НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання комп'ютерного практикуму

# ДОСЛІДЖЕННЯ РЕАЛІЗАЦІЙ ПРОТОКОЛІВ IPSEC

Виконали студенти
групи ФІ-32мн
Мельник Ілля,
Міснік Аліна

Перевірила:
Селюх П.В.

Київ — 2024

**Мета роботи:** Дослідити особливості реалізації криптографічних механізмів протоколів IPSec, їх місце в мережевій моделі OSI та взаємодію зі стеком TCP/IP. Ознайомитись із концепцією безпечних асоціацій (SA) та проаналізувати структуру заголовків протоколів AH та ESP.

**Постановка задачі:**

1) Описати основне призначення протоколу IPSec та його місце в мережевій архітектурі.

2) Вивчити архітектуру стеку протоколів IPSec, включаючи AH, ESP, ISAKMP, IKE, IKEv2, KINK.

3) Проаналізувати концепцію безпечних асоціацій (SA) та їх реалізацію через SPD і SAD.

4) Розглянути структуру заголовків AH та ESP для транспортного і тунельного режимів.

5) Визначити особливості криптографічних алгоритмів (аутентифікації, шифрування) для IPSec.

6) Вивчити варіанти використання IPSec для побудови VPN-тунелів.

# 1 ХІД РОБОТИ

## 1.1 Основне призначення протоколу IPSec та його місце в мережевій архітектурі

**Загальна інформація про IPSec**

IPSec (Internet Protocol Security) – це набір протоколів і технологій, розроблених для забезпечення безпеки на мережевому рівні (рівень 3 моделі OSI). Його основною метою є захист даних, що передаються через незахищені мережі, наприклад, Інтернет, шляхом застосування різноманітних криптографічних методів.

IPSec був стандартизований організацією IETF (Internet Engineering Task Force) і забезпечує такі базові функції:

1. **Конфіденційність (Encryption)** – дані шифруються, щоб запобігти їх перегляду сторонніми особами.

2. **Цілісність даних (Data Integrity)** – IPSec гарантує, що дані не були змінені під час передачі.

3. **Аутентифікація (Authentication)** – перевірка джерела даних для забезпечення його достовірності.

4. **Антивідтворення (Anti-Replay Protection)** – захист від повторного використання раніше перехоплених пакетів.

**Основні компоненти IPSec**

IPSec складається з кількох ключових елементів:

1) **Протокол AH (Authentication Header)**

– Забезпечує автентифікацію джерела даних і контроль цілісності пакетів.

– Не забезпечує шифрування даних.

– Використовується у випадках, коли потрібно лише перевірити достовірність та цілісність інформації.

2) **Протокол ESP (Encapsulating Security Payload)**

– Забезпечує шифрування, аутентифікацію та контроль цілісності даних.

– Використовується для забезпечення конфіденційності, що особливо важливо для захищених мережевих з'єднань.

3) **SA (Security Association)**

– Логічне з'єднання між двома пристроями, що визначає параметри безпеки, необхідні для IPSec-комунікації.

– Включає параметри шифрування, алгоритми аутентифікації, ключі та методи роботи.

4) **Ключова інфраструктура**

– IPSec використовує протоколи обміну ключами, такі як IKE (Internet Key Exchange), для безпечного встановлення ключів.

**Режими роботи IPSec**

IPSec складається з кількох ключових елементів:

1) **Транспортний режим (Transport Mode)**

– Захищає лише корисне навантаження (payload) IP-пакета.

– Вихідний IP-заголовок залишається без змін, що зменшує накладні витрати.

– Використовується, коли необхідно захистити дані між двома конкретними вузлами.

2) **Тунельний режим (Tunnel Mode)**

– Захищає весь IP-пакет, включаючи його заголовок.

– Увесь пакет інкапсулюється в новий IP-пакет з новим заголовком.

– Використовується для створення віртуальних приватних мереж (VPN).

**Призначення IPSec**

Основне призначення IPSec – це забезпечення безпеки даних при їх передачі в мережі. Протокол використовується для:

— Захисту конфіденційної інформації: IPSec забезпечує безпечну передачу даних через незахищені мережі, такі як Інтернет.

— Побудови VPN-тунелів: IPSec є основою для створення віртуальних

приватних мереж, які дозволяють організаціям безпечно з'єднувати офіси, віддалені працівники можуть підключатися до корпоративних мереж.

— Забезпечення захищеного доступу: Наприклад, між пристроями в одній корпоративній мережі.

— Міжмережевий захист: IPSec інтегрується з міжмережевими екранами (firewalls) для запобігання несанкціонованому доступу.

**Місце в мережевій архітектурі**

IPSec працює на **мережевому рівні (рівень 3 моделі OSI)**, що дозволяє йому забезпечувати безпеку без прив'язки до конкретних додатків. Це дає такі переваги:

1. Захист забезпечується для всіх додатків, які працюють через IP, без необхідності їхньої модифікації.

2. Інтегрується зі стеком TCP/IP, що дозволяє забезпечувати захист на рівні IP-пакетів.

IPSec працює між рівнями «Мережевий доступ» та «Транспортний рівень». Оскільки він оперує на рівні IP, то захищає як TCP, так і UDP трафік.

## 1.2 Архітектура стеку протоколів IPSec

Архітектура стеку IPSec побудована таким чином, щоб забезпечити безпеку на мережевому рівні шляхом використання різних протоколів, механізмів аутентифікації, шифрування та управління ключами. Кожен елемент стеку виконує специфічну функцію, необхідну для створення, підтримки та захисту IPSec-з'єднань.

**Основні компоненти стеку IPSec**

**AH (Authentication Header)** – протокол, який забезпечує цілісність і аутентифікацію IP-пакетів.

1) Функціональність: перевіряє, чи дані, передані між вузлами, не були змінені, гарантує автентичність джерела даних.

2) Особливості: не забезпечує шифрування даних, використовує HMAC

(Hash-based Message Authentication Code) для перевірки цілісності.

3) Недоліки: не захищає конфіденційність даних.

**ESP (Encapsulating Security Payload)** – протокол, який забезпечує шифрування, аутентифікацію і контроль цілісності даних.

1) Функціональність: шифрує дані для захисту конфіденційності, перевіряє цілісність і автентичність даних.

2) Особливості: може працювати як самостійно, так і разом з AH, підтримує різні алгоритми шифрування, такі як AES, 3DES.

3) Режими роботи: транспортний режим (захищає лише корисне навантаження), тунельний режим (захищає весь IP-пакет).

**ISAKMP (Internet Security Association and Key Management Protocol)** – протокол, який забезпечує управління безпековими асоціаціями (SA).

1) Функціональність: визначає параметри безпеки, необхідні для роботи IPSec, відповідає за обмін ключами між пристроями.

2) Особливості: не виконує аутентифікацію або шифрування даних безпосередньо, є основою для роботи протоколу IKE.

**IKE (Internet Key Exchange)** – протокол, який працює на основі ISAKMP і використовується для управління ключами.

1) Функціональність: проводить аутентифікацію вузлів, створює безпекові асоціації (SA) для AH та ESP, встановлює криптографічні ключі для шифрування даних.

2) Режими роботи: Main Mode (основний режим, повільний, але забезпечує кращу безпеку), Aggressive Mode (агресивний режим, швидший, але менш безпечний).

**IKEv2** – покращена версія IKE, яка спрощує процес встановлення з'єднання і підвищує ефективність.

1) Особливості: знижує кількість обмінів повідомленнями, підтримує мобільність та мультихомінг (з'єднання через декілька інтерфейсів), інтегрує механізми для відновлення з'єднання після його втрати.

**KINK (Kerberized Internet Negotiation of Keys)** – протокол, який

використовує систему Kerberos для управління ключами.

1) Функціональність: забезпечує взаємну аутентифікацію між вузлами, дозволяє обмінюватися ключами через Kerberos.

2) Особливості: використовується в специфічних сценаріях, наприклад, у корпоративних мережах з уже налаштованою Kerberos.

**Взаємодія між компонентами**

1. AH і ESP: ці два протоколи забезпечують основну функціональність IPSec. AH гарантує цілісність і автентичність даних, тоді як ESP додає шифрування.

2. ISAKMP, IKE та IKEv2: забезпечують управління безпековими асоціаціями (SA) та управління ключами для AH та ESP.

3. KINK: використовується для спеціальних випадків, коли потрібна інтеграція з Kerberos.

**Архітектура стеку IPSec**

Уявімо архітектуру стеку IPSec як багаторівневу структуру:

1. Нижній рівень: реалізація протоколів AH та ESP для забезпечення цілісності, автентифікації та шифрування.

2. Середній рівень: управління безпековими асоціаціями через ISAKMP, IKE або IKEv2.

3. Верхній рівень: обмін ключами та взаємна аутентифікація через KINK (у разі використання).

## 1.3 Аналіз концепції безпечних асоціацій (SA) та їх реалізації через SPD і SAD

Безпечні асоціації (Security Associations, SA) є основним елементом роботи IPSec, оскільки вони визначають параметри безпеки для обміну даними між вузлами.

Безпечна асоціація (SA) – це набір параметрів безпеки, які використовуються для захисту даних, що передаються між двома вузлами.

SA визначає правила та механізми шифрування, аутентифікації та забезпечення цілісності, які застосовуються до переданого трафіку.

**Основні характеристики SA**:

1. Односторонність: SA діє тільки в одному напрямку: від відправника до отримувача. Для двостороннього зв'язку необхідно створити дві SA – одну для кожного напряму.

2. Унікальність: кожна SA ідентифікується унікальним ключем, що складається з трьох параметрів: IP-адреса призначення, ідентифікатор протоколу безпеки (AH або ESP), SPI (Security Parameters Index) – унікальний числовий ідентифікатор SA.

3. Динамічність: SA створюються та керуються динамічно за допомогою протоколів, таких як IKE (Internet Key Exchange).

Для забезпечення роботи SA використовуються дві основні бази даних:

1. SPD (Security Policy Database) – База політик безпеки.

2. SAD (Security Association Database) – База безпечних асоціацій.

**SPD (Security Policy Database)**

SPD (Security Policy Database) – це база даних, яка визначає, як обробляти вхідний та вихідний трафік у контексті безпеки. Вона є своєрідним «фільтром», який аналізує мережевий трафік та вирішує, що з ним робити: дозволити його передавання без змін, застосувати до нього безпекові механізми IPSec або повністю заблокувати.

У цій базі зберігаються політики, що визначають правила роботи з трафіком, наприклад, на основі IP-адрес джерела та призначення, типу протоколу чи портів. Політики в SPD можуть бути налаштовані таким чином, щоб один тип трафіку (наприклад, HTTP) проходив без змін, тоді як інший (наприклад, SSH) шифрувався з використанням IPSec. Кожен запис у SPD визначає набір умов, за якими трафік порівнюється, та відповідну дію (дозволити, захистити чи відхилити).

SPD працює як на вихідному, так і на вхідному трафіку. Наприклад, коли пристрій надсилає дані, SPD перевіряє, чи потрібно застосувати IPSec. Якщо захист необхідний, база даних шукає відповідну SA у SAD (Security

Association Database). Якщо SA ще не створена, система ініціює її налаштування, щоб забезпечити захист цього типу трафіку.

**SAD (Security Association Database)**

SAD (Security Association Database) – це база даних, яка містить активні безпечні асоціації (SA), що використовуються для обробки трафіку. Якщо SPD визначає, що трафік потрібно захистити, саме SAD зберігає параметри, необхідні для цього. У базі SAD зберігаються такі параметри, як індекс параметрів безпеки (SPI), який є унікальним ідентифікатором SA, алгоритми шифрування й аутентифікації, а також ключі, які застосовуються до захищеного трафіку.

Коли вхідний трафік надходить до пристрою, система перевіряє його заголовок IPSec (AH або ESP), щоб знайти SPI. Потім цей SPI використовується для пошуку відповідної SA в SAD. Знайшовши відповідний запис, пристрій використовує інформацію з SAD для дешифрування даних, перевірки їх цілісності й автентичності.

SAD і SPD працюють у тісному взаємозв'язку. SPD відповідає за аналіз трафіку та прийняття рішень щодо його обробки, тоді як SAD забезпечує технічну реалізацію захисту, визначеного цими рішеннями. Наприклад, якщо SPD визначило, що конкретний тип трафіку має бути зашифрованим, SAD надасть інформацію про ключі та алгоритми, необхідні для цього.

**Взаємодія між SPD і SAD**

Ці дві бази доповнюють одна одну. SPD є точкою прийняття рішень: воно визначає, що робити з трафіком. SAD, у свою чергу, виконує ці рішення, надаючи всю технічну інформацію для реалізації безпеки. Коли IPSec-з'єднання встановлено, кожне передавання даних відбувається з перевіркою та обробкою через ці бази даних. SPD перевіряє політику, а SAD гарантує, що трафік буде належним чином захищений або оброблений.

Цей механізм забезпечує надійну архітектуру для управління захищеними з'єднаннями, що дозволяє IPSec динамічно адаптуватися до потреб мережі.

## 1.4 Структура заголовків AH та ESP для транспортного і тунельного режимів

Для забезпечення захисту даних у мережах IPSec використовує два основних протоколи: Authentication Header (AH) та Encapsulating Security Payload (ESP). Кожен із них додає спеціальний заголовок до IP-пакетів, який використовується для забезпечення безпеки. AH відповідає за аутентифікацію та контроль цілісності, тоді як ESP додає ще й шифрування даних. Ці заголовки працюють по-різному залежно від обраного режиму – транспортного чи тунельного.

**Authentication Header (AH)**

AH забезпечує автентифікацію джерела даних та контроль цілісності пакетів. Він не виконує шифрування, тобто конфіденційність даних не гарантується. AH додає власний заголовок між базовим IP-заголовком і корисним навантаженням пакета.

Структура заголовка AH:

1. Next Header: Вказує на тип протоколу, який йде після AH (наприклад, TCP чи UDP).

2. Payload Length: Визначає довжину заголовка AH.

3. Security Parameters Index (SPI): Ідентифікує конкретну SA (Security Association), яка використовується для цього пакета.

4. Sequence Number: Захищає від атак із повторним відтворенням.

5. Authentication Data: Містить хеш-код (наприклад, HMAC-SHA1), який використовується для перевірки цілісності та автентичності даних.

У транспортному режимі AH захищає лише корисне навантаження (payload) IP-пакета, залишаючи оригінальний IP-заголовок без змін. У цьому випадку AH додається між IP-заголовком і корисним навантаженням. Наприклад, якщо хтось змінить дані або IP-адресу в оригінальному заголовку, AH виявить це і відхилить пакет.

У тунельному режимі AH захищає весь оригінальний IP-пакет

(заголовок + дані), який інкапсулюється у новий IP-пакет із новим заголовком. Таким чином, AH гарантує, що навіть заголовок оригінального пакета не може бути змінений. Це корисно для створення захищених VPN-з'єднань між мережами.

**Encapsulating Security Payload (ESP)**

ESP забезпечує як автентифікацію, так і шифрування даних. На відміну від AH, він не тільки гарантує цілісність, але й приховує вміст пакетів. Це робить ESP більш універсальним, адже він підходить як для забезпечення конфіденційності, так і для перевірки автентичності.

Структура заголовка ESP:

1. Security Parameters Index (SPI): Як і в AH, SPI ідентифікує конкретну SA для пакета.

2. Sequence Number: Захищає від атак із повторним відтворенням.

3. Encrypted Payload: Корисне навантаження, зашифроване з використанням алгоритмів, таких як AES чи 3DES.

4. Authentication Data: Забезпечує контроль цілісності та автентичності, подібно до AH, але для зашифрованого вмісту.

У транспортному режимі ESP шифрує тільки корисне навантаження IP-пакета. Оригінальний IP-заголовок залишається незмінним, що дозволяє використовувати ESP для точного налаштування безпеки між двома вузлами. Наприклад, це ідеально підходить для захисту з'єднань між двома серверами в одній мережі.

У тунельному режимі ESP шифрує весь оригінальний IP-пакет (заголовок і дані), а потім інкапсулює його в новий IP-пакет із новим заголовком. Таким чином, ні адреса відправника, ні призначення оригінального пакета не видно стороннім. Тунельний режим використовується в основному для VPN-з'єднань.

## 1.5 Особливості криптографічних алгоритмів для IPSec

IPSec забезпечує захист мережевих даних завдяки використанню різних криптографічних алгоритмів, які відповідають за три основні функції: конфіденційність, автентичність і цілісність інформації. Ці алгоритми гарантують, що дані, які передаються між пристроями, залишаються недоступними для сторонніх осіб, не змінюються під час передачі та походять від достовірного джерела.

Криптографія в IPSec використовує два основні типи алгоритмів: для шифрування даних і для їх аутентифікації. Алгоритми шифрування відповідають за конфіденційність, тобто за те, щоб навіть якщо дані будуть перехоплені, їхній зміст залишиться незрозумілим без відповідного ключа. Найпоширенішим алгоритмом у цьому контексті є AES (Advanced Encryption Standard), який став стандартом завдяки своїй надійності та ефективності. AES підтримує різні розміри ключів, зокрема 128, 192 та 256 біт, що дозволяє обирати рівень безпеки залежно від потреб. Іншим популярним алгоритмом, що історично використовувався в IPSec, є 3DES, який шифрує дані тричі для підвищення безпеки. Однак, через його порівняно низьку швидкість, він поступово витісняється більш сучасним AES.

Алгоритми аутентифікації, у свою чергу, гарантують, що дані дійсно були відправлені тим, хто стверджує, що їх відправив, і що вони не були змінені під час передачі. Для цього IPSec використовує хеш-функції, такі як SHA-1 або SHA-256. У контексті IPSec ці алгоритми реалізуються через механізм HMAC (Hash-based Message Authentication Code), який додає до хешу секретний ключ. Це забезпечує не тільки перевірку цілісності даних, але й підтвердження того, що їх відправило саме довірене джерело. Наприклад, HMAC-SHA256 є одним із найпоширеніших і сучасних алгоритмів для забезпечення автентичності, оскільки він генерує хеш-коди довжиною 256 біт і надійно захищений від атак.

У протоколі AH (Authentication Header) використовується виключно аутентифікація. AH додає до кожного IP-пакета хеш-код, який дозволяє приймаючій стороні перевірити, чи були дані змінені під час передачі, і підтвердити автентичність джерела. Цей протокол не забезпечує шифрування, тому конфіденційність даних не гарантується. Протокол ESP (Encapsulating Security Payload), навпаки, включає як шифрування, так і аутентифікацію, що робить його більш універсальним. ESP може одночасно шифрувати дані, захищаючи їхній зміст, і перевіряти їхню автентичність.

Особливістю роботи IPSec є підтримка різних алгоритмів шифрування та аутентифікації, що дозволяє адаптувати систему під конкретні потреби. Наприклад, у випадках, коли потрібна висока швидкість обробки даних, можна використовувати алгоритми, що оптимізовані для продуктивності, такі як ChaCha20-Poly1305, який поєднує швидке шифрування та аутентифікацію. Якщо ж пріоритетом є максимальна безпека, зазвичай обирають AES-256 для шифрування і HMAC-SHA256 для аутентифікації.

## 1.6 Використання IPSec для побудови VPN-тунелів

IPSec є ключовою технологією для створення віртуальних приватних мереж (VPN), що забезпечують безпечне з'єднання через незахищені мережі, такі як Інтернет. Завдяки механізмам шифрування, автентифікації та перевірки цілісності, IPSec гарантує, що дані, які передаються між пристроями чи мережами, залишаються конфіденційними, достовірними та незмінними під час передачі. Основна ідея VPN на основі IPSec полягає у створенні захищеного «тунелю», через який проходить мережевий трафік.

Завдяки своїй архітектурі IPSec підтримує широкий спектр сценаріїв використання у VPN. Один із найпоширеніших варіантів — міжмережеві з'єднання, також відомі як site-to-site VPN. У цьому випадку IPSec забезпечує шифрування даних між двома мережами, наприклад, головним офісом і його філіями. Кінцевими точками такого тунелю є маршрутизатори чи спеціалізовані VPN-шлюзи, які виконують функцію

шифрування та дешифрування трафіку.

Іншим поширеним варіантом є VPN для віддаленого доступу (remote-access VPN). У цьому випадку IPSec забезпечує безпечний зв'язок між віддаленим працівником і корпоративною мережею. Наприклад, працівник, використовуючи ноутбук чи смартфон, може під'єднатися до офісної мережі через Інтернет, створюючи IPSec-тунель до VPN-шлюзу компанії. Це дозволяє йому працювати так, ніби він знаходиться у фізичному офісі, з доступом до всіх ресурсів компанії.

IPSec у VPN-тунелях активно використовує протокол IKE (Internet Key Exchange), який відповідає за обмін ключами та налаштування параметрів безпеки. Покращена версія IKEv2 дозволяє швидше встановлювати з'єднання та підтримує мобільність, що робить її особливо корисною для сучасних сценаріїв віддаленої роботи.

Однією з найбільших переваг IPSec для VPN є його здатність забезпечувати захист на рівні IP. Це дозволяє шифрувати весь трафік, незалежно від того, які протоколи чи додатки використовуються, що робить IPSec універсальним рішенням. Завдяки цьому VPN на базі IPSec підходять для широкого спектра завдань, від захисту внутрішнього корпоративного трафіку до створення глобальних безпечних мереж.

Таким чином, IPSec залишається одним із найефективніших і найнадійніших інструментів для побудови VPN, забезпечуючи конфіденційність, цілісність і автентичність даних у будь-яких мережевих умовах.

# ВИСНОВКИ

У ході виконання лабораторної роботи було досліджено основні аспекти роботи протоколу IPSec, його архітектуру, компоненти та можливості використання. Зокрема, було розглянуто основне призначення IPSec, яке полягає в забезпеченні безпеки даних у мережах завдяки шифруванню, аутентифікації та контролю цілісності. Особливе значення має його здатність працювати на мережевому рівні, що дозволяє захищати будь-який тип трафіку, незалежно від використовуваних протоколів.

Було детально проаналізовано архітектуру стеку IPSec, включаючи компоненти AH, ESP, ISAKMP, IKE, IKEv2 та KINK. Кожен із цих елементів відіграє важливу роль у забезпеченні безпеки: від перевірки автентичності й цілісності до шифрування даних та управління ключами. Взаємодія між цими компонентами забезпечує гнучкість і масштабованість IPSec, що робить його універсальним для різних мережевих сценаріїв.

Концепції безпечних асоціацій (SA) та їхні реалізації через бази даних SPD і SAD дозволяють IPSec ефективно управляти трафіком, захищати дані та динамічно адаптуватися до змін у мережі. Структура заголовків AH і ESP у транспортному і тунельному режимах демонструє, як IPSec забезпечує різні рівні захисту залежно від потреб конкретного з'єднання.

Криптографічні алгоритми, які використовуються в IPSec для шифрування, аутентифікації та перевірки цілісності, такі як AES і HMAC-SHA256, гарантують високий рівень захисту даних.

Різноманітність сценаріїв використання IPSec для побудови VPN-тунелів, від міжмережевих з'єднань до віддаленого доступу, демонструє його ефективність у створенні захищених мережевих середовищ. Завдяки підтримці тунельного режиму та інтеграції з протоколом IKE, IPSec забезпечує як конфіденційність, так і зручність роботи в сучасних умовах.