю станів для кожного з 5 тунелів (ключі, хеши, сесійна інформація) можна розрахувати за формулою 3.1:

$$RAM_{Контроль\,каналів} = S_{Розмір\,пам'яті} \times N_{Тунелів}, \quad (3.1)$$

Підставляємо значення:

$$RAM_{канали} = 50 \times 5 = 250\,КБ.$$

Де:

$S_{Розмір\,пам'яті} = 50\,КБ$ на тунель (сертифікати, ключі, протокольні дані).

4. Службові потреби ОС(Операційна система)

ОС для VPN-шлюза, наприклад, на базі спеціалізованого Cisco IOS, займає: мінімум 1 ГБ для ядра, драйверів і фонових процесів.

5. Резерв для пікових навантажень

Резерв пам’яті на випадок збільшення кількості блоків або неочікуваного навантаження $RAM_{резерв} = 500\,МБ$.

Об’єднаємо всі частини:

Буферизація та шифрування: 140 КБ.

Контроль каналів: 250 КБ.

ОС: 1 ГБ.

Резерв: 500 МБ.

Загальну пам’ять можна вирахувати за формулою 3.2:

$$RAM_{загальна} = RAM_{буфер} + RAM_{AES} + RAM_{канали} + RAM_{ОС} + RAM_{резерв}, \quad (3.2)$$

Підставляємо значення:

$$RAM_{загальна} = 70\,КБ + 70\,КБ + 250\,КБ + 1\,ГБ + 500\,МБ = 1.64\,ГБ.$$

Для округлення та гарантування стабільної роботи обирається значення 2 ГБ.

Ці значення є мінімально достатніми для виконання функцій шифрування та дешифрування блоків у VPN-шлюзах, забезпечуючи стабільне і швидке з'єднання без негативного впливу на основні завдання комп'ютера користувача. Приклад такого апаратного VPN-шлюза можна побачити на рис. 3.1-3.3.

Рисунок 3.1 - Апаратний VPN-шлюз Cisco Meraki MX250

Рисунок 3.2 - Апаратний VPN-шлюз FortiGate 100F

Рисунок 3.3 - Апаратний VPN-шлюз Ubiquiti UniFi Dream Machine Pro

Система повинна враховувати обсяг переданих даних. Якщо обсяг невеликий, всі блоки можуть бути зібрані, зашифровані та відправлені одразу. Якщо обсяг великий (понад певне значення), шифрування блоків відбувається в режимі реального часу, що дозволяє миттєво розподіляти блоки між каналами для уникнення затримок. Оптимальний обсяг даних для перемикання між режимами шифрування розраховано з урахуванням ресурсів VPN-шлюза[18, 29].

Розрахунок обсягу даних для перемикання між режимами шифрування базується на наступних параметрах[18, 29]:

Середня пропускна здатність VPN-шлюза – 1 Гбіт/с, або 125 МБ/с.

Швидкість шифрування (AES-256) – орієнтовно 50 МБ/с для середньостатистичного VPN-шлюза з апаратним шифруванням. Це є консервативною оцінкою для процесора середнього класу з апаратним шифруванням.

Обмеження за часом – припустимо, що для забезпечення безперебійної роботи без затримок шифрування та передача блоків даних мають завершитися за 2 секунди.

Проводимо розрахунки:

Виходячи з цих параметрів, можемо обчислити обсяг даних, який може бути оброблений протягом 2 секунд за наступною формулою 3.3:

$$a_{Максимальний\ обсяг\ даних} = ¿ ¿\left(R_{Пропускна\ здатність\ VPN-шлюза}, V_{Швидкість\ шифрування}\right) \times t_{Обмеження\ за\ часом}, (3.3)$$

де:

$R_{Пропускна\ здатність\ VPN-шлюза} = 125\ МБ/с$,

$V_{Швидкість\ шифрування} = 50\ МБ/с$,

$t_{Обмеження\ за\ часом} = 2\ с$,

Підставляємо значення в формулу 3.3:

$$a_{Максимальний\ обсяг\ даних} = min(125,50) \times 2 = 50 \times 2 = 100\ МБ.$$

Таким чином, 100 МБ — це оптимальне значення обсягу даних, при якому ще можна проводити повне шифрування всіх блоків одночасно без затримок. При перевищенні цього обсягу доцільно перемикатись на режим шифрування в реальному часі, щоб уникнути надмірного навантаження на систему.

Далі будуть проведені розрахунки оптимального розміру передаваємих блоків інформації. За нинішніми стандартами для протоколу IPsec найефективніший розмір передаваємих блоків знаходиться в діапазоні 1,400-1,440 байтів[18, 29].

Основні елементи блоку: Розмір корисного блоку даних: 1300 байтів (для корисної інформації).

Маркер порядкового номера: Розмір: 4 байти.

Хеші попереднього і наступного блоків: Хешування з використанням алгоритму SHA-256 для кожного блоку, що займає 32 байти на хеш. Накладні витрати: 2 хеші = 64 байти.

Заголовки VPN (IPsec IKEv2): Включають приблизно 20–24 байти для заголовка, 8 байтів для ESP-трейлера, та 32 байти для SHA-256, що разом становить 60–64 байти.

Підсумок розрахунків: Об'єднаймо всі елементи, щоб перевірити суму накладних витрат та розмір блоку за формулою 3.4:

$$S_{Загальний\ розмір\ блоку} = ¿ ¿ S_{Дані} + S_{Маркер\ порядкового\ номера} + S_{Хеші} + S_{Заголовки\ VPN}, \quad (3.4)$$

Підставляємо значення в формулу:

$$S_{Загальний\ розмір\ блоку} = 1300 + 4 + 64 + 64 = 1432\ байти.$$

Таким чином, розмір одного блоку з усіма накладними витратами становить 1432 байти, що відповідає вимогам щодо розміру в діапазоні 1400–1440 байтів.

Цей розмір блоку є оптимальним для ефективної передачі даних через VPN-канали з MTU(Maximum Transmission Unit – максимальний розмір блоку корисного навантаження) 1500 байтів, мінімізуючи накладні витрати на фрагментацію та підвищуючи надійність передачі.

Розмір блоку 1,432 байтів було обрано на основі оптимального балансу між продуктивністю, ефективністю шифрування, та мінімізацією затримок. Такий розмір відповідає ряду вимог, які забезпечують надійність та швидкість обробки даних в реальному часі без значного навантаження на ресурси.

Розмір блоку 1,432 байтів обрано для забезпечення балансу між продуктивністю, ефективністю шифрування та мінімізацією затримок. Цей розмір оптимальний для швидкої обробки даних і зменшує навантаження на VPN-шлюзи, дозволяючи шифрувати дані великими частинами. При пропускній здатності 1 Гбіт/с блок передається за 0.0115 мс, що відповідає можливостям мережі без перевантаження обладнання. Менший розмір збільшив би навантаження, а більший — ризик затримок. Блоки такого розміру зручно

обробляються операційними системами й мережевими інфраструктурами, полегшуючи маршрутизацію, розподіл між каналами та відновлення даних.

Цей розмір є достатньо великим для мінімізації кількості операцій, але не надто великим, щоб викликати надмірне навантаження на обладнання або створити ризики затримок у зв’язку.

Далі розрахункового обґрунтуємо розмір блоку в 1,432 байтів розглядаючи основні фактори, які включають час обробки шифрування, затримки передачі, та обмеження пропускної здатності для VPN-шлюза і комп’ютерів. Проведемо оцінку відповідно до доступної пропускної здатності, швидкості шифрування, обсягу RAM, та продуктивності процесора[18, 29, 34].

Вхідні дані для розрахунків[18, 29]:

Пропускна здатність VPN-шлюза та мережі: 1 Гбіт/с (або 125 МБ/с).

Продуктивність VPN-шлюза для шифрування: розглянемо продуктивність у межах 50 МБ/с для AES-256.

Час затримки на обробку кожного блоку шифрування та передачі.

Розрахунок часу обробки для блоку розміром 1,432 байтів

1. Час шифрування одного блоку розміром 1,432 байтів можна розрахувати за формулою 3.5:

$$t_{шифрування} = \frac{S_{Розмір\,блоку}}{V_{Швидкість\,шифрування}}, \tag{3.5}$$

При швидкості шифрування в 50 МБ/с на шифрування одного блоку розміром 1,432 байтів знадобиться:

$$t_{шифрування} = \frac{1{,}432}{50} = 0.00002731323\,(\,або\,27.3\,мкс\,).$$

Отже, час шифрування блоку 1,432 байтів дорівнює 27.3 мкс.

2. Час передачі одного блоку розміром 1,432 байтів через мережу можна розрахувати за формулою 3.6:

$$t_{передачі} = \frac{S_{Розмір\,блоку}}{R_{Пропускна\,здатність}}, \tag{3.6}$$

При пропускній здатності каналу 1 Гбіт/с (125 МБ/с), на передачу блоку розміром 1,432 байтів знадобиться:

$$t_{передачі} = \frac{1{,}432}{125} = 0.00001092529\,(с)\,(або\ 10.9\ мкс).$$

Час передачі блоку 1,432 байтів — 10.9 мкс.

3. Загальний час обробки і передачі блоку розміром 1,432 байтів розраховуватимемо за формулою 3.7:

$$t_{загальний} = t_{шифрування} + t_{передачі}, \tag{3.7}$$

Загальний час для обробки і передачі одного блоку розміром 1,432 байтів складається з часу шифрування і часу передачі:

$$t_{загальний} = 27.3 + 10.9 \approx 38.23\ мкс.$$

Таким чином, загальний час для передачі одного блоку 1,432 байтів через VPN-шлюз з шифруванням становить 38.23 мкс.

Розрахунок кількості блоків і обробки будемо проводити за формулою 3.8:

$$N_{блоків} = \frac{1\,с}{t_{загальний}}, \tag{3.8}$$

При загальному часі мкс мкс для одного блоку 1 МБ VPN-шлюз може обробляти:

$$N_{блоків} = \frac{1}{0.00003823852} \approx 26152\ блоків/с.$$

Ефективна швидкість передачі даних обчислюється за формулою 3.9:

$$V_{Ефективна\ швидкість} = N_{блоків} \times S_{Розмір\ блоку}, \tag{3.19}$$

Підставляємо значення в формулу:

$$V_{Ефективна\ швидкість} = 26152\left(\frac{блоків}{с}\right) \times 1{,}432\,(байт) \approx 36.2\left(\frac{МБ}{с}\right).$$

Ефективність використання каналу розраховується за формулою 3.10:

$$\eta_{каналу} = \frac{V_{Ефективна\ швидкість}}{V_{Максимальна\ швидкість}}, \tag{3.10}$$

Де:

$V_{Максимальна\ швидкість} = 125\ МБ/с.$

Підставляємо значення в формулу:

$$\eta_{каналу} = \frac{36.2\left(\frac{МБ}{с}\right)}{125\left(\frac{МБ}{с}\right)} \times 100\,\% \approx 28.9\,\%.$$

Таким чином, при розмірі блоку 1,432 байтів VPN-шлюз з мінімальними параметрами забезпечує ефективність каналу на рівні 28.9%, залишаючи резерв для інших потреб мережі.

Ця ефективність зумовлена швидкістю шифрування 50 МБ/с, яка є мінімальною для апаратних VPN-шлюзів. Якщо використовувати потужніший пристрій зі швидкістю шифрування 250 МБ/с, ефективність каналу становитиме 66,7% і більше.

Розмір блоку 1,432 байтів мінімізує потребу у фрагментації, що повністю узгоджується з обмеженнями MTU для більшості VPN-протоколів, таких як IPsec. Це дозволяє зменшити кількість пакетів і знизити ризик втрати інформації, забезпечуючи кращу надійність передачі.

Зменшення затримок і полегшення відновлення пакетів: Менший розмір блоку зменшує кількість даних, які можуть бути втрачені через затримку чи збої в мережі. У разі втрати пакета потрібна повторна передача лише окремих невеликих блоків, що прискорює відновлення та зменшує затримки.

Гнучкість при підвищеному навантаженні: Розмір блоку 1,432 байтів сприяє ефективнішому розподіленню трафіку між кількома VPN-каналами, дозволяючи мережі адаптуватися до високих навантажень або непередбачуваних коливань трафіку. Це критично важливо для корпоративних мереж, де потрібні висока надійність і стабільність навіть під час пікових навантажень[18, 29].

3.2.2 Метод шифрування

Для нового закритого каналу передачі, який забезпечується на основі VPN-технології, шифрування і дешифрування даних виконується на апаратних VPN-шлюзах із застосуванням алгоритму AES-256. Цей алгоритм є стандартом для захищених комунікацій у сучасних мережах завдяки своїй ефективності та високому рівню захисту. Його обирають через такі ключові переваги: стійкість до атак «грубої сили» завдяки 256-бітовому ключу, швидкість обробки даних і сумісність з апаратними модулями шифрування [3, 30].

Основні кроки методу шифрування [3, 30, 34]:

1. Генерація ключів. VPN-шлюз генерує унікальні ключі для шифрування кожної сесії зв’язку, зокрема сесійні ключі, які використовуються для симетричного шифрування даних. Для їх обміну між шлюзами застосовують асиметричне шифрування з алгоритмом RSA, що забезпечують захист ключів під час передачі.

2. Розбиття даних на блоки та їх шифрування. Кожен блок проходить шифрування на VPN-шлюзі, використовуючи AES-256.

3. Контроль цілісності з використанням хеш-функції. Для кожного блоку даних VPN-шлюз генерує контрольну хеш-суму (SHA-256), яка дозволяє перевірити цілісність даних при їх зборі на боці отримувача.

В контексті нового закритого каналу, шифрування і дешифрування мають низку особливостей, пов’язаних з багатоканальною передачею даних і додатковими заходами безпеки:

Шифрування для багатоканальної передачі. Дані, зашифровані на VPN-шлюзі, випадково розподіляються між кількома закритими каналами зв’язку. Це підвищує рівень безпеки, оскільки навіть при перехопленні частини трафіку зловмисник не зможе відновити цілісне повідомлення. Кожен VPN-шлюз підтримує розподіл трафіку на основі унікальних ідентифікаторів блоків та надає окремий ключ для кожного з каналів, що посилює безпеку передачі.

Автоматизоване управління ключами. Ключі шифрування для кожної сесії генеруються автоматично, і процес їх обміну здійснюється з мінімальним втручанням оператора. Це знижує ризик витоку ключів і підвищує надійність системи, а також дозволяє здійснювати регулярну ротацію ключів.

Стійкість до відмов. Оскільки дані передаються через кілька каналів, при відмові одного з каналів система може перерозподілити блоки на інші доступні канали, забезпечуючи безперервність передачі. Це можливо завдяки тому, що кожен блок шифрується окремо, і VPN-шлюз може динамічно керувати маршрутизацією блоків [3, 30].

3.2.3 Середовище передачі

У розробленій концепції закритого каналу передачі даних середовище передачі побудовано на основі використання кількох паралельних тунельних каналів, що забезпечує додатковий захист і відмовостійкість. Дані передаються одночасно через декілька маршрутизованих каналів, які проходять через різні вузли в мережі інтернету. Ці вузли можуть перетинатися лише частково або бути зовсім різними, забезпечуючи незалежність маршрутів. Саме цей розподіл інформаційного потоку на кілька каналів знижує ймовірність перехоплення, оскільки зловмисник мусив би одночасно контролювати всі канали для відновлення повної інформації.

Інтернет як середовище передачі є відкритим, а це означає, що дані проходять через численні проміжні вузли, де можуть змішуватися з різними типами трафіку інших користувачів. У цьому підході кожен тунельний канал є зашифрованим і самостійно захищеним від потенційних загроз, що мінімізує ризик перехоплення даних навіть у відкритому середовищі. За допомогою технології тунелювання створюються віртуальні маршрути, які прокладаються поверх загальної інтернет-інфраструктури, забезпечуючи при цьому високий рівень конфіденційності та захисту.

Усі канали передають дані незалежно і можуть мати свої специфічні характеристики, такі як відмінності в кількості проміжних вузлів, рівні затримки та швидкості передачі. Це ускладнює спроби перехоплення, оскільки кожен блок даних може проходити власним маршрутом і об’єднується в правильному порядку лише на приймальній стороні.

Оскільки інтернет є відкритим середовищем передачі, дані проходять через численні проміжні вузли, які обробляють великий обсяг трафіку і забезпечують одночасний доступ для безлічі користувачів. У магістральних мережах, де використовуються потужні маршрутизатори, пропускна здатність може досягати від 40 Гбіт/с до кількох Тбіт/с. Наприклад, сучасні маршрутизатори інтернет-провайдерів мають інтерфейси зі швидкістю до 100 або навіть 400 Гбіт/с, що дозволяє обробляти великі обсяги трафіку з низькою затримкою навіть у найвищих точках навантаження.

Маршрутизатори інтернет-провайдерів і вузли обміну трафіком, які з'єднують мережі кількох провайдерів, зазвичай мають пропускну здатність від 10 до 100 Гбіт/с на один інтерфейс. Ці вузли забезпечують взаємозв’язок між кількома мережами, передаючи значні обсяги трафіку між провайдерами. У порівнянні з магістральними маршрутизаторами, вузли обміну трафіком можуть мати дещо меншу пропускну здатність, але вона залишається значною для підтримки стабільного з'єднання та передачі даних високої інтенсивності.

У мережах доступу, які з'єднують кінцевих користувачів, використовуються комутатори з пропускною здатністю в діапазоні від 1 до 10 Гбіт/с. Вони забезпечують обслуговування локальних підключень та менших обсягів даних порівняно з магістральними вузлами. Для великих провайдерів, що підключають локальні мережі до загальної інфраструктури інтернету, типові маршрутизатори у WAN(Wide Area Network)-середовищі мають пропускну здатність від 1 до 10 Гбіт/с, що дозволяє їм з’єднувати менші мережі з магістральними вузлами та забезпечувати прийнятний рівень обробки трафіку. Спрощену схему передачі інформації даним каналом можна побачити на рис. 3.4.

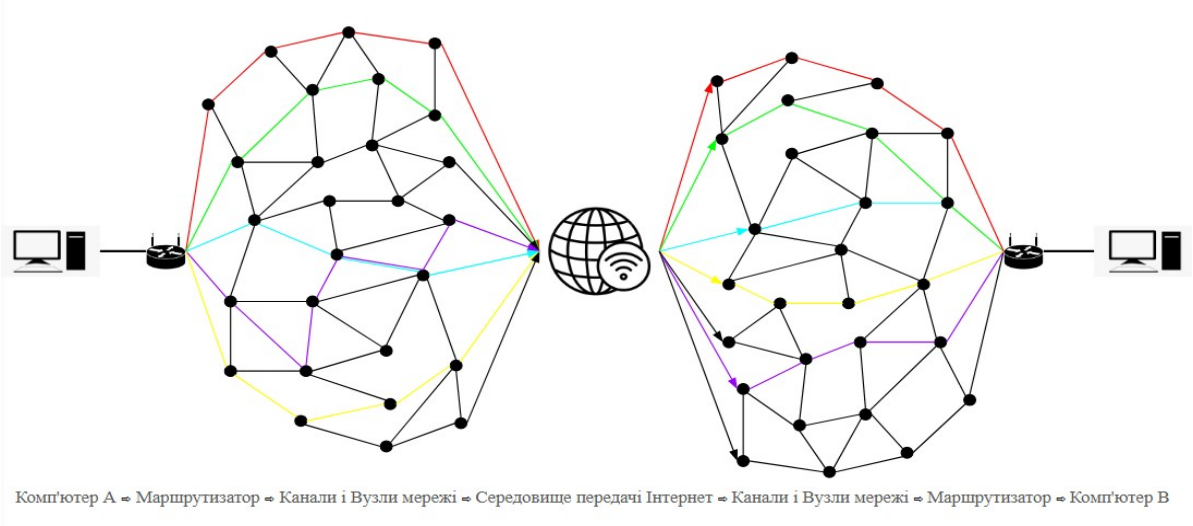


Рисунок 3.4 - Багатоканальна схема передачі інформації

В цьому багатоканальному підході VPN-тунелювання дозволяє створити віртуальні маршрути поверх існуючої інфраструктури інтернету, де кожен канал може передавати дані через різні комбінації вузлів, таких як маршрутизатори і комутатори, залежно від доступної пропускної здатності на кожному вузлі. Така

інфраструктура забезпечує додатковий рівень захисту і дозволяє стабільно передавати дані навіть при високому навантаженні в мережі [11, 14].

3.2.4 Контроль доступу та автентифікація

В даному закритому каналі передачі даних контроль доступу та автентифікація в першу чергу забезпечується через протокол EAP (Extensible Authentication Protocol), підтверджують особу користувача через паролі, сертифікати чи двофакторну аутентифікацію. Зокрема, використовується його версія EAP-TLS, який забезпечує обмін ключами через асиметричне шифрування, використовуючи сертифікати X.509 для автентифікації обох сторін з'єднання. Під час рукостискання сертифікати перевіряють справжність за допомогою відкритих і закритих ключів: відкритий ключ підтверджує підпис, зроблений закритим ключем відправника. Після успішної автентифікації EAP-TLS встановлює симетричний сеансовий ключ для шифрування даних у поточному сеансі, що оптимізує ефективність обробки інформації та зменшує час її передавання.

Для більшої безпеки в даному каналі використовується VPN-з'єднання на основі протоколу IPsec у конфігурації для тунельного режиму. Кожен з VPN-каналів, побудованих на основі IPsec у тунельному режимі, буде проходити через різні маршрути, тому захист переданих даних та автентифікація повинні враховувати цю особливість. Для кожного каналу застосовується протокол IPsec IKEv2, який забезпечує стійкість з'єднання, а також підтримує AES-256 для конфіденційності та SHA-256 для цілісності даних. IPsec VPN використовує ESP для інкапсуляції й автентифікації даних, що гарантує захист як самого вмісту, так і заголовків пакетів на кожному окремому маршруті[11, 30].

Для узагальнення використовується наступна версія протоколу IPsec IKEv2. Протокол IKEv2 має модульну структуру, що дозволяє налаштувати його для підтримки конкретних алгоритмів шифрування та методів аутентифікації. Кожен із протоколів у даній конфігурації виконує власну функцію в рамках тунельного з’єднання:

Протокол EAP-TLS забезпечує обмін ключами, що підтверджує особу користувача та автентифікує кожну сторону через сертифікати X.509. Це працює як на етапі встановлення з’єднання, так і для подальшої перевірки безпеки.

Протокол ESP забезпечує тунелювання та шифрування даних на рівні IP, інкапсулюючи та захищаючи пакети для надійної передачі між двома точками.

Шифрування AES-256 використовується для конфіденційності, що гарантує високий рівень захисту даних під час передачі, оскільки AES-256 є одним із найбільш стійких алгоритмів для шифрування.

SHA-256 служить для забезпечення цілісності даних, перевіряючи, що дані залишаються незмінними під час передачі [19-20].

3.3 Методи дослідження

У цьому підрозділі досліджується проектований закритий канал передачі даних, який був розроблений із застосуванням багатоканальної архітектури та сучасних криптографічних методів. Основна мета дослідження полягає у визначенні рівня захищеності, продуктивності та ефективності запропонованого рішення.

У наступних підрозділах буде описано методи дослідження, що включають порівняльний аналіз із традиційними рішеннями, криптографічний аналіз стійкості та оцінку відповідності каналу вимогам безпеки в сучасних мережах. Це дозволить отримати комплексну картину його можливостей і визначити оптимальні сфери застосування.

3.3.1 Порівняльний аналіз різних технологій закритих каналів

Для проведення порівняльного аналізу різних технологій закритих каналів передачі даних, націленого на новий запропонований канал, можна виділити наступні ключові аспекти. Це дозволить оцінити, як новий канал виглядає на фоні інших технологій та обґрунтувати його потенційні переваги і недоліки[18, 30]:

1. Рівень захисту від перехоплення: Багатоканальна архітектура нового каналу розподіляє блоки даних між незалежними шифрованими каналами, кожен з яких передає окремий фрагмент. Це забезпечує додатковий рівень безпеки, оскільки для повного перехоплення інформації зловмиснику потрібен доступ до всіх каналів одночасно.

Перевага перед фізично захищеними лініями: Фізично захищені лінії обмежуються інфраструктурними бар'єрами, що створює ризики за компрометації обладнання. У таких лініях шифрування — лише додатковий рівень захисту. Новий канал із багатоканальним шифруванням забезпечує захист навіть у публічних мережах, що робить його ідеальним для корпоративних потреб і мобільного доступу.

Порівняння з мобільними і супутниковими каналами: Мобільні та супутникові канали захищені протоколами аутентифікації та шифрування, але вразливі до атак на сигнал. Багатоканальна архітектура нового каналу розподіляє дані між кількома шляхами, ускладнюючи перехоплення повного обсягу даних навіть при часткових зламах.

Захист у порівнянні зі стандартними VPN: Стандартні VPN передають потік через один тунель, що піддає його ризику атак типу MITM. Новий канал розподіляє дані між кількома тунелями, знижуючи ефективність атак і забезпечуючи більший рівень безпеки навіть при спробах перехоплення.

2. Цілісність даних: Новий канал використовує технологію на основі блокчейн-технологій для контролю цілісності: кожен блок містить хеші сусідніх блоків, що дозволяє одразу виявити зміни чи втрати даних під час передачі і правильно відновити послідовність блоків даних. Багато існуючих закритих каналів, зокрема мобільні мережі 5G, основний акцент роблять на швидкості, тоді як новий канал забезпечує високу цілісність переданих даних, що є критичним для корпоративних або урядових структур.

Перевага перед мобільними мережами (зокрема 5G): 5G забезпечує високу швидкість, але контроль цілісності часто недостатній для критичних даних.

Новий канал із блокчейн-перевіркою автоматично виявляє втрати чи зміни даних, підвищуючи надійність передачі.

Перевага перед стандартними VPN та фізично захищеними лініями: Стандартні VPN використовують хешування, але не забезпечують детального багаторівневого контролю кожного блоку. Фізично захищені лінії обмежені в контролі цілісності, тоді як новий канал із блокчейн-контролем дозволяє миттєво виявляти зміни в даних.

Захист у порівнянні з супутниковими каналами: У супутникових мережах передачі інформація часто піддається природним перешкодам і затримкам, що може вплинути на цілісність даних. У новому каналі хешування блоку гарантує виявлення будь-яких зовнішніх змін або технічних проблем, зберігаючи надійність передачі.

3. Продуктивність і затримки: Новий канал із апаратними VPN-шлюзами забезпечує високу продуктивність і менші затримки порівняно зі стандартним VPN із програмним шифруванням. Завдяки спеціалізованим мікросхемам апаратні шлюзи швидше обробляють дані, зменшуючи навантаження на систему. Однак при великих обсягах даних або численних з'єднаннях вони можуть бути перевантажені, що впливає на швидкість передачі. Фізично захищені лінії не мають такого обмеження, оскільки їх продуктивність не залежить від шифрування.

Перевага над стандартним VPN з програмним шифруванням: Стандартний VPN, який використовує програмне шифрування, витрачає більше часу на обробку даних, оскільки всі операції здійснюються за допомогою процесора комп'ютера чи сервера. Це може призвести до значного навантаження на систему і затримок, особливо при передачі великих обсягів інформації. Апаратні шлюзи в новому каналі, навпаки, виконують шифрування швидше завдяки спеціалізованим мікросхемам, що знижує загальну затримку і дозволяє обробляти дані ефективніше.

Порівняння з мобільними мережами: Мобільні мережі (4G/5G) можуть мати затримки через змінні умови сигналу, зокрема відстань до базової станції.

Новий канал, завдяки VPN із апаратним шифруванням, забезпечує стабільність, але під значним навантаженням може втрачати продуктивність, як і всі канали.

4. Гнучкість і можливість масштабування: Новий канал із паралельними VPN-тунелями дозволяє легко розширювати інфраструктуру, змінювати конфігурацію і забезпечувати стабільну передачу даних навіть при збоях. Це важливо для корпоративних мереж, які потребують додаткових ресурсів і нових маршрутів для безперебійної роботи.

Перевага над фізично захищеними лініями: Фізично захищені лінії не мають гнучкості для змін маршруту чи додавання каналів, тоді як новий канал дозволяє динамічно налаштовувати маршрути і підвищує стійкість до збоїв.

Резервування каналів: Багатоканальна архітектура забезпечує резервування — при виході з ладу одного VPN-каналу трафік перенаправляється через інші, зберігаючи продуктивність і дані. Це надійніше, ніж у мобільних чи супутникових мережах, де резервування залежить від сигналу.

Управління навантаженням: Кілька тунелів розподіляють навантаження, зменшуючи затримки і підвищуючи ефективність передачі. На відміну від мобільних і супутникових каналів, новий канал забезпечує кращу масштабованість і гнучкість.

5. Автентифікація та контроль доступу: Новий канал передачі даних використовує протоколи EAP-TLS та IPsec IKEv2, що забезпечують високий рівень автентифікації користувачів та шифрування з'єднань. Ці протоколи створюють багаторівневу структуру автентифікації, яка значно підвищує надійність каналу порівняно з мобільними та супутниковими мережами. Високий рівень автентифікації захищає канал від підробки особи і знижує ризик несанкціонованого доступу, що може бути критичним для корпоративних мереж.

Перевага багаторівневої автентифікації: EAP-TLS використовує сертифікати X.509, що ускладнюють підробку, оскільки для автентифікації потрібен сертифікат від центру сертифікації (CA). На відміну від мобільних і супутникових мереж, де часто застосовуються прості методи, наприклад SIM-карта, цей підхід значно підвищує рівень захисту.

Захист від підробки особи: Протокол IKEv2 забезпечує захищений обмін симетричними ключами для шифрування даних, знижуючи ризик атак типу MITM. Для перехоплення зловмисникам потрібно заволодіти як сертифікатом, так і закритим ключем, що є складним завданням.

6. Складність налаштування і вартість підтримки: Хоча новий канал надає багато переваг з точки зору безпеки, він також є складнішим у налаштуванні та підтримці порівняно з фізичними захищеними лініями чи мобільними каналами, що можуть працювати без складних процедур управління кількома VPN-тунелями.

Складність налаштування VPN і проектованого каналу: Стандартні VPN налаштовуються, як правило, за допомогою одного тунелю між кінцевими точками, що забезпечує базовий рівень безпеки. У випадку проектованого каналу, необхідно створити кілька паралельних тунелів, кожен з яких вимагає окремих налаштувань для шифрування, маршрутизації та автентифікації. Така архітектура вимагає більше часу на початкове налаштування, оскільки кожен канал потребує відповідного налаштування апаратних шлюзів, маршрутизації та захисту.

Вартість підтримки і технічні вимоги:

Стандартний VPN: Зазвичай, стандартні VPN-послуги надаються через підписку і можуть працювати як для малого бізнесу, так і для особистих потреб. Ціни залежать від постачальника, функціоналу (наприклад, кількість серверів, підтримка швидкості та доступність додаткових функцій, як-от розширений захист). Загальні етапи і витрати:

Купівля VPN-підписки: Більшість популярних VPN-сервісів, таких як NordVPN, ExpressVPN або CyberGhost, коштують від $5 до $15 на місяць за підписку для одного користувача, але для бізнес-рівня (корпоративний VPN) ціни можуть стартувати від $50 за користувача на місяць або близько $500–$1000 на рік за корпоративний план з більшим набором функцій.

Встановлення та налаштування: Зазвичай VPN-провайдери надають дуже прості інструкції з налаштування, тож цей етап не потребує значних

ресурсів для малого бізнесу. Однак, якщо необхідно налаштовувати VPN для більшої кількості користувачів, часто залучають IT-спеціаліста, послуги якого коштуватимуть у середньому від $100 до $500.

Загальний кошторис на рік: $600–$2000.

Проектований багатоканальний VPN: Cisco Meraki MX250 – це обладнання корпоративного рівня з можливостями VPN, яке може забезпечити безпеку та зв’язок для середніх і великих бізнесів. Даний пристрій взятий як приклад апаратного VPN-шлюзу для обчислення можливої вартості встановлення даного каналу.

Для Cisco Meraki MX250 з реалізацією запропонованого багатоканального VPN-підходу, який включає поділ даних на декілька каналів, підвищений рівень шифрування та автентифікації, витрати та процеси включають кілька ключових елементів. Нижче наводиться детальний аналіз вартості та технічних вимог для повноцінної реалізації такої системи з використанням Cisco Meraki MX250. Загальні етапи і витрати:

Закупівля обладнання на прикладі Cisco Meraki MX250:

Вартість апаратного забезпечення: Cisco Meraki MX250 — потужне корпоративне рішення з вбудованими можливостями VPN, що також слугуватиме основним VPN-шлюзом у цій архітектурі. Вартість обладнання коливається в межах $7000–$9000.

Ліцензування: Cisco Meraki потребує ліцензії для роботи з повним набором функцій безпеки та управління. Найбільш підходящі плани ліцензування, що включають підтримку VPN і шифрування це 1-річна ліцензія, яка коштує приблизно $1000–$2000, 3-річна ліцензія ціною близько $2500–$4500 і 5-річна ліцензія $5000–$7000.

Встановлення та налаштування багатоканальної VPN-системи з посиленим шифруванням:

У даній архітектурі VPN має забезпечувати поділ трафіку на кілька паралельних тунелів, шифрування кожного блоку даних окремо і розподіл через

різні канали. Це вимагатиме налаштування як програмного, так і мережевого рівнів:

Розгортання та базове налаштування MX250: вартість праці мережевого інженера або Cisco-спеціаліста може складати від $1000 до $3000, залежно від обсягу робіт.

Налаштування багатоканального VPN: Cisco Meraki підтримує кілька одночасних тунелів VPN, але для відповідності багатоканальній концепції потрібно вручну конфігурувати розподіл трафіку між каналами. Приблизна додаткова вартість становить від $1500 до $3000.

Інтеграція шифрування AES-256 і SHA-256: Cisco Meraki MX250 підтримує IPsec та інші надійні VPN-протоколи, що дозволяють використовувати шифрування AES-256 і SHA-256. Це забезпечує захист, але вимагає детальної настройки та перевірки на відповідність корпоративним стандартам.

Інтеграція контролю доступу та багаторівневої автентифікації:

Задля досягнення підвищеного рівня безпеки передача даних включатиме багаторівневу автентифікацію:

Налаштування автентифікації EAP-TLS та IPsec IKEv2: Вартість налаштування та впровадження залежить від IT-інфраструктури компанії, орієнтовно від $1000 до $2000 для початкового налаштування всіх компонентів контролю доступу.

Підтримка сертифікатів і сесійних ключів: для відповідності концепції потрібні сертифікати на кожного користувача або пристрій, що потребує оновлення й підтримки.

Загальний кошторис на рік: $11,500–$24,000 у перший рік (включно з покупкою), і $1000–$7000 на рік надалі для ліцензування.

Таблиця 3.1 — Підсумок: Порівняння VPN та Cisco Meraki MX250

Категорія	**Стандартний VPN**	**Cisco Meraki MX250**
Покупка	$500–$1500/рік	$7000–$9000 (одноразово)

Ліцензія	Включено	$1000–$7000 (залежно від тривалості ліцензії)
Встановлення та налаштування	$100–$500 одноразово	$1000–$3000 (базове налаштування) + $1500–$3000 (багатоканальна система)
Інтеграція шифрування та автентифікації	Включено	$1000–$2000 одноразово
Загальна вартість (перший рік)	$600–$2000	$11,500–$24,000
Загальна вартість (наступні роки)	Витрати на ремонти та оновлення, які можуть варіюватися залежно від обставин	$1000–$7000 на ліцензування, з додатковими витратами на ремонти та оновлення, які можуть варіюватися залежно від обставин

Порівняння з фізично захищеними і мобільними каналами: Фізично захищені канали характеризуються високою початковою вартістю прокладання, але їхня подальша підтримка значно простіша, оскільки не потребує управління кількома тунелями. Мобільні мережі забезпечують швидке налаштування і низькі витрати на підтримку, оскільки оператори беруть на себе всі функції захисту. У випадку багатоканального VPN необхідно постійно підтримувати кілька маршрутів і контролювати навантаження на кожен з них, що збільшує операційні витрати.

Технічне обслуговування і ризики простоїв: Обслуговування багатоканального VPN вимагає регулярних оновлень налаштувань, перевірки стабільності каналів і тестування обладнання, що підвищує вимоги до персоналу. Це значно підвищує вимоги до персоналу, оскільки адміністратори повинні моніторити продуктивність і реагувати на несправності окремих тунелів. Простий VPN в цьому плані є більш надійним, адже потребує мінімальної кількості апаратних компонентів і менше залежить від кількості каналів.

Порівняння ключових показників надає основу для визначення оптимальної сфери використання кожного рішення. Новий канал, завдяки своїм перевагам, є особливо придатним для корпоративних середовищ з високими вимогами до безпеки і цілісності даних, що передаються через публічні мережі[18, 30].

3.3.2 Криптографічний аналіз захищеності каналів зв'язку

Для криптографічного аналізу захищеності проектуємого нового закритого каналу передачі даних, що побудований на VPN-технології, звернемося до таких методів шифрування та автентифікації[20-21, 26, 34]:

1. Алгоритм шифрування AES-256: У дані системі AES-256 забезпечує високий рівень конфіденційності завдяки 256-бітному ключу, який робить цей алгоритм стійким до атак «грубої сили». AES є одним із найстійкіших алгоритмів, підтримуваних апаратними модулями, що знижує навантаження на VPN-шлюзи та прискорює шифрування і дешифрування. Це зменшує ризик перехоплення, адже, навіть якщо зловмисник отримає доступ до зашифрованих даних, дешифрувати їх без ключа майже неможливо.

2. Хеш-алгоритм SHA-256: Використовується для забезпечення цілісності даних під час передачі. SHA-256 генерує 256-бітний хеш кожного блоку, що дозволяє отримувачу підтвердити, що дані не було модифіковано. Це важливо для запобігання маніпуляціям із вмістом даних, адже навіть незначна зміна блоку змінить хеш.

3. Протокол EAP-TLS: Цей протокол автентифікації на основі сертифікатів забезпечує безпечний обмін ключами і підтверджує особи користувача та сервера. EAP-TLS створює захищений канал через асиметричне шифрування, а потім встановлює симетричний сеансовий ключ для поточного сеансу. Використання сертифікатів X.509 гарантує автентичність сторін, що є важливим для недопущення несанкціонованого доступу до мережі.

4. Протокол тунелювання IPsec із ESP: Цей протокол додає шари безпеки на рівні IP, шифруючі як вміст пакетів, так і заголовки, що забезпечує захист навіть

у відкритому середовищі передачі (Інтернеті). ESP знижує ризик перехоплення, приховуючи інформацію про джерело і призначення трафіку.

Для аргументації надійності AES-256 розглянемо складність його злому за допомогою атаки «грубої сили», а також оцінку тривалості такої атаки із сучасними обчислювальними потужностями.

Алгоритм AES-256 використовує ключ довжиною 256 біт, що означає 2^{256} можливих комбінацій ключів. Це надзвичайно велика кількість варіантів, яка робить спроби злому «грубої сили» практично неможливими навіть для найпотужніших сучасних комп’ютерів.

Для прикладу, навіть з урахуванням сучасних квантових обчислень, які здатні прискорити процес взлому деяких алгоритмів шифрування (зокрема, асиметричних), AES-256 залишається стійким до атак. Квантові комп’ютери можуть скоротити кількість можливих комбінацій до приблизно 2^{128}, але навіть це все одно залишається занадто великим числом для атаки на практиці[20-21, 26].

Розрахунок часу злому для атаки «грубої сили» [20-21, 26]:

Сучасний суперкомп'ютер: Потужні суперкомп'ютери можуть обробляти близько 10^{18} (квінтильйон) комбінацій в секунду. Однак навіть при такій швидкості обробка всіх можливих комбінацій AES-256 можна розрахувати за формулою 3.11:

$$t_{злам} = \frac{N_{Кількість\ комбінацій\ AES}}{V_{Швидкість\ перебору\ суперкомпёютера}}, \tag{3.11}$$

Підставляємо значення:

$$t_{злам} = \frac{2^{256}}{10^{18}} = 3.6 \times 10^{52} c.$$

Переведення часу: Щоб зрозуміти цей час, переведемо його у роки. Отримане число в секундах дорівнює приблизно:

$$3.6 \times 10^{52} c \approx 1.14 \times 10^{45} років.$$

Ця кількість років значно перевищує вік Всесвіту (приблизно 13.8 мільярда років), що робить AES-256 надзвичайно стійким до зламу за допомогою підбору ключа для найпотужніших сучасних систем.

Цей розрахунок демонструє, що AES-256 є надзвичайно надійним для використання в будь-якому середовищі, включно з вашим каналом передачі даних. Навіть якщо зловмисник зуміє перехопити зашифрований файл або блок даних, без наявного ключа зламати AES-256 у розумні терміни неможливо.

Окрім атаки «грубої сили», існує кілька інших аспектів, що підвищують надійність AES-256 як криптографічного алгоритму — навіть проти більш специфічних типів атак, які можуть пришвидшити процес дешифрування. Проте проти більшості з них уже існують готові та перевірені рішення[20-21, 26, 34]:

Атаки сторонніх каналів (англ. Side-Channel Attacks) ґрунтуються на аналізі фізичних характеристик процесу шифрування, таких як енергоспоживання чи електромагнітні випромінювання, і потребують фізичного доступу до пристрою або спеціального обладнання. Для захисту від них використовуються екрановані пристрої або платформи з мінімізацією витоків фізичних даних. Атаки з витоком часу обчислень (англ. Timing Attacks) спираються на вимірювання часу, необхідного для криптографічних операцій, щоб виявити ключові дані. Апаратні модулі, як-от AES-NI, ускладнюють реалізацію таких атак, знижуючи різницю в часі виконання. Диференціальний і лінійний криптоаналіз, що базується на пошуку статистичних закономірностей, малоефективний проти AES-256 завдяки 14 раундам шифрування. Загалом AES-256 забезпечує високу стійкість до сучасних атак і оптимальний захист у захищених каналах передачі даних, особливо за апаратної реалізації та з дотриманням принципів безпеки.

SHA-256 є частиною родини алгоритмів SHA-2, розроблених Національним інститутом стандартів і технологій США (NIST). Він має кілька важливих характеристик, які роблять його надзвичайно надійним.

SHA-256 забезпечує високу стійкість до колізій, тобто випадків, коли два різних повідомлення мають однаковий хеш. Ймовірність такої колізії дуже мала і вимагає приблизно 2^{128} обчислень, що робить атаку майже неможливою навіть для сучасних обчислювальних потужностей. Крім того, алгоритм має лавиноподібний ефект: будь-яка, навіть незначна зміна у вхідних даних значно

змінює хеш, що забезпечує надійну перевірку цілісності. Незважаючи на розвиток квантових обчислень, SHA-256 залишається захищеним, адже алгоритм Гровера може знизити складність лише до 2^{128} комбінацій. Це означає, що навіть для квантових комп'ютерів така атака вимагає значних ресурсів і малоймовірна на практиці.

Для додаткові аргументи на користь надійності SHA-256 далі розпишемо вже в контексті проектуємого каналу передачі[26, 34].

Перевірка цілісності на всіх етапах передачі: У контексті нового каналу передачі даних SHA-256 використовується для генерації хешу кожного блоку, що дозволяє одержувачу підтвердити цілісність на кожному етапі передачі. Якщо хоча б один блок змінюється або модифікується, це одразу буде виявлено під час перевірки хешів, що мінімізує ризик прихованих змін.

Стійкість до атак MITM на рівні цілісності: У випадках, коли зловмисник намагається модифікувати дані під час їхньої передачі, SHA-256 забезпечує надійну перевірку, оскільки будь-яка зміна блоку або пакета даних зробить хеш недійсним. Це значно ускладнює для зловмисника можливість непомітного внесення змін.

Підбиваючи висновки, можна сказати, що SHA-256 є надійним алгоритмом для забезпечення цілісності даних під час передачі, особливо в умовах захищених каналів. Завдяки стійкості до колізій, незворотності та чутливості до змін, SHA-256 ефективно виявляє будь-які спроби модифікації даних або їх підробки[20-21, 34].

Протокол EAP-TLS є одним із найбільш надійних протоколів автентифікації, який широко застосовується для захищених з'єднань у мережах. Він базується на сертифікатах і асиметричному шифруванні, що забезпечує високий рівень захисту від підробки автентифікації та гарантує безпечний обмін ключами. Розглянемо основні аргументи на користь його надійності[20-21, 26]:

1. Використання сертифікатів X.509 для автентифікації.

У EAP-TLS автентифікація здійснюється за допомогою сертифікатів X.509, які містять унікальні криптографічні ключі (відкритий і закритий).

Сертифікати X.509 гарантують, що кожна сторона з’єднання — як клієнт, так і сервер — є автентичною та може підтвердити свою особу, не розкриваючи приватний ключ.

Складність підробки сертифікатів X.509 зумовлена тим, що їх видають авторитетні CA, які перевіряють особу заявника перед випуском сертифіката. Кожен сертифікат містить публічний і приватний ключі: публічний ключ доступний відкрито, тоді як приватний зберігається у власника сертифіката та використовується для підпису даних.

Щоб пройти автентифікацію, зловмиснику необхідно отримати або підробити приватний ключ, пов'язаний із сертифікатом, що практично неможливо через складність криптографії. Центри сертифікації підписують сертифікати своїм власним закритим ключем, і ця підпис підтверджує справжність сертифіката. Навіть якщо зловмисник має доступ до публічного ключа, він не може підробити автентифікацію без приватного ключа, підписаного CA, що забезпечує надійність автентифікації через сертифікати X.509.

2. Захищений обмін ключами на основі асиметричного шифрування.

EAP-TLS використовує асиметричне шифрування для початкового обміну ключами, що дозволяє надійно захистити процес автентифікації. Під час початкового «рукостискання» (handshake) клієнт і сервер обмінюються сертифікатами, перевіряючи їх справжність.

Асиметричне шифрування забезпечує захист від атаки MITM, оскільки зловмисник не може підмінити ключі під час рукостискання без приватного ключа. Якщо зловмисник спробує перехопити або змінити сертифікати під час рукостискання, система одразу виявить це, оскільки підпис не пройде верифікацію. Для обходу такого захисту зловмиснику потрібно отримати контроль над приватними ключами.

3. Встановлення симетричного сеансового ключа для шифрування даних сеансу.

Після успішного рукостискання та підтвердження автентичності сторін протокол EAP-TLS створює симетричний сеансовий ключ, який використовується для шифрування даних протягом поточного сеансу. Це забезпечує ефективне та швидке шифрування даних після встановлення з'єднання.

Стійкість до атак на сеансовий ключ: Навіть якщо зловмисник перехопить зашифрований трафік, він не зможе дешифрувати дані без сеансового ключа, який генерується під час рукостискання і не передається по мережі у відкритому вигляді. Підробка автентифікації або розкриття даних сеансу вимагає доступу до цього симетричного ключа, який не розкривається та унеможливлює атаку «грубої сили» в рамках одного сеансу через обмеження часу.

Завдяки використанню сертифікатів X.509, асиметричного шифрування під час рукостискання та генерації симетричного сеансового ключа, EAP-TLS є надзвичайно надійним протоколом автентифікації. Складність отримання або підробки сертифікатів, стійкість до атак MITM і використання сеансових ключів забезпечують високий рівень захисту проти несанкціонованого доступу.

Протокол IPsec з використанням ESP є потужним інструментом для забезпечення захищеної передачі даних у відкритих мережах, таких як Інтернет. Завдяки шифруванню як самого вмісту пакета, так і заголовків, IPsec із ESP приховує ключову інформацію про джерело та призначення трафіку. Ця особливість робить його одним із найбільш надійних протоколів для тунелювання та захисту даних від перехоплення і аналізу:

Шифрування вмісту та заголовків: ESP шифрує як дані пакета, так і заголовки, що містять інформацію про джерело та призначення трафіку. Завдяки цьому навіть при перехопленні зловмисник не може дізнатися відправника, одержувача або зміст без розшифрування. Шифрування заголовків також ускладнює аналіз трафіку, не дозволяючи виявити частоту чи обсяг передач між певними IP-адресами.

Алгоритм AES-256 для шифрування: На апаратних VPN-шлюзах AES-256 дозволяє забезпечувати швидке шифрування та дешифрування без істотного

навантаження на обчислювальні ресурси, що підвищує ефективність і захищеність передачі даних.

Складність атаки перехоплення в умовах багатоканальної передачі: у зпроектованій архітектурі дані розподіляються через кілька VPN-тунелів, що посилює захист. Навіть якщо зловмисник зуміє перехопити один із тунелів, він не отримає всіх блоків даних, оскільки пакети передаються випадковими шляхами. Для повного перехоплення зловмиснику необхідно контролювати всі канали одночасно, що практично неможливо в умовах багатоканальної передачі через розподілені мережеві вузли.

Об'єднання AES-256, SHA-256, EAP-TLS, та IPsec із ESP в протокол IPsec IKEv2 створює багаторівневий захист для забезпечення конфіденційності, цілісності та автентичності даних. На практиці ці механізми значно ускладнюють спроби несанкціонованого доступу до даних, перехоплення чи модифікації інформації в процесі передачі[20-21].

Узагальнюючи всю вище перелічену інформацію, можна сказати, що протокол IPsec IKEv2, який використовується для налаштування, управління та автентифікації з'єднань IPsec, є дуже складним для зламу завдяки кільком важливим аспектам[20-21, 26, 34]:

1. **Захищений обмін ключами та стійкість до MITM-атак**: IKEv2 здійснює обмін ключами через двоетапне рукостискання, під час якого сторони спочатку автентифікуються, а потім обмінюються секретами для сеансових ключів. Для автентифікації використовуються цифрові сертифікати або узгоджені ключі, що дозволяє кожній стороні перевірити підписи й хеші іншої. Це асиметричне шифрування і перевірка гарантують, що з'єднання встановлюється тільки між авторизованими сторонами, роблячи втручання зловмисників, зокрема атаки типу MITM, практично неможливими.

2. **Захист від Replay-атак**: IKEv2 захищає від повторного використання даних, застосовуючи унікальні ідентифікатори сеансів і nonce. Nonce — унікального випадкового значення, що генерується для кожної сесії. Це значення забезпечує унікальність кожного сеансу, унеможливлюючи повторне

використання перехоплених пакетів зловмисником. Завдяки nonce кожна сесія отримує свій неповторний набір даних, що критично для встановлення захищеного з'єднання. Це унеможливлює повторний доступ зловмисника до перехоплених даних, оскільки кожен сеанс має власні параметри.

3. **Динамічна ротація ключів**: IKEv2 підтримує періодичне оновлення сеансових ключів під час передачі, що ускладнює їх злам. Навіть якщо зловмисник перехопить ключ, його швидка заміна обмежує можливості дешифрування.

4. **Шифрування AES-256**: Для шифрування даних використовується AES-256, який забезпечує високий рівень захисту завдяки своїй стійкості до криптоаналітичних атак. Це дозволяє надійно захищати передані дані навіть у випадку перехоплення.

5. **Забезпечення цілісності з SHA-256**: Для перевірки цілісності кожного блоку переданих даних IKEv2 використовує SHA-256, що гарантує виявлення будь-яких змін. Завдяки хешуванню будь-яке спотворення даних під час передачі буде миттєво виявлено, забезпечуючи точність і цілісність інформації.

Невеликий приклад роз’яснення складності зламу IPsec IKEv2[20-21]:

Припустимо, зловмисник намагається перехопити сеансовий ключ, використаний у IKEv2 для встановлення IPsec-з'єднання. Навіть якщо він має доступ до мережі, складність обчислень для атак на IKEv2 залишається надзвичайно високою через комбінацію захищених процедур[20-21]:

Отримання сеансових ключів потребує розкриття обміну ключами, які були захищені асиметричним шифруванням. Навіть якщо зловмисник перехопить повідомлення під час обміну, вони залишаться недоступними без приватних ключів сторін.

Спроба повторного використання пакетів не спрацює через унікальні nonce та ідентифікатори, що генеруються для кожного сеансу.

Спроба атаки MITM ускладнена, адже кожна сторона має підтвердити автентичність іншої, використовуючи перевірені сертифікати або ключі, що робить маніпуляцію з повідомленнями неможливою без переривання з'єднання.

Завдяки багатоступеневому рукостисканню, захисту від повторного використання, підтримці динамічного оновлення ключів, IPsec IKEv2 є одним із найбільш захищених протоколів тунелювання для передачі даних. Ці особливості роблять його стійким до сучасних атак і забезпечують високий рівень надійності при створенні безпечних каналів у відкритих мережах[20-21, 26].

3.3.3 Оцінка ефективності методів захисту від несанкціонованого доступу

У цьому підрозділі розглядається оцінка ефективності методів захисту від несанкціонованого доступу, реалізованих у проектованому закритому каналі передачі даних. Основна увага приділяється тестуванню таких компонентів, як автентифікація через сертифікати X.509, захист від атак MITM та Replay-атак. Використання сучасних криптографічних протоколів і багаторівневої перевірки автентичності дозволяє забезпечити надійний рівень захищеності для різних умов застосування[37-38].

Тест на ефективність автентифікації з сертифікатами X.509

Дослідження автентифікації через сертифікати X.509: У звітах від NIST та IEEE(Інститут інженерів з електротехніки і електроніки) підтверджується, що сертифікати X.509 є основним інструментом автентифікації у багатьох сучасних системах через свою надійність. Такі сертифікати генеруються сертифікаційними CA з криптографічно захищеними підписами, що робить їх підробку практично неможливою без компрометації приватних ключів CA.

Виходячи з наукових звітів, можна прогнозувати, що система відхилить будь-які спроби підключення з підробленими сертифікатами. За даними досліджень, ймовірність успішної атаки з підробленим сертифікатом мінімальна, оскільки для цього потрібно мати доступ до приватного ключа CA[24, 37-39].

Мета тесту: Перевірити, чи система успішно відхиляє спроби несанкціонованого підключення за допомогою підроблених або недійсних сертифікатів.

Компоненти:

- Клієнт і сервер з підтримкою EAP-TLS.

- RADIUS(Remote Authentication Dial-in User Service)-сервер для обробки запитів автентифікації і підтвердження сертифікатів.

- Wireshark для аналізу трафіку, особливо для відстеження обміну сертифікатами.

Процес тестування[32-33, 37-39]:

1. Налаштування сертифікатів: Для клієнта і сервера видаються сертифікати X.509 на основі довіреного CA. Сервер автентифікації налаштовується на прийом запитів EAP-TLS і перевірку цих сертифікатів.

2. Підключення клієнта до сервера через RADIUS: Клієнт ініціює з’єднання із сервером через RADIUS-сервер, який запускає процес автентифікації.

3. Захоплення трафіку: Wireshark використовується для захоплення трафіку, що дозволяє побачити обмін сертифікатами та процес підтвердження автентичності.

4. Аналіз результатів: Очікується, що система дозволить з’єднання, якщо сертифікати справжні, і відхилить підключення, якщо вони не відповідають очікуваному CA.

Проходження тесту з дійсним сертифікатом: З'єднання успішно встановлюється, оскільки сертифікат був виданий надійним CA і підтверджується системою.

Спроба з підробленим сертифікатом: Буде відхилено через відсутність відповідної цифрової підпису CA або невідповідність сертифіката з базою довірених центрів сертифікації.

Реакція системи на підроблений сертифікат: Автоматичне блокування спроби підключення і запис відповідного попередження в журналі подій для подальшого аналізу.

Висновок: Система повинна надійно відкидати всі спроби автентифікації з недійсними або підробленими сертифікатами, що підтверджує надійність автентифікації через EAP-TLS.

Виходячи з наукових звітів, можна прогнозувати, що система відхилить будь-які спроби підключення з підробленими сертифікатами. За даними досліджень, ймовірність успішної атаки з підробленим сертифікатом мінімальна, оскільки для цього потрібно мати доступ до приватного ключа CA.

Для класичної обчислювальної потужності, яка є в розпорядженні атакувальників сьогодні, злом 2048-бітного ключа CA займає мільярди років на найпотужніших комп'ютерах сучасності. Це можна виразити такою оцінкою: менше ніж 1 з 10^{30}, що практично дорівнює нулю[32-33, 37-39].

Тест на обмін ключами

У дослідженнях протоколу EAP-TLS, зокрема у звітах ENISA(Європейське агентство з мережевої та інформаційної безпеки), зазначається, що протокол забезпечує надійний захист під час обміну ключами завдяки асиметричному шифруванню. Обмін сертифікатами із застосуванням асиметричного шифрування гарантує, що зловмисник не зможе отримати доступ до ключів без компрометації приватного ключа.

Згідно з дослідженнями, ймовірність успішного перехоплення ключа без доступу до приватних ключів автентифікованих сторін є вкрай низькою. Асиметричне шифрування захищає дані протягом усього процесу обміну, що підтверджує надійність EAP-TLS у забезпеченні захищеного обміну ключами.

В реальних умовах ймовірність перехоплення або успішної атаки на обмін ключами без доступу до приватних ключів сторін настільки мала, що її можна оцінити як меншу за 10^{-30}на основі поточної обчислювальної складності та криптостійкості.

Мета тесту: Перевірити, наскільки надійно і безпечно EAP-TLS виконує обмін ключами між клієнтом і сервером, не дозволяючи стороннім особам отримати доступ до ключів або даних сеансу[32-33, 40].

Компоненти:

- Клієнт і сервер з підтримкою EAP-TLS і сертифікатами X.509.
- RADIUS-сервер для автентифікації.
- Wireshark для моніторингу та аналізу процесу обміну ключами.

Процес тестування[32-33, 37-38, 40]:

1. Запуск сеансу: Клієнт і сервер встановлюють новий сеанс через RADIUS-сервер.

2. Захоплення процесу обміну ключами: Інструмент Wireshark використовується для фіксації процесу обміну ключами, зокрема передачі сертифікатів і підтвердження автентичності.

3. Перевірка секретності ключів: Переконатися, що ключі не передаються у відкритому вигляді. Зловмисники не повинні мати змоги отримати ключі без доступу до приватних ключів.

4. Аналіз завершення сеансу: Система повинна успішно завершити автентифікацію і обмін ключами, не допускаючи розголошення сеансових ключів.

Безпечний обмін ключами між клієнтом і сервером: Під час початкового рукостискання клієнт і сервер обмінюються сертифікатами, щоб підтвердити автентичність. Потім генерується унікальний сеансовий ключ для поточного з'єднання. Очікується, що цей ключ буде доступний тільки автентифікованим сторонам і не передаватиметься у відкритому вигляді.

Спроба перехоплення ключів сторонніми особами: Заблоковано через те, що обмін ключами захищений асиметричним шифруванням. Навіть якщо зловмисник перехопить повідомлення під час рукостискання, ключі залишаться недоступними без доступу до приватних ключів обох сторін.

Реакція на спробу отримати ключі: Будь-які спроби доступу до ключів, які не були автентифіковані, автоматично відхилені системою.

Висновок: Система забезпечує надійний і безпечний обмін ключами між сторонами, не допускаючи сторонніх осіб до отримання ключів. Цей тест підтверджує ефективність EAP-TLS для захисту даних під час автентифікації[32-33, 37-38, 40].

Тест на стійкість до атак MITM

За результатами досліджень, проведених у ACM Journal of Cryptographic Engineering, EAP-TLS забезпечує стійкість до MITM-атак за рахунок верифікації

сертифікатів і використання криптографічного захисту під час обміну ключами. Автентифікація сторін через X.509 робить спроби підміни сертифіката зловмисником малоймовірними, оскільки відсутність валідного сертифіката CA автоматично призведе до відхилення з’єднання.

Результати досліджень показують, що EAP-TLS має високу стійкість до MITM-атак. У проектуємому закритому каналі спроби MITM-атаки повинні автоматично блокуватися, оскільки система повинна виявити будь-які розбіжності в сертифікатах під час верифікації[32-33, 37, 41].

Мета тесту: Оцінити, наскільки EAP-TLS здатний захистити з'єднання від атак MITM, коли зловмисник намагається перехопити, змінити дані під час обміну сертифікатами та ключами.

Компоненти:

- Клієнт і сервер з підтримкою EAP-TLS і сертифікатами X.509.

- RADIUS-сервер для підтвердження автентифікації.

- Bettercap для симуляції MITM-атаки.

- Wireshark для моніторингу мережевого трафіку та фіксації будь-якого втручання.

Процес тестування[32-33, 37, 41]:

1. Підключення зловмисника: Зловмисник намагається втрутитися у з’єднання між клієнтом і сервером, використовуючи Bettercap для MITM-атаки.

2. Аналіз обміну сертифікатами: Wireshark фіксує обмін сертифікатами, що дозволяє перевірити, чи виявить система підміну сертифіката або спроби модифікації даних.

3. Перевірка реакції системи: Система повинна автоматично виявити і заблокувати підміну сертифіката. Автентифікація EAP-TLS базується на криптографічному підтвердженні сертифікатів, тому будь-яка фальшива інформація повинна викликати розрив з'єднання.

4. Аналіз логів подій: Переконатися, що в системі записані всі спроби втручання в журнали подій для подальшого аналізу.

Атака з підробленим сертифікатом MITM: Система виявляє спробу MITM-атаки, якщо зловмисник втручається в процес обміну сертифікатами. Автентифікація за допомогою EAP-TLS передбачає перевірку сертифікатів обох сторін, і будь-який підроблений сертифікат без дійсного цифрового підпису CA буде відхилено.

Перевірка цілісності сертифікатів: EAP-TLS використовує хеш-функції та цифрові підписи для підтвердження цілісності і справжності сертифікатів. Коли зловмисник пробує змінити дані або підробити підпис, система виявляє розбіжність і не встановлює з'єднання.

Реакція системи на атаку MITM: Спроба перехоплення або зміни даних під час з'єднання зафіксована в журналі подій, а з'єднання припинене.

Висновок: Система відхиляє всі спроби MITM-атаки та гарантує цілісність і справжність з'єднання, що підтверджує високу надійність EAP-TLS у запобіганні MITM-атакам[32-33, 37, 41].

Захист від повторного використання сеансових даних (Replay Attacks)

Дослідження, зокрема звіти OWASP(Відкритий проект з безпеки вебзастосунків), підтверджують, що використання унікальних ідентифікаторів сесії (nonce) і одноразових чисел робить EAP-TLS ефективним проти Replay-атак. Кожен сеанс у EAP-TLS є унікальним завдяки одноразовим ідентифікаторам, що унеможливлює повторне використання перехоплених даних.

На основі досліджень очікується, що система зможе успішно виявити й заблокувати всі спроби Replay-атак, оскільки кожне з'єднання має власний сеансовий ідентифікатор, який не допускає повторне використання старих даних.

Мета тесту: Перевірити, чи здатен EAP-TLS захистити сеанс від атак повторного використання, коли зловмисник намагається відтворити або повторно використовувати перехоплені дані для несанкціонованого доступу [32-33, 37, 42].

Компоненти:

- Клієнт і сервер з підтримкою EAP-TLS і сертифікатами X.509.

- Scapy для генерації повторюваних пакетів на основі перехопленого трафіку.

- Wireshark для моніторингу і аналізу трафіку під час атаки.

Процес тестування [32-33, 37, 42]:

1. Перехоплення легітимного трафіку: Клієнт і сервер встановлюють з’єднання, і Wireshark використовується для захоплення цього трафіку.

2. Створення Replay атаки: Scapy налаштовується для відтворення перехоплених пакетів, щоб симулювати Replay атаку.

3. Перевірка унікальних ідентифікаторів сесії: Кожне з'єднання в EAP-TLS має мати унікальні ідентифікатори і одноразові числа (nonce), що забезпечує захист від повторного використання перехоплених даних. Система повинна виявити, що відправлені пакети не відповідають поточному сеансу.

4. Аналіз реакції системи: Очікується, що система автоматично заблокує пакети Replay атаки, оскільки вони не відповідатимуть унікальним сеансовим ідентифікаторам.

Захист від повторного використання даних: EAP-TLS блокує будь-які спроби повторного використання даних завдяки унікальним сеансовим ідентифікаторам та випадковим nonce. Кожне з'єднання генерує новий сеансовий ключ, і зловмисник не зможе повторити попередній сеанс.

Реакція на спробу Replay-атаки: Якщо зловмисник спробує відтворити перехоплені пакети, система розпізнає їх як недійсні, оскільки вони не відповідають унікальним параметрам поточного сеансу. Система автоматично відхиляє всі пакети, які не відповідають унікальному сеансовому ідентифікатору або nonce.

Логування подій: Будь-яка невдала спроба повторного використання даних записується в журналі подій.

Висновок: Завдяки використанню сеансових ідентифікаторів та випадкових чисел, EAP-TLS захисщає з'єднання від повторного використання даних, що підтверджує надійність цього протоколу для захисту від Replay-атак.

Результати оцінки показали високу ефективність методів захисту, зокрема автентифікації на основі сертифікатів X.509, які практично виключають можливість підробки сертифікатів. Також протокол EAP-TLS успішно блокує спроби Replay-атак завдяки унікальним сеансовим ідентифікаторам, а криптографічний захист IPsec IKEv2 забезпечує стійкість до атак MITM. Усі ці аспекти підтверджують, що проектований канал є надійним рішенням для захисту даних у середовищах із підвищеними ризиками несанкціонованого доступу [32-33, 37, 42].

3.3.4 Моделювання ризиків

Щоб зрозуміти, за яких обставин найкраще використовувати певний закритий канал передачі, потрібно знати не лише його сильні сторони, але й слабкі. З цією метою було проведено дослідження з моделювання ризиків для виявлення потенційних вразливостей у проектованому закритому каналі захисту інформації, що використовує модифіковану VPN-архітектуру з багатоканальним підходом. Можна виділити такі найбільш ризикові аспекти [18, 37-38]:

1. Атаки типу MITM

Опис: Атаки MITM можуть виникати на етапах встановлення з’єднання між кінцевими точками каналу, коли відбувається обмін ключами. Навіть з криптографічними протоколами (EAP-TLS, IPsec IKEv2), існує ризик, що зловмисник може перехопити цей процес.

Чому це небезпечно: Ця атака дозволяє зловмиснику перехоплювати трафік у режимі реального часу, підміняти його або втручатися в комунікацію.

Ймовірність реалізації: Середня. Для успіху зловмисник має отримати доступ до одного з маршрутизаторів на яких і відбувається шифрування і дешифрування даних, що потребує доступу до самого маршрутизатора або зловмиснику потрібно буде моніторити велику частину мережі, щоб знайти всі канали.

2. Витік даних через сторонні канали (англ. Side-Channel Attacks)

Опис: Апаратні VPN-шлюзи можуть бути вразливі до атак сторонніх каналів, які використовують витоки фізичних характеристик шифрування (наприклад, енергоспоживання).

Чому це небезпечно: Цей тип атак здатний надати зловмиснику доступ до криптографічних ключів, що значно спрощує подальший злом.

Ймовірність реалізації: Низька. Атака потребує фізичного доступу до VPN-шлюзів або спеціального обладнання для перехоплення фізичних сигналів і специфічних навичок.

3. Перевантаження VPN-шлюзів (DoS-атаки)

Опис: Використання декількох VPN-тунелів та апаратного шифрування створює додаткове навантаження на шлюзи. Зловмисник може скористатися цим для проведення DoS-атаки, спрямованої на перевантаження шлюзів.

Чому це небезпечно: У випадку успішної атаки продуктивність каналу різко падає або припиняється, що впливає на стабільність і доступність.

Ймовірність реалізації: Середня. Для реалізації DoS-атаки потрібно відправити великий обсяг запитів на шлюзи, що підвищує ймовірність атаки в умовах високого мережевого трафіку.

4. Компрометація сесійних ключів

Опис: Якщо зловмисник зможе перехопити і дешифрувати сесійні ключі, це дозволить йому відновити структуру тунелів і отримати доступ до переданих даних.

Чому це небезпечно: У разі компрометації ключів зловмисник може перехоплювати, підміняти та аналізувати трафік, що значно знижує рівень захищеності каналу.

Ймовірність реалізації: Низька. Реалізація вимагає спеціального обладнання та знань.

5. Атака на кінцеві точки (Джерело даних і Отримувач даних)

Опис: Джерело даних і Отримувач є кінцевими точками, які можуть бути вразливими до атак через їхній безпосередній зв’язок із системою. Зловмисник

може отримати доступ до кінцевих точок, наприклад, через шкідливе ПЗ (malware) або фішингові атаки.

Чому це небезпечно: Компрометація кінцевої точки дозволяє зловмиснику не тільки перехоплювати або маніпулювати даними, але й отримати повний контроль над з'єднанням, оскільки він може обійти шифрування.

Ймовірність реалізації: Середня. Для успішної атаки зловмиснику необхідно інфікувати кінцевий пристрій шкідливим ПЗ або скомпрометувати його фізично, що можливе при недостатньому захисті пристрою, але це загальна вразливість всіх закритих каналів.

Проведення моделювання ризиків дозволяє виявити критичні точки системи та створити запобіжні механізми, які зменшать ймовірність реалізації основних загроз. Пріоритизація заходів безпеки допоможе сконцентрувати ресурси на найбільш ризикованих ділянках каналу, що дозволить зменшити потенційні втрати від несанкціонованого доступу або перебоїв у роботі системи [18, 37-38].

3.3.5 Аналіз продуктивності

Для застосування методу аналізу продуктивності до проектуємого закритого каналу передачі даних, побудованого на базі VPN з використанням AES-256 та багатоканальної архітектури, варто врахувати такі аспекти: швидкість передачі/пропускну здатність, затримка (latency) і вплив криптографічних технологій на продуктивність. Нижче описано основні очікування щодо результатів продуктивності для кожного показника, включаючи розрахунок для різних сценаріїв навантаження [35, 32-33].

1. Швидкість передачі даних/Пропускна здатність [35, 32-33]:

Максимальна швидкість передачі даних: Максимальна пропускна здатність кожного каналу передачі даних за ідеальних умов складає 1 Гбіт/с, що відповідає 125 МБ/с. Таким чином, у разі відсутності накладних витрат на шифрування, маршрутизацію, а також додаткових метаданих, теоретична швидкість передачі даних через один канал могла б досягати 125 МБ/с.

Оптимальна швидкість передачі даних: Зважаючи на архітектуру з кількома паралельними VPN-тунелями, а також на накладні витрати, спричинені криптографічним шифруванням (алгоритм AES-256) і додатковою передачею метаданих, реальна ефективна швидкість каналу буде меншою. За даними з файлу та попередніми дослідженнями, накладні витрати на шифрування та метадані становлять близько 10-20% від загальної пропускної здатності. Таким чином, оптимальна швидкість передачі даних складатиме приблизно 100-112.5 МБ/с.

Можлива швидкість передачі даних в умовах навантаження: За умов високого навантаження на VPN-шлюзи, наприклад, через одночасну обробку великих обсягів даних або підвищення кількості з'єднань, швидкість передачі може знижуватись через обмеження апаратних ресурсів. Для таких умов продуктивність може бути знижена до 50–60% від оптимальної, що становить приблизно 53–67.2 МБ/с.

Ці дані відображають актуальний потенціал продуктивності, враховуючи як архітектурні особливості каналу, так і навантаження на систему шифрування і обробку даних.

2. Затримка (latency) [31, 35, 32-33]:

Затримка перед повторною передачею: Оскільки таймаут для повторного запиту базується на часі проходження сигналу (RTT) з урахуванням VPN, застосовується наступний підхід. RTT з VPN у середніх умовах становить від 40 до 250 мс, що враховує **Базову затримку в мережі (30-200 мс)** і **Додаткові витрати VPN (10-50 мс).**

Затримка перед повторною передачею для повторного запиту визначається на основі RTT з урахуванням VPN. Для забезпечення надійності передачі рекомендований таймаут для повторного запиту встановлюється як подвійний RTT, тобто:

Звичайні умови: якщо мережа стабільна і затримки відносно низькі, оптимальний таймаут для повторного запиту становить від 80 до 500 мс, залежно від середньої RTT (затримки передачі сигналу в обидва боки).

Глобальні мережі з високою затримкою: якщо передача відбувається на великі відстані або через насичені мережі (наприклад, з'єднання між континентами), таймаут рекомендується збільшити до 800 мс і більше, щоб компенсувати вищу затримку RTT.

Такий підхід до вибору часу очікування допомагає зменшити навантаження на канал, запобігаючи надмірним повторним запитам.

Таким чином, **час очікування для повторної передачі** в середньому варіюється від 80 до 500 мс, а для глобальних мереж із високою затримкою може сягати 800 мс і більше.

3. Вплив криптографії на продуктивність [30, 35, 32-34]:

У запропонованому закритому каналі застосовуються шифрування AES-256 для конфіденційності та SHA-256 для перевірки цілісності даних. Вплив цих криптографічних алгоритмів на продуктивність залежить від обсягу та інтенсивності передачі даних:

1. **Навантаження на систему**: За великих обсягів даних шифрування та хешування можуть знижувати продуктивність системи на 10–20%. Це пов’язано з необхідністю обробки кожного блоку через AES-256 для шифрування та SHA-256 для створення хешів, що потребує додаткових обчислень і часу.

2. **Додаткові затримки**: Під час інтенсивної передачі даних (наприклад, при обробці великих файлів або передачі в реальному часі) шифрування і хешування можуть додати 2–5 мс затримки для кожного тунелю. Це значення враховує навантаження на VPN-шлюзи, особливо за підвищеної активності.

Завдяки ефективності апаратного шифрування та багатоканальній архітектурі новий канал зберігає баланс між безпекою та швидкістю передачі, знижуючи вплив криптографії на загальну продуктивність.

Згідно з розрахунками, запропонована архітектура забезпечить ефективний баланс між захищеністю даних та продуктивністю. Багатоканальна система дозволить підтримувати швидкість передачі на рівні, близькому до максимальної, а затримка залишатиметься в межах прийнятних значень для критично важливих застосувань.

3.4 Висновок до третього розділу

Розроблений закритий канал передачі даних ґрунтується на використанні VPN-технологій з покращеною багатоканальною архітектурою, яка посилює захист інформації через розподіл трафіку на кілька незалежних каналів. Кожен блок даних шифрується окремо за допомогою AES-256, що забезпечує високу конфіденційність, а контроль цілісності даних здійснюється через хеш-алгоритм SHA-256. Такий підхід ускладнює перехоплення, оскільки кожен канал передає тільки частину інформації, що зменшує ймовірність повного відновлення даних стороннім спостерігачем.

До основних переваг каналу належать високий рівень безпеки, забезпечений багатоканальним шифруванням, стійкість до відмов завдяки розподілу блоків між каналами, а також надійна автентифікація користувачів через EAP-TLS та IPsec IKEv2. Завдяки використанню апаратних VPN-шлюзів знижується затримка при обробці даних, що підвищує продуктивність системи. Слабкою стороною каналу є складність налаштування, підтримки та необхідність значних ресурсів для одночасної роботи кількох тунелів.

Розроблений канал передачі даних, досліджений за допомогою різноманітних методів, показав високу ефективність для корпоративних середовищ з критичними вимогами до безпеки та цілісності даних. Багатоканальна архітектура та шифрування на основі AES-256 забезпечують стійкість до перехоплення, підвищуючи конфіденційність і надійність передачі даних через публічні мережі.

Водночас канал є надмірним для середовищ із низькими вимогами до захисту, таких як телекомунікаційні послуги в громадських місцях або компанії, що обробляють неконфіденційні дані. Для таких випадків звичайний VPN з одним тунелем є простішим і більш економічним рішенням, що достатньо відповідає їхнім потребам.

Також проектований канал є недоцільним для середовищ з обмеженою інфраструктурою або нестабільним зв’язком, де підтримка паралельних тунелів

ускладнена. Отже, оптимальна сфера його застосування — це корпоративні та урядові мережі, де важливий комплексний захист даних на всіх етапах передачі.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було вирішено наступні завдання:

1. проведено аналіз понять та визначень, які формулюють сутність закритих ліній передачі даних;
2. класифіковано основні види закритих ліній передачі даних, визначено їхні технологічні характеристики;
3. досліджено сучасні методи шифрування даних, зокрема AES, RSA, ECC, а також криптографічні протоколи SSL/TLS, IPsec;
4. оцінено вплив основних кіберзагроз та розглянуто можливості забезпечення захисту інформації в закритих каналах зв’язку;
5. проведено моделювання роботи закритої лінії передачі даних та створено новий канал передачі даних на основі існуючих технологій.

У першому розділі кваліфікаційної роботи розглянуто поняття закритих ліній передачі даних, їхні ключові характеристики та класифікацію. Було досліджено основні види закритих ліній передачі даних, а також їхні особливості. Окремо проаналізовано будову закритого каналу передачі даних і більш детально розглянуто конструктивні елементи кожного з раніше зазначених каналів.

У другому розділі досліджено сучасні методи шифрування, зокрема симетричні (AES) та асиметричні (RSA, ECC) алгоритми, а також їх поєднання для підвищення ефективності захисту даних. Розглянуто криптографічні протоколи (SSL/TLS, IPsec), які забезпечують захист інформації на різних рівнях передачі. Проведено аналіз загроз, таких як атаки «людина посередині», перехоплення даних, компрометація ключів, і визначено основні підходи до їх мінімізації.

У третьому розділі було висунуто ідею створення нового закритого каналу передачі даних, описано його будову та досліджено ефективність запропонованого рішення за допомогою математичного моделювання, симуляційного аналізу та оцінки захищеності від можливих кіберзагроз.

Проведені дослідження підтвердили доцільність використання запропонованого каналу для забезпечення високого рівня безпеки даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. Luciano, D., Прічетт, Г. Криптологія: від шифрів Цезаря до криптосистем із відкритим ключем // Математичний журнал коледжу. – 1987. – Січень.
2. Конрад, Е., Фельдман, Дж. Навчальний посібник CISSP. – 2-ге вид. – 2012.
3. Stallings, W. Cryptography and Network Security: Principles and Practice.
4. Kibbler, J. C. A History of Communication Technology. – 2008. *Альтернатива:* Loubere, P. A History of Communication Technology.
5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
6. Cybersecurity: Critical for All Organizations Large and Small: [Електронний ресурс]. IFAC – Режим доступу до ресурсу: https://www.ifac.org/knowledge-gateway/discussion/cybersecurity-critical-all-organizations-large-and-small.
7. Detecting Disruption in Closed Systems: [Електронний ресурс]. Atlantic Council – Режим доступу до ресурсу: https://www.atlanticcouncil.org/in-depth-research-reports/report/detecting-disruption-in-closed-systems/.
8. The Difference Between AES and RSA: [Електронний ресурс]. Cryptomathic – Режим доступу до ресурсу: https://www.cryptomathic.com/news-events/blog/the-difference-between-aes-and-rsa.
9. Palais, J. C. Fiber Optic Communications.
10. Rescorla, E. SSL and TLS: Designing and Building Secure Systems.
11. Snader, J. C. VPNs Illustrated: Tunnels, VPNs, and IPsec.
12. Maral, G., Bousquet, M. Satellite Communications Systems: Systems, Techniques and Technology.
13. Schiller, J. Mobile Communications.
14. Azure VPN Gateway vs ExpressRoute: Quick Comparison: [Електронний ресурс]. Microsoft Tech Community – Режим доступу до ресурсу: https://techcommunity.microsoft.com/t5/fasttrack-for-azure/azure-vpn-gateway-vs-expressroute-quick-comparison/ba-p/3725670.
15. VPN Hardware: [Електронний ресурс]. NordVPN – Режим доступу до ресурсу: https://nordvpn.com/blog/vpn-hardware/.
16. Bandwidth vs Data Rate: [Електронний ресурс]. Cloudwards – Режим доступу до ресурсу: https://www.cloudwards.net/bandwidth-vs-data-rate/.
17. IEEE Document 8466376: [Електронний ресурс]. IEEE Xplore – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8466376.
18. Stallings, W. Data and Computer Communications. – 2017.
19. NIST Special Publication 800-77. Guide to IPsec VPNs.

20. RFC 4301: Security Architecture for the Internet Protocol (IPsec).
21. RFC 5246: Transport Layer Security (TLS) Protocol Version 1.2.
22. ITU-T Recommendation G.709: Optical Transport Network (OTN).
23. 3GPP TS 33.501. Security Architecture and Procedures for 5G System (Release 16).
24. National Institute of Standards and Technology (NIST). Guide to Access Control (SP 800-162).
25. Quantum Information Processing: [Електронний ресурс]. ArXiv – Режим доступу до ресурсу: https://arxiv.org/abs/quant-ph/0101098.
26. Paar, C., Pelzl, J. Understanding Cryptography: A Textbook for Students and Practitioners. – ISBN: 978-3642041006.
27. Marvell Security Solutions: [Електронний ресурс]. – Режим доступу до ресурсу: https://www.marvell.com/products/security-solutions/nitrox-v.html.
28. A Brief History of Data Communications: [Електронний ресурс]. Incognito – Режим доступу до ресурсу: https://www.incognito.com/blog/brief-history-data-communications.
29. Tanenbaum, A. S., Wetherall, D. J. Computer Networking. – 2019.
30. Schneier, B. Cryptography and Network Security: Principles and Practice. – Pearson, 2015.
31. RFC 6298: Computing TCP's Retransmission Timer.
32. Kurose, J. F., Ross, K. W. Computer Networking: A Top-Down Approach. – Pearson, 2020.
33. Stallings, W. Network Security Essentials: Applications and Standards.
34. Eastlake, D., Hansen, T. US Secure Hash Algorithm 2 (SHA-2): [Електронний ресурс]. Internet Engineering Task Force (IETF), RFC 6234. – Режим доступу до ресурсу: https://www.rfc-editor.org/info/rfc6234.
35. IEEE 802.1X. Standard for Port-Based Network Access Control.
36. Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. Handbook of Applied Cryptography. – 1996.
37. Practical Risk Modeling in Cybersecurity // SANS Institute.
38. Risk Management Framework (RMF) Guidelines // NIST.
39. NIST Special Publication 800-52.
40. Algorithms, Key Size and Parameters: [Електронний ресурс]. ENISA – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014.
41. EAP-TLS Wireless Infrastructure: [Електронний ресурс]. Versprite – Режим доступу до ресурсу: https://versprite.com/blog/eap-tls-wireless-infrastructure/.

42. Identification and Authentication Failures: [Електронний ресурс]. OWASP – Режим доступу до ресурсу: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/.

43. Кулініч С.Р., Пепа Ю.В. Роль шифрування в забезпеченні безпеки закритих ліній передачі даних // Тези доповідей Всеукраїнської науково-практичної конференції «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем». – Київ: ДУІКТ, 2024. – С. 2.

ДОДАТКИ

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

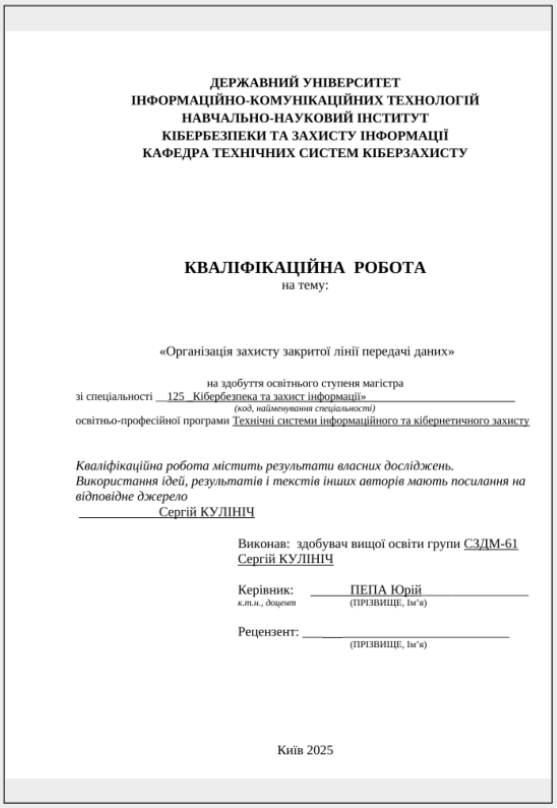
Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

ОРГАНІЗАЦІЯ ЗАХИСТУ ЗАКРИТОЇ ЛІНІЇ ПЕРЕДАЧІ ДАНИХ

Спеціальність: 125 - Кібербезпека та захист інформації
Виконав: Сергій КУЛІНІЧ
Керівник: к.т.н., доцент Юрій ПЕПА

Київ - 2025

АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ РОБОТИ



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

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

«Організація захисту закритої лінії передачі даних»

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
Сергій КУЛІНІЧ

Виконав: здобувач вищої освіти групи СЗДМ-61
Сергій КУЛІНІЧ

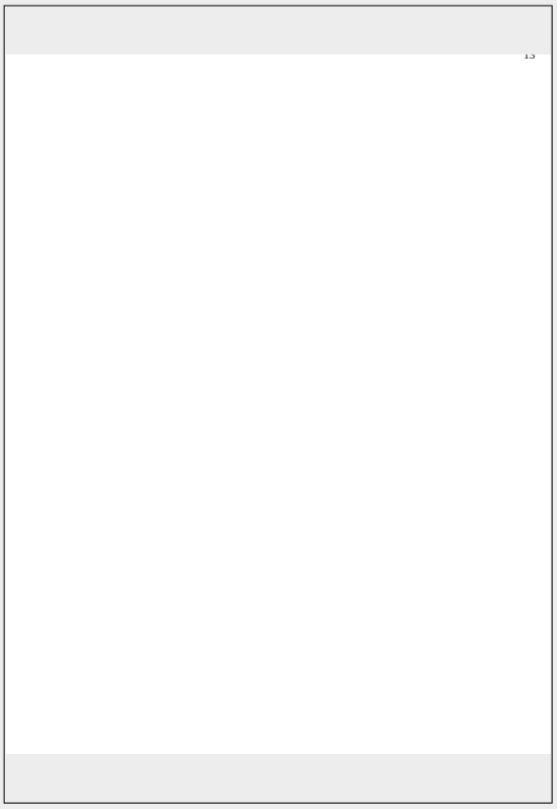
Керівник: ПЕПА Юрій
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

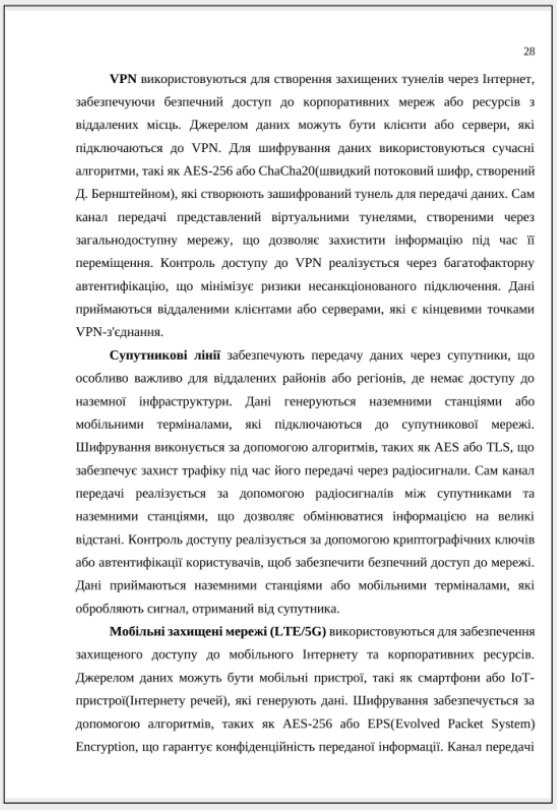
- Актуальність теми визначається зростанням обсягів передавання даних і появою нових кіберзагроз для каналів зв’язку.
- Мета роботи - дослідження, розробка та оцінка ефективних методів побудови й використання закритих ліній передачі даних.
- Основні завдання: аналіз видів закритих ліній; дослідження AES, RSA, ECC, SSL/TLS, IPsec; розробка захищеного каналу на основі VPN-технологій.

ПОНЯТТЯ ЗАКРИТОЇ ЛІНІЇ ПЕРЕДАЧІ ДАНИХ



- Закрита лінія передачі даних розглядається як захищений канал зв’язку для передавання інформації між обмеженою кількістю користувачів.
- Ключові властивості: конфіденційність, цілісність, автентифікація сторін та контроль доступу.
- Для захисту застосовуються фізична ізоляція каналів, криптографічні протоколи, VPN-тунелі та механізми перевірки доступу.

КЛАСИФІКАЦІЯ ЗАКРИТИХ ЛІНІЙ ПЕРЕДАЧІ ДАНИХ



28

VPN використовуються для створення захищених тунелів через Інтернет, забезпечуючи безпечний доступ до корпоративних мереж або ресурсів з віддалених місць. Джерелом даних можуть бути клієнти або сервери, які підключаються до VPN. Для шифрування даних використовуються сучасні алгоритми, такі як AES-256 або ChaCha20(швидкий потоковий шифр, створений Д. Бернштейном), які створюють зашифрований тунель для передачі даних. Сам канал передачі представлений віртуальними тунелями, створеними через загальнодоступну мережу, що дозволяє захистити інформацію під час її переміщення. Контроль доступу до VPN реалізується через багатофакторну автентифікацію, що мінімізує ризики несанкціонованого підключення. Дані приймаються віддаленими клієнтами або серверами, які є кінцевими точками VPN-з'єднання.

Супутникові лінії забезпечують передачу даних через супутники, що особливо важливо для віддалених районів або регіонів, де немає доступу до наземної інфраструктури. Дані генеруються наземними станціями або мобільними терміналами, які підключаються до супутникової мережі. Шифрування виконується за допомогою алгоритмів, таких як AES або TLS, що забезпечує захист трафіку під час його передачі через радіосигнали. Сам канал передачі реалізується за допомогою радіосигналів між супутниками та наземними станціями, що дозволяє обмінюватися інформацією на великі відстані. Контроль доступу реалізується за допомогою криптографічних ключів або автентифікації користувачів, щоб забезпечити безпечний доступ до мережі. Дані приймаються наземними станціями або мобільними терміналами, які обробляють сигнал, отриманий від супутника.

Мобільні захищені мережі (LTE/5G) використовуються для забезпечення захищеного доступу до мобільного Інтернету та корпоративних ресурсів. Джерелом даних можуть бути мобільні пристрої, такі як смартфони або IoT-пристрої(Інтернету речей), які генерують дані. Шифрування забезпечується за допомогою алгоритмів, таких як AES-256 або EPS(Evolved Packet System) Encryption, що гарантує конфіденційність переданої інформації. Канал передачі

- Фізичні захищені лінії: оптоволоконні кабелі та виділені канали з обмеженим фізичним доступом.
- Віртуальні захищені канали: VPN, TLS/SSL, IPsec та інші протоколи шифрування трафіку.
- Спеціалізовані середовища: супутникові захищені лінії, мобільні мережі LTE/5G та рішення з квантовим розподілом ключів.

УЗАГАЛЬНЕНА БУДОВА ЗАКРИТОГО КАНАЛУ ПЕРЕДАЧІ ДАНИХ

30

мережі (LTE/5G)	пристрої	Encryption	мережі	SIM-карти	сервери

Рисунок 1.1 — Узагальнена схема будову закритого каналу передачі даних.

Кожен вид каналу передачі має свою специфіку в забезпеченні безпеки, що робить його більш ефективним для певних задач і умов використання[8-13].

1.4 Висновок до першого розділу

У першому розділі було здійснено детальний аналіз концепції закритих ліній передачі даних, які сьогодні є важливим елементом інформаційної безпеки для організацій різних рівнів. Закриті лінії передачі даних визначаються як спеціально розроблені канали зв'язку, що забезпечують захищену та конфіденційну передачу даних між двома або більше сторонами. Вони

- Типовий канал містить джерело даних, засіб шифрування, фізичне або віртуальне середовище передачі, контроль доступу та отримувача.
- Для підвищення захисту поєднуються криптографічний, організаційний і технічний рівні безпеки.
- Вибір структури каналу залежить від критичності даних, допустимої затримки, вартості та вимог до доступності.

МЕТОДИ ШИФРУВАННЯ У ЗАКРИТИХ ЛІНІЯХ ЗВ’ЯЗКУ

34

У фізично захищених лініях шифрування виконує допоміжну роль, адже безпека забезпечується фізичним захистом. Тому симетричні алгоритми шифрування, такі як AES, часто є оптимальним вибором, оскільки вони забезпечують високу швидкість шифрування і дешифрування[18].

У лініях з шифруванням даних, де безпека є головним пріоритетом, зазвичай використовують як симетричні, так і асиметричні алгоритми. В лініях з шифруванням даних, де безпека є критично важливою, комбінують асиметричні (RSA, ECC) для обміну ключами та симетричні (AES) для шифрування, що дозволяє досягти балансу між швидкістю та захистом.

У VPN-з'єднаннях використовуються обидва типи шифрування. Під час ініціалізації з'єднання асиметричне шифрування (RSA або ECC) використовується для захищеного обміну ключами, а симетричне шифрування (AES) застосовується для передачі даних після встановлення захищеного каналу. Це дозволяє забезпечити високу продуктивність та безпеку.

У супутникових захищених лініях передачі також застосовуються симетричні та асиметричні алгоритми. Супутниковий зв'язок через високу вразливість до перехоплення використовує симетричні алгоритми (AES) для шифрування даних і асиметричні для обміну ключами, гарантучи конфіденційність[26].

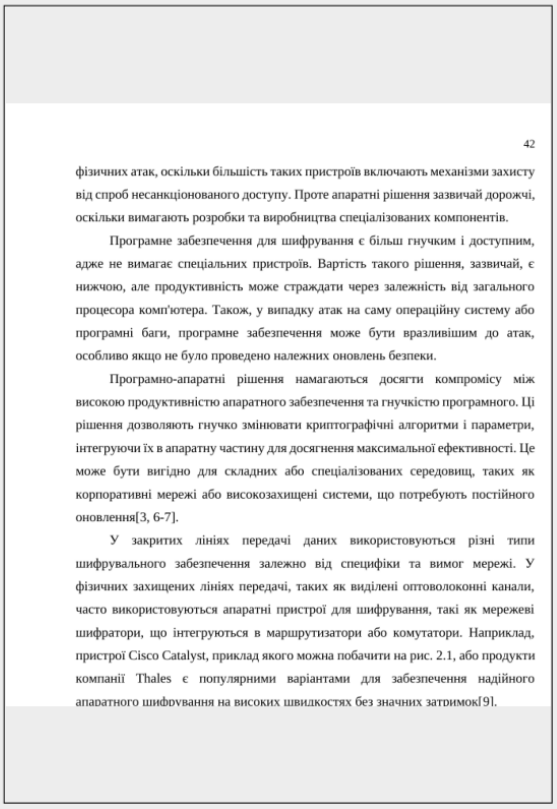
У мобільних захищених мережах, таких як LTE та 5G, шифрування відіграє ключову роль. У мобільних мережах LTE і 5G симетричне шифрування (AES) забезпечує швидкість і захист радіоінтерфейсу, а асиметричні алгоритми підтримують автентифікацію і створення захищеного каналу між пристроєм і мережею [28].

AES, RSA та ECC[3, 8, 17-19]:

1. **AES** — симетричний алгоритм шифрування, розроблений у 1998 році Вінсентом Рейменом і Жоаном Дайменом, які перемогли в конкурсі NIST(The National Institute of Standards and Technology). У 2001 році AES став стандартом для захисту державної та комерційної інформації, замінивши DES.

- У роботі розглянуто симетричні та асиметричні алгоритми, зокрема AES, RSA та ECC.
- AES забезпечує високу швидкість обробки та застосовується у VPN, оптоволоконних і супутникових каналах.
- RSA та ECC використовуються для обміну ключами, електронних сертифікатів та підтвердження автентичності сторін.

КРИПТОГРАФІЧНІ ПРОТОКОЛИ ЗАХИЩЕНИХ КАНАЛІВ



42

фізичних атак, оскільки більшість таких пристроїв включають механізми захисту від спроб несанкціонованого доступу. Проте апаратні рішення зазвичай дорожчі, оскільки вимагають розробки та виробництва спеціалізованих компонентів.

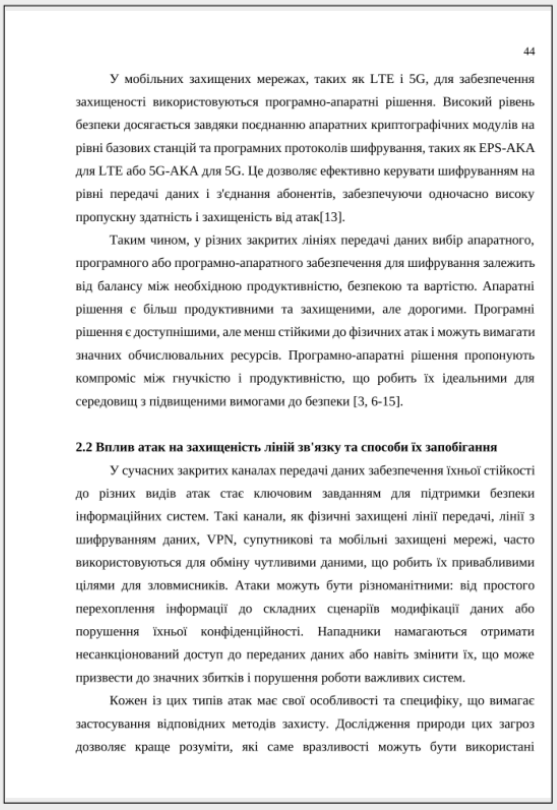
Програмне забезпечення для шифрування є більш гнучким і доступним, адже не вимагає спеціальних пристроїв. Вартість такого рішення, зазвичай, є нижчою, але продуктивність може страждати через залежність від загального процесора комп'ютера. Також, у випадку атак на саму операційну систему або програмні баги, програмне забезпечення може бути вразливішим до атак, особливо якщо не було проведено належних оновлень безпеки.

Програмно-апаратні рішення намагаються досягти компромісу між високою продуктивністю апаратного забезпечення та гнучкістю програмного. Ці рішення дозволяють гнучко змінювати криптографічні алгоритми і параметри, інтегруючи їх в апаратну частину для досягнення максимальної ефективності. Це може бути вигідно для складних або спеціалізованих середовищ, таких як корпоративні мережі або високозахищені системи, що потребують постійного оновлення[3, 6-7].

У закритих лініях передачі даних використовуються різні типи шифрувального забезпечення залежно від специфіки та вимог мережі. У фізичних захищених лініях передачі, таких як виділені оптоволоконні канали, часто використовуються апаратні пристрої для шифрування, такі як мережеві шифратори, що інтегруються в маршрутизатори або комутатори. Наприклад, пристрої Cisco Catalyst, приклад якого можна побачити на рис. 2.1, або продукти компанії Thales є популярними варіантами для забезпечення надійного апаратного шифрування на високих швидкостях без значних затримок[9].

- IPsec забезпечує захист IP-трафіку, підтримує тунельний і транспортний режими та застосовується у корпоративних VPN.
- SSL/TLS використовується для захисту веб-трафіку та поєднує асиметричний обмін ключами з симетричним шифруванням даних.
- Для апаратних рішень важливими є продуктивність шифрування, підтримка сертифікатів і стійкість до атак на кінцеві точки.

ТИПИ АТАК НА ЗАКРИТІ ЛІНІЇ ТА ЇХ ВПЛИВ



44

У мобільних захищених мережах, таких як LTE і 5G, для забезпечення захищеності використовуються програмно-апаратні рішення. Високий рівень безпеки досягається завдяки поєднанню апаратних криптографічних модулів на рівні базових станцій та програмних протоколів шифрування, таких як EPS-AKA для LTE або 5G-AKA для 5G. Це дозволяє ефективно керувати шифруванням на рівні передачі даних і з'єднання абонентів, забезпечуючи одночасно високу пропускну здатність і захищеність від атак[13].

Таким чином, у різних закритих лініях передачі даних вибір апаратного, програмного або програмно-апаратного забезпечення для шифрування залежить від балансу між необхідною продуктивністю, безпекою та вартістю. Апаратні рішення є більш продуктивними та захищеними, але дорогими. Програмні рішення є доступнішими, але менш стійкими до фізичних атак і можуть вимагати значних обчислювальних ресурсів. Програмно-апаратні рішення пропонують компроміс між гнучкістю і продуктивністю, що робить їх ідеальними для середовищ з підвищеними вимогами до безпеки [3, 6-15].

2.2 Вплив атак на захищеність ліній зв'язку та способи їх запобігання

У сучасних закритих каналах передачі даних забезпечення їхньої стійкості до різних видів атак стає ключовим завданням для підтримки безпеки інформаційних систем. Такі канали, як фізичні захищені лінії передачі, лінії з шифруванням даних, VPN, супутникові та мобільні захищені мережі, часто використовуються для обміну чутливими даними, що робить їх привабливими цілями для зловмисників. Атаки можуть бути різноманітними: від простого перехоплення інформації до складних сценаріїв модифікації даних або порушення їхньої конфіденційності. Нападники намагаються отримати несанкціонований доступ до переданих даних або навіть змінити їх, що може призвести до значних збитків і порушення роботи важливих систем.

Кожен із цих типів атак має свої особливості та специфіку, що вимагає застосування відповідних методів захисту. Дослідження природи цих загроз дозволяє краще розуміти, які саме вразливості можуть бути використані

- Основні загрози: перехоплення трафіку, атаки Man-in-the-Middle, модифікація повідомлень, DoS-атаки та компрометація кінцевих пристроїв.
- Уразливості можуть виникати через помилки налаштування, слабку автентифікацію, застарілі протоколи або недостатній контроль доступу.
- Оцінка загроз має враховувати ймовірність реалізації атаки та потенційний вплив на конфіденційність, цілісність і доступність даних.

ЗАСОБИ ПРОТИДІЇ: VPN, IDS/IPS, БРАНДМАУЕРИ ТА КОНТРОЛЬ ДОСТУПУ

користувачам на основі їхнього місцезнаходження або типу підключення. Це важливо для забезпечення того, щоб лише уповноважені користувачі могли отримати доступ до стратегічних або конфіденційних даних [2, 10-13, 16-21].

2.2.3 Використання брандмауерів, системи контролю доступу, систем виявлення та запобігання вторгнень (IDS(Intrusion Detection System)/IPS(Intrusion Prevention System))

Брандмауери (Firewall) є основним інструментом для захисту мереж від несанкціонованого доступу. Вони фільтрують мережевий трафік на основі попередньо встановлених правил, що дозволяє блокувати небажані підключення або атаки. Це рішення використовується в усіх типах закритих ліній передачі даних: фізичних захищених лініях, лініях з шифруванням, VPN, супутникових та мобільних захищених мережах. У фізичних лініях брандмауери контролюють доступ до критичних точок, у VPN та шифрованих лініях – захищають трафік на вході й виході з каналів, у супутникових мережах – захищають наземні станції, а в мобільних мережах LTE і 5G – базові станції й пристрої.

Переваги брандмауерів включають швидку фільтрацію трафіку та гнучке налаштування політик. Недоліком є відсутність глибокого аналізу трафіку або захисту від складних атак, наприклад, всередині зашифрованих каналів. Прикладом ефективного рішення є Cisco ASA Firewall для фізичних, рис. 2.6, і VPN-мереж, який забезпечує як апаратну, так і програмну безпеку.

Рисунок 2.6 — Cisco ASA 5500-X Series Firewalls

Системи контролю доступу (Access Control Systems, ACS) використовуються для забезпечення того, що лише авторизовані користувачі можуть отримати доступ до критичних ресурсів у закритих лініях передачі

- VPN створює захищений тунель і зменшує ризик перехоплення даних під час передавання через відкриті мережі.
- Брандмауери та системи IDS/IPS забезпечують фільтрацію трафіку, контроль політик доступу та виявлення підозрілої активності.
- Багатофакторна автентифікація та сертифікати X.509 підвищують стійкість каналу до підміни користувача або вузла мережі.

ІДЕЯ РОЗРОБЛЕНОГО ЗАКРИТОГО КАНАЛУ ПЕРЕДАЧІ ДАНИХ

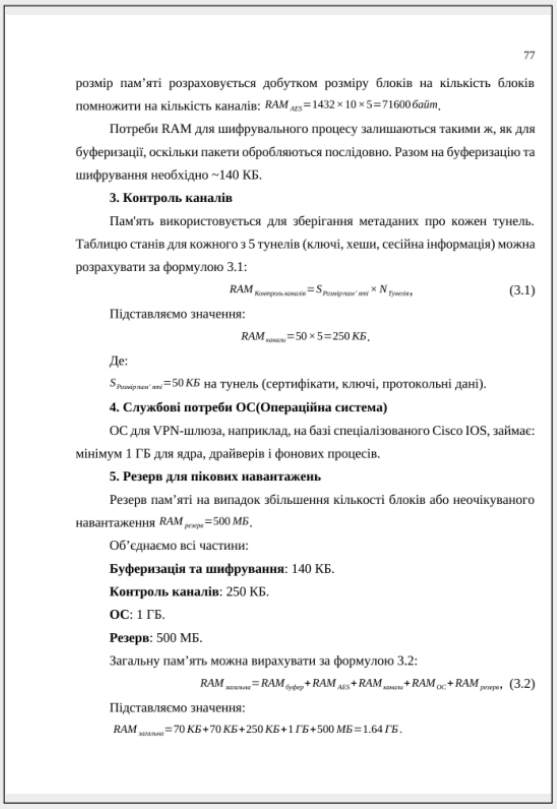
РОЗДІЛ 3 РОЗРОБЛЕНИЙ ЗАКРИТИЙ КАНАЛ ПЕРЕДАЧІ ДАНИХ

3.1 Опис ідеї закритого каналу передачі даних

Цей розділ присвячений розробці нового підходу до створення закритого каналу передачі даних, що базується на модифікації існуючих VPN-технологій. Основна концепція полягає у забезпеченні високого рівня захисту за рахунок поділу інформаційного потоку на кілька паралельних каналів з меншою пропускною здатністю. На відміну від традиційного VPN, який використовує один канал для передачі всіх даних, ця модель передбачає одночасну роботу

- Запропонована концепція передбачає багаторівневий захист передавання даних із використанням VPN-тунелю, шифрування та контролю цілісності.
- Канал орієнтований на корпоративне середовище, де критично важливі захищеність, керованість і контроль доступу.
- Архітектура поєднує апаратний VPN-шлюз, криптографічні механізми, багатофакторну автентифікацію та журналювання подій.

РОЗРАХУНОК ПАРАМЕТРІВ ТА ОБРОБКА БЛОКІВ ДАНИХ



77

розмір пам’яті розраховується добутком розміру блоків на кількість блоків помножити на кількість каналів: $RAM_{AES} = 1432 \times 10 \times 5 = 71600\,байт$.

Потреби RAM для шифрувального процесу залишаються такими ж, як для буферизації, оскільки пакети обробляються послідовно. Разом на буферизацію та шифрування необхідно ~140 КБ.

3. Контроль каналів

Пам'ять використовується для зберігання метаданих про кожен тунель. Таблицю станів для кожного з 5 тунелів (ключі, хеши, сесійна інформація) можна розрахувати за формулою 3.1:

$$RAM_{Контроль\ каналів} = S_{Розмір\ пам'яті} \times N_{тунелів}, \quad (3.1)$$

Підставляємо значення:

$$RAM_{канали} = 50 \times 5 = 250\,КБ.$$

Де:

$S_{Розмір\ пам'яті} = 50\,КБ$ на тунель (сертифікати, ключі, протокольні дані).

4. Службові потреби ОС(Операційна система)

ОС для VPN-шлюза, наприклад, на базі спеціалізованого Cisco IOS, займає: мінімум 1 ГБ для ядра, драйверів і фонових процесів.

5. Резерв для пікових навантажень

Резерв пам’яті на випадок збільшення кількості блоків або неочікуваного навантаження $RAM_{резерв} = 500\,МБ$.

Об’єднаємо всі частини:

Буферизація та шифрування: 140 КБ.

Контроль каналів: 250 КБ.

ОС: 1 ГБ.

Резерв: 500 МБ.

Загальну пам’ять можна вирахувати за формулою 3.2:

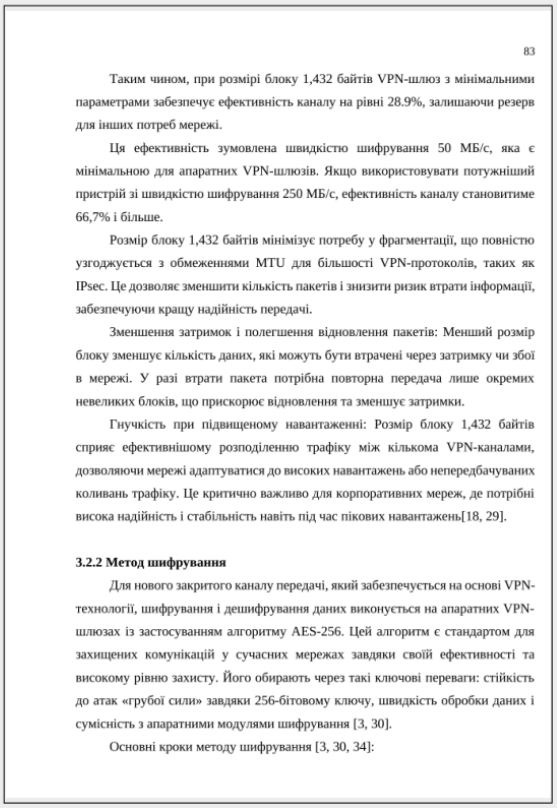
$$RAM_{загальна} = RAM_{буфер} + RAM_{AES} + RAM_{канали} + RAM_{ОС} + RAM_{резерв}, \quad (3.2)$$

Підставляємо значення:

$$RAM_{загальна} = 70\,КБ + 70\,КБ + 250\,КБ + 1\,ГБ + 500\,МБ = 1.64\,ГБ.$$

- У роботі розглянуто параметри розміру блоку, часу шифрування, передачі та буферизації даних.
- Для забезпечення стабільної роботи каналу враховуються пропускна здатність, затримка, обчислювальні ресурси VPN-шлюзу і розмір пакетів.
- Оптимізація блоків дозволяє зменшити затримку і підтримати баланс між продуктивністю та захистом.

ВИКОРИСТАННЯ VPN-ШЛЮЗУ ТА АПАРАТНОГО ШИФРУВАННЯ



83

Таким чином, при розмірі блоку 1,432 байтів VPN-шлюз з мінімальними параметрами забезпечує ефективність каналу на рівні 28.9%, залишаючи резерв для інших потреб мережі.

Ця ефективність зумовлена швидкістю шифрування 50 МБ/с, яка є мінімальною для апаратних VPN-шлюзів. Якщо використовувати потужніший пристрій зі швидкістю шифрування 250 МБ/с, ефективність каналу становитиме 66,7% і більше.

Розмір блоку 1,432 байтів мінімізує потребу у фрагментації, що повністю узгоджується з обмеженнями MTU для більшості VPN-протоколів, таких як IPsec. Це дозволяє зменшити кількість пакетів і знизити ризик втрати інформації, забезпечуючи кращу надійність передачі.

Зменшення затримок і полегшення відновлення пакетів: Менший розмір блоку зменшує кількість даних, які можуть бути втрачені через затримку чи збої в мережі. У разі втрати пакета потрібна повторна передача лише окремих невеликих блоків, що прискорює відновлення та зменшує затримки.

Гнучкість при підвищеному навантаженні: Розмір блоку 1,432 байтів сприяє ефективнішому розподіленню трафіку між кількома VPN-каналами, дозволяючи мережі адаптуватися до високих навантажень або непередбачуваних коливань трафіку. Це критично важливо для корпоративних мереж, де потрібні висока надійність і стабільність навіть під час пікових навантажень[18, 29].

3.2.2 Метод шифрування

Для нового закритого каналу передачі, який забезпечується на основі VPN-технології, шифрування і дешифрування даних виконується на апаратних VPN-шлюзах із застосуванням алгоритму AES-256. Цей алгоритм є стандартом для захищених комунікацій у сучасних мережах завдяки своїй ефективності та високому рівню захисту. Його обирають через такі ключові переваги: стійкість до атак «грубої сили» завдяки 256-бітовому ключу, швидкість обробки даних і сумісність з апаратними модулями шифрування [3, 30].

Основні кроки методу шифрування [3, 30, 34]:

- VPN-шлюз виконує генерацію ключів, шифрування, інкапсуляцію трафіку та створення захищеного тунелю.
- Апаратне шифрування знижує навантаження на програмні компоненти та підвищує стабільність роботи каналу.
- Застосування AES-256 і захищеного обміну ключами забезпечує високий рівень конфіденційності переданих даних.

КОНТРОЛЬ ДОСТУПУ ТА АВТЕНТИФІКАЦІЯ У ЗАПРОПОНОВАНОМУ КАНАЛІ

інфраструктура забезпечує додатковий рівень захисту і дозволяє стабільно передавати дані навіть при високому навантаженні в мережі [11, 14].

3.2.4 Контроль доступу та автентифікація

В даному закритому каналі передачі даних контроль доступу та автентифікація в першу чергу забезпечується через протокол EAP (Extensible Authentication Protocol), підтверджують особу користувача через паролі, сертифікати чи двофакторну аутентифікацію. Зокрема, використовується його версія EAP-TLS, який забезпечує обмін ключами через асиметричне шифрування, використовуючи сертифікати X.509 для автентифікації обох сторін з'єднання. Під час рукостискання сертифікати перевіряють справжність за допомогою відкритих і закритих ключів: відкритий ключ підтверджує підпис, зроблений закритим ключем відправника. Після успішної автентифікації EAP-TLS встановлює симетричний сеансовий ключ для шифрування даних у поточному сеансі, що оптимізує ефективність обробки інформації та зменшує час її передавання.

Для більшої безпеки в даному каналі використовується VPN-з'єднання на основі протоколу IPsec у конфігурації для тунельного режиму. Кожен з VPN-каналів, побудованих на основі IPsec у тунельному режимі, буде проходити через різні маршрути, тому захист переданих даних та автентифікація повинні враховувати цю особливість. Для кожного каналу застосовується протокол IPsec IKEv2, який забезпечує стійкість з'єднання, а також підтримує AES-256 для конфіденційності та SHA-256 для цілісності даних. IPsec VPN використовує ESP для інкапсуляції й автентифікації даних, що гарантує захист як самого вмісту, так і заголовків пакетів на кожному окремому маршруті[11, 30].

Для узагальнення використовується наступна версія протоколу IPsec IKEv2. Протокол IKEv2 має модульну структуру, що дозволяє налаштувати його для підтримки конкретних алгоритмів шифрування та методів аутентифікації. Кожен із протоколів у даній конфігурації виконує власну функцію в рамках тунельного з'єднання:

- Контроль доступу базується на автентифікації користувачів і пристроїв із використанням сертифікатів та протоколів перевірки.
- EAP-TLS і RADIUS можуть застосовуватися для централізованої перевірки облікових даних та політик доступу.
- Додатковий захист забезпечують MFA, перевірка цілісності повідомлень і виявлення повторного використання пакетів.

ОЦІНКА ЗАХИЩЕНОСТІ, РИЗИКІВ ТА ПРОДУКТИВНОСТІ

Результати оцінки показали високу ефективність методів захисту, зокрема автентифікації на основі сертифікатів X.509, які практично виключають можливість підробки сертифікатів. Також протокол EAP-TLS успішно блокує спроби Replay-атак завдяки унікальним сеансовим ідентифікаторам, а криптографічний захист IPsec IKEv2 забезпечує стійкість до атак MITM. Усі ці аспекти підтверджують, що проектований канал є надійним рішенням для захисту даних у середовищах із підвищеними ризиками несанкціонованого доступу [32-33, 37, 42].

3.3.4 Моделювання ризиків

Щоб зрозуміти, за яких обставин найкраще використовувати певний закритий канал передачі, потрібно знати не лише його сильні сторони, але й слабкі. З цією метою було проведено дослідження з моделювання ризиків для виявлення потенційних вразливостей у проектованому закритому каналі захисту інформації, що використовує модифіковану VPN-архітектуру з багатоканальним підходом. Можна виділити такі найбільш ризикові аспекти [18, 37-38]:

1. Атаки типу MITM

Опис: Атаки MITM можуть виникати на етапах встановлення з'єднання між кінцевими точками каналу, коли відбувається обмін ключами. Навіть з криптографічними протоколами (EAP-TLS, IPsec IKEv2), існує ризик, що зловмисник може перехопити цей процес.

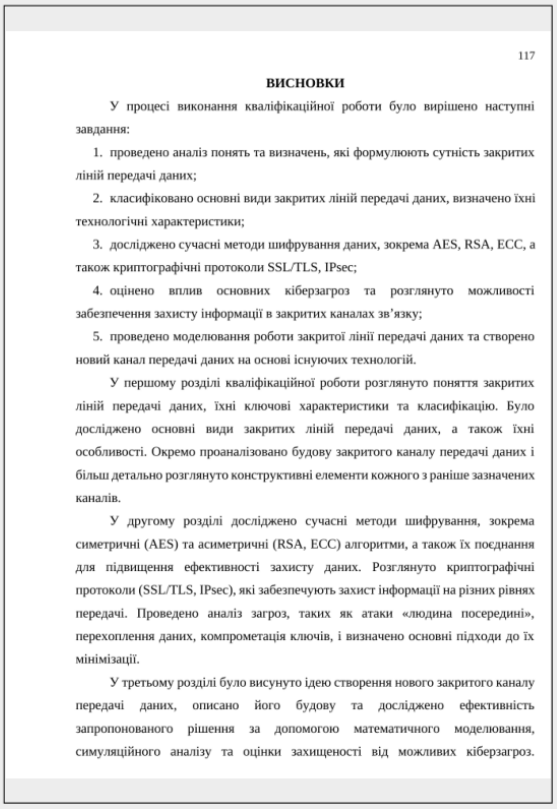
Чому це небезпечно: Ця атака дозволяє зловмиснику перехоплювати трафік у режимі реального часу, підміняти його або втручатися в комунікацію.

Ймовірність реалізації: Середня. Для успіху зловмисник має отримати доступ до одного з маршрутизаторів на яких і відбувається шифрування і дешифрування даних, що потребує доступу до самого маршрутизатора або зловмиснику потрібно буде моніторити велику частину мережі, щоб знайти всі канали.

2. Витік даних через сторонні канали (англ. Side-Channel Attacks)

- Проведене моделювання показує, що комбінування VPN, AES-256, сертифікатів X.509 і MFA істотно знижує ризик НСД.
- Найбільш значущими залишаються ризики компрометації кінцевих точок, помилок конфігурації та впливу атак на доступність.
- Аналіз продуктивності підтверджує доцільність застосування апаратного шифрування для корпоративних каналів із високими вимогами до безпеки.

ВИСНОВКИ ТА ПРАКТИЧНЕ ЗНАЧЕННЯ РОБОТИ



117

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було вирішено наступні завдання:

1. проведено аналіз понять та визначень, які формулюють сутність закритих ліній передачі даних;
2. класифіковано основні види закритих ліній передачі даних, визначено їхні технологічні характеристики;
3. досліджено сучасні методи шифрування даних, зокрема AES, RSA, ECC, а також криптографічні протоколи SSL/TLS, IPsec;
4. оцінено вплив основних кіберзагроз та розглянуто можливості забезпечення захисту інформації в закритих каналах зв'язку;
5. проведено моделювання роботи закритої лінії передачі даних та створено новий канал передачі даних на основі існуючих технологій.

У першому розділі кваліфікаційної роботи розглянуто поняття закритих ліній передачі даних, їхні ключові характеристики та класифікацію. Було досліджено основні види закритих ліній передачі даних, а також їхні особливості. Окремо проаналізовано будову закритого каналу передачі даних і більш детально розглянуто конструктивні елементи кожного з раніше зазначених каналів.

У другому розділі досліджено сучасні методи шифрування, зокрема симетричні (AES) та асиметричні (RSA, ECC) алгоритми, а також їх поєднання для підвищення ефективності захисту даних. Розглянуто криптографічні протоколи (SSL/TLS, IPsec), які забезпечують захист інформації на різних рівнях передачі. Проведено аналіз загроз, таких як атаки «людина посередині», перехоплення даних, компрометація ключів, і визначено основні підходи до їх мінімізації.

У третьому розділі було висунуто ідею створення нового закритого каналу передачі даних, описано його будову та досліджено ефективність запропонованого рішення за допомогою математичного моделювання, симуляційного аналізу та оцінки захищеності від можливих кіберзагроз.

- У роботі досліджено сутність закритих ліній передачі даних, їх класифікацію, технічні характеристики та застосування у захищених комунікаціях.
- Проаналізовано AES, RSA, ECC, IPsec, SSL/TLS, VPN, MFA та засоби контролю доступу для протидії сучасним кіберзагрозам.
- Запропонований закритий канал доцільно застосовувати в корпоративних і державних інформаційних системах, де потрібні конфіденційність, цілісність і контроль доступу.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Сергій КУЛІНІЧ

Тема: «Організація захисту закритої лінії передачі даних»

Київ - 2025