# Віртуальні приватні мережі - VPN

# План

- Поняття про віртуальні приватні мережі (VPN)
- Види віртуальних приватних мереж
- Сервіси VPN
- Способи утворення захищених тунелів
- Рівні реалізації VPN
- Протоколи: SSL, SOCKS, IPSec, PPTP, L2F, L2TF

# Поняття про віртуальні приватні мережі (VPN)

Захист інформації в процесі передавання її відкритими каналами зв’язку базується на виконанні таких функцій:

- Автентифікація сторін, що взаємодіють
- Криптографічне закриття інформації, яка передається
- Підтвердження справжності й цілісності доставленої інформації
- Захист від повтору, затримки та видалення повідомлень
- Захист від відмовлення від фактів відправлення й одержання повідомлень

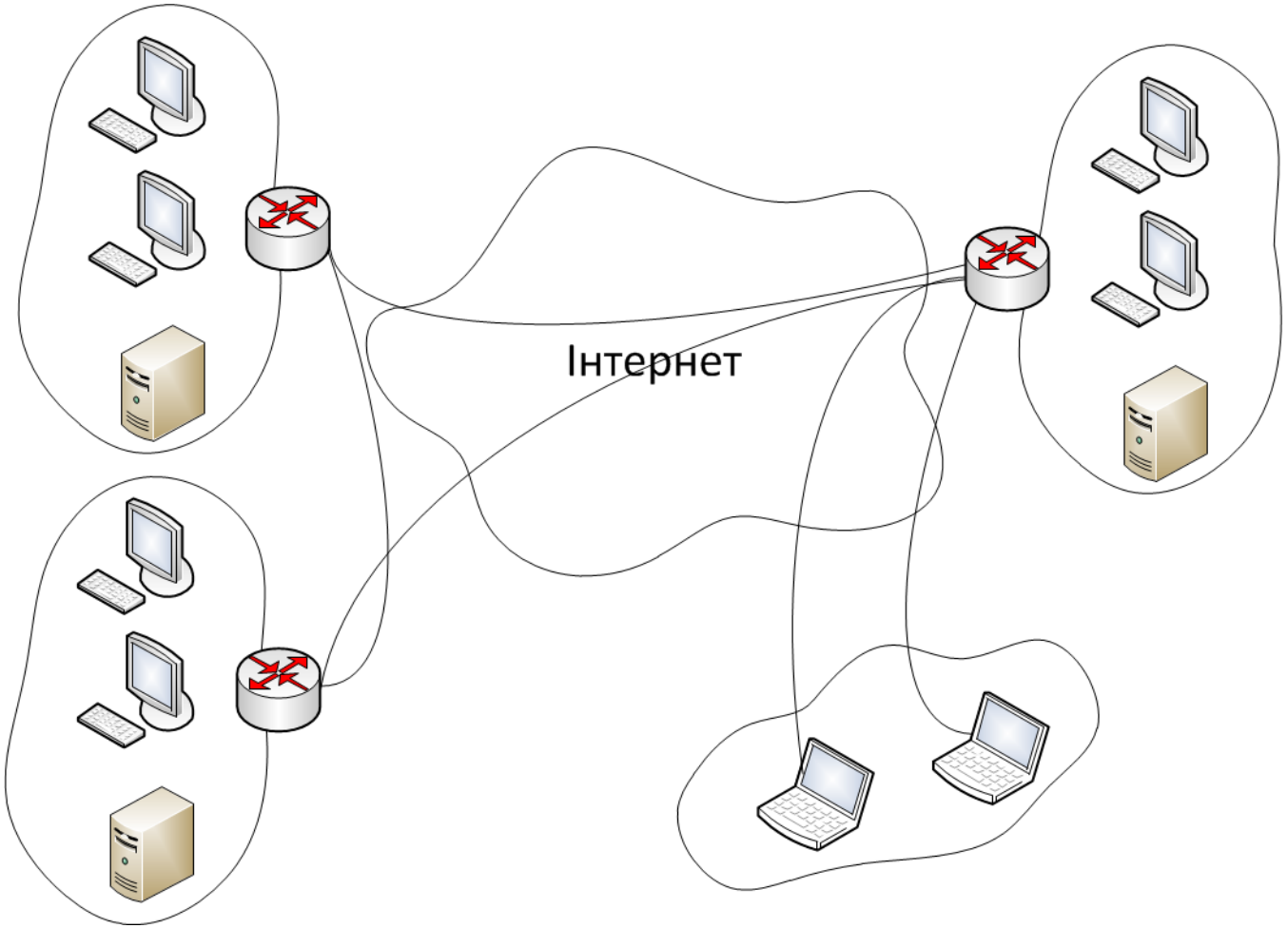
# Поняття про віртуальні приватні мережі (VPN)

- Об’єднання локальних мереж і окремих комп’ютерів через відкрите зовнішнє середовище передавання інформації в єдину віртуальну мережу, яка забезпечує захист інформації, що в ній циркулює, називається захищеною (або приватною) віртуальною мережею (англ. – *Virtual Private Network*, VPN)
- Термін “віртуальна” означає, що така мережа формується як деяка підмножина реальної мережі, з каналами зв’язку, що моделюються реальними каналами
- Особливою ознакою віртуальної приватної (захищеної) мережі є її відокремлення від реальної мережі, яке повинне бути достатньо надійним для гарантування конфіденційності та цілісності інформації, що в ній передається, а також для забезпечення автентифікації сторін і унеможливлення відмовлення від авторства (англ. – *Non-Repudiation*)

# Види віртуальних приватних мереж

- VPN віддаленого доступу (англ. – *Remote Access VPN*)
- Корпоративні VPN (англ. – *Intranet VPN*)
- Міжкорпоративні VPN (англ. – *Extranet VPN*)

# Види віртуальних приватних мереж



# VPN віддаленого доступу

- Віртуальні приватні мережі віддаленого доступу дозволяють значно скоротити витрати на використання комутованих та виділених ліній
- Принцип їх роботи
  - Користувачі встановлюють з’єднання з місцевою точкою доступу до глобальної мережі (точкою присутності провайдера Інтернет)
  - Дані, які передають користувачі, “тунелюються” через Інтернет
  - Дані від усіх користувачів концентруються на спеціальних пристроях – шлюзах віртуальної приватної мережі та передаються у корпоративну мережу

# Корпоративна мережа VPN

- Організації, що бажають організувати для своїх філій та відділень доступ до централізованих сховищ інформації, звичайно підключають віддалені вузли через виділені лінії
  - Використання виділених ліній означає зростання поточних витрат по мірі збільшення смуги пропускання та відстані між об’єктами
- Для скорочення витрат організація може з’єднати вузли за допомогою віртуальної приватної мережі
  - Для цього достатньо відмовитись від використання дорогих виділених ліній, замінивши їх більш дешевим зв’язком через Інтернет

# Міжкорпоративна мережа VPN

- Extranet – це мережна технологія, яка забезпечує прямий доступ з мережі однієї організації до мережі іншої організації і таким чином сприяє підвищенню якості зв’язку, що підтримується в ході ділового співробітництва
- Мережі Extranet VPN в цілому подібні до корпоративних VPN з тією різницею, що проблема захисту інформації є для них ще гострішою
  - Коли кілька організацій приймають рішення працювати разом і відкривають одна для одної свої мережі, вони повинні потурбуватись про те, щоби їхні нові партнери мали доступ лише до визначеного кола інформації
  - При цьому конфіденційна інформація повинна бути надійно захищеною від несанкціонованого використання
  - Також особливо важливою є автентифікація користувачів, яка повинна гарантувати, що доступ до інформації отримують лише ті, кому він дійсно дозволений

# Сервіси VPN

- Забезпечення конфіденційності
- Забезпечення цілісності
- Автентифікація та запобігання відмовленню від авторства

# Забезпечення конфіденційності

- Найпростішим і найпоширенішим способом забезпечення конфіденційності інформації є її шифрування, або криптографічне закриття
  - Незважаючи на те, що самі алгоритми шифрування дуже складні, їх реалізація великих утруднень не викликає
  - Доволі значну проблему становить керування ключами, особливо в разі значного збільшення кількості користувачів
  - В реалізації VPN керування ключами є одною з головних проблем, що потребує надійного і ефективного рішення
- Шифрування має неминучий побічний ефект – деяку втрату продуктивності
  - Апаратно реалізоване шифрування звільняє пристрої захисту від додаткового навантаження, пов’язаного з виконанням алгоритмів шифрування

# Забезпечення цілісності

- Цілісність контролюється використанням математичних алгоритмів гешування
  - Важливо підкреслити, що криптографічні механізми не забезпечують захист цілісності, а лише дозволяють впевнитись, що цілісність не була порушена, або, навпаки, виявити порушення
- Алгоритми гешування також потребують значних ресурсів процесора
  - Це дає підстави реалізовувати виконання цих алгоритмів в апаратних засобах з використанням інтегральних схем прикладної орієнтації

# Автентифікація та запобігання відмовленню від авторства

- Запобігання відмовленню від авторства (англ. – Non-Repudiation) – це додаткова функція, що реалізується на базі автентифікації
  - У захищеному спілкуванні часто виникають випадки, коли крім підтвердження того, що абонент є саме тим, за кого він себе намагається видати, важливо отримати незаперечні докази того, що повідомлення одержано від конкретного користувача
  - Також буває необхідним доказове підтвердження того, що певний користувач дійсно одержав деяке повідомлення
- Ці функції захисту у ряді випадків повинні бути невід'ємною складовою реалізації VPN

# Способи утворення захищених віртуальних каналів

- Будь-який з двох вузлів віртуальної мережі, між якими формується захищений тунель, може належати кінцевій чи проміжній точці потоку повідомлень, який захищають. Відповідно можливі різні способи утворення захищеного віртуального каналу
  - Кінцеві точки тунелю співпадають з кінцевими точками потоку повідомлень
  - Кінцевою точкою захищеного тунелю обирають брандмауер або граничний маршрутизатор локальної мережі, захищений тунель утворюється лише у публічній мережі

# Кінцеві точки тунелю співпадають з кінцевими точками потоку повідомлень

- Цей варіант є найкращим з міркувань безпеки
- Приклади кінцевих точок:
  - Сервер у центральному офісі компанії і робоча станція користувача у віддаленій філії
  - Портативний комп'ютер співробітника, який перебуває у відрядженні
- Перевагою такого варіанту є те, що захист інформаційного обміну забезпечується на всьому шляху пакетів повідомлень
- Суттєвий недолік цього варіанту – децентралізація керування
  - Засоби утворення захищених тунелів повинні встановлюватись і належним чином налаштовуватись на кожному клієнтському комп'ютері, що у великих мережах є занадто трудомісткою задачею

# Кінцева точка захищеного тунелю – брандмауер або граничний маршрутизатор локальної мережі

- Захищений тунель утворюється лише у публічній мережі
- Якщо відмовитись від захисту трафіка всередині локальної мережі (або локальних мереж), що входить до складу VPN, можна досягти помітного спрощення задач адміністрування
  - Захист трафіка всередині локальної мережі може забезпечуватись іншими засобами, такими, як, наприклад, реєстрація дій користувачів і організаційні заходи

# Реалізації VPN

- Реалізація VPN можлива засобами протоколів
  - Сеансового рівня (SSL/TLS, SOCKS)
  - Мережного рівня (IPsec)
  - Канального рівня (PPTP, L2TP)
- Поза розглядом залишаються системи шифрування на прикладному рівні, які реалізуються у деяких протоколах (SSH тощо), або просто деякими спеціальними прикладними програмами (наприклад, PGP)
  - Зазначені засоби здатні забезпечити захист інформаційного обміну, але вони
    - не є прозорими для прикладних програм
    - як правило, вони не забезпечують усіх необхідних функцій
    - вони не відносяться до засобів утворення VPN

# Захист віртуальних каналів на канальному рівні

- Утворення захищених тунелів на канальному рівні моделі OSI забезпечує незалежність від протоколів мережного рівня і всіх вищих рівнів
  - Таким чином досягається максимальна прозорість VPN
- Недоліки:
  - Ускладнюються задачі конфігурації і підтримки віртуальних каналів
  - Ускладнюється керування криптографічними ключами
  - Зменшується набір реалізованих функцій безпеки
- В якості протоколів на цьому рівні використовуються:
  - PPTP (англ. – *Point-to-Point Tunneling Protocol*)
  - L2F (англ. – *Layer-2 Forwarding*)
  - L2TP (англ. – *Layer-2 Tunneling Protocol*)
- Усі названі протоколи не специфікують протоколи автентифікації та шифрування

# Захист віртуальних каналів на мережному рівні

- Утворення захищених віртуальних каналів на мережному рівні дозволяє досягти оптимального співвідношення між прозорістю і якістю захисту
  - Реалізація засобів захисту на цьому рівні робить їх прозорими для мережних застосувань, оскільки мережний рівень завжди буде відокремлений від застосування реалізацією транспортного рівня
  - З іншого боку, на мережному рівні можлива достатньо повна реалізація функцій захисту трафіка і керування ключами, оскільки саме мережний рівень відповідає за маршрутизацію пакетів
- Стандартні засоби захисту на мережному рівні для IP мережі визначаються набором протоколів IPSec (англ. – Internet Protocol Security)
  - IPSec є складовою частиною IPv6
  - IPSec є сумісним з версією протоколу IPv4 (підтримка IPSec не є обов'язковою, але бажана, і в наш час, як правило, реалізована)
- IPSec вимагає підтримки стандарту IPSec лише від пристроїв по обидва боки з'єднання, що спілкуються між собою
  - Всі інші пристрої, що розташовані між ними, просто забезпечують передачу IP-пакетів

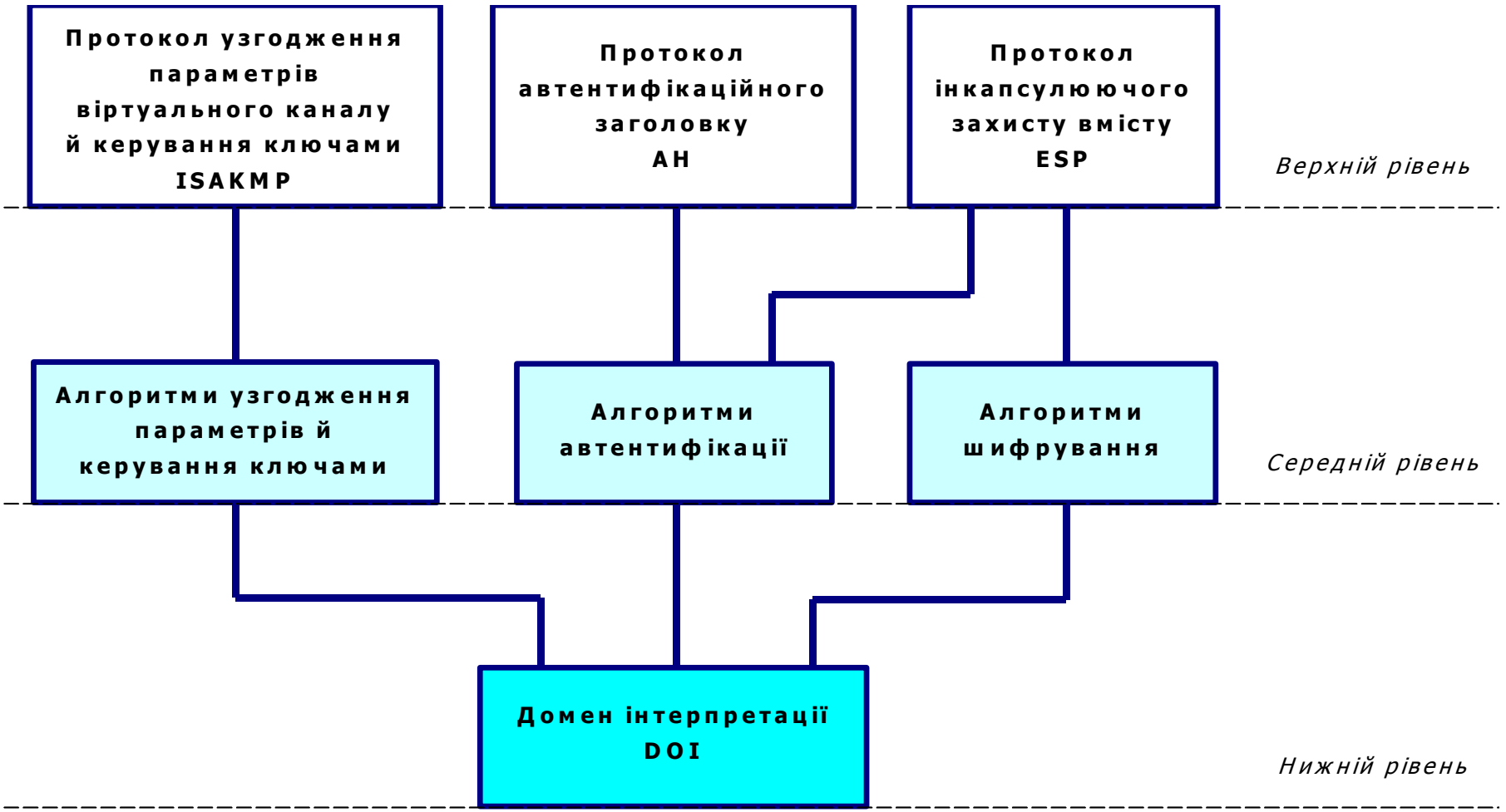
# Архітектура засобів захисту IPSec

- Технологія IPSec охоплює кілька абсолютно різних областей, в число яких входять:
  - шифрування,
  - автентифікація
  - керування ключами
- Відповідно до IPSec, архітектура засобів безпеки інформаційного обміну поділяється на три рівня
  - RFC-4301, Security Architecture for the Internet Protocol / S. Kent, K. Seo. – December 2005

# Рівні архітектури IPSec

- Верхній рівень – протоколи захисту віртуального каналу і узгодження параметрів захисту
  - Протоколи AH та ESP не залежать від конкретних алгоритмів шифрування й автентифікації. Можуть застосовуватись різні:
    - методи автентифікації
    - типи ключів
    - алгоритми шифрування та розподілу ключів
  - Протоколи AH та ESP зареєстровані організацією IANA (*Internet Address Naming Authority*) під номерами 51 та 50, відповідно
- Середній рівень – криптографічні алгоритми, що використовуються в протоколах AH та ESP, а також певні алгоритми узгодження і керування ключами, які використовує протокол ISAKMP
- Нижній рівень – так званий “домен інтерпретації” (*Domain of Interpretation*, *DOI*)
  - Це, фактично, база даних, яка містить інформацію про усі протоколи і алгоритми, що застосовуються в IPSec, а також про їхні параметри, ідентифікатори тощо
  - Наявність такої бази пояснюється тим, що відкрита архітектура IPSec припускає застосування протоколів і алгоритмів, які не розроблялись для неї чи з урахуванням її вимог
  - Необхідною умовою застосування сторонніх алгоритмів автентифікації або шифрування (наприклад, тих, що відповідають національним стандартам) є реєстрація їх у домені інтерпретації

# Архітектура засобів захисту IPSec



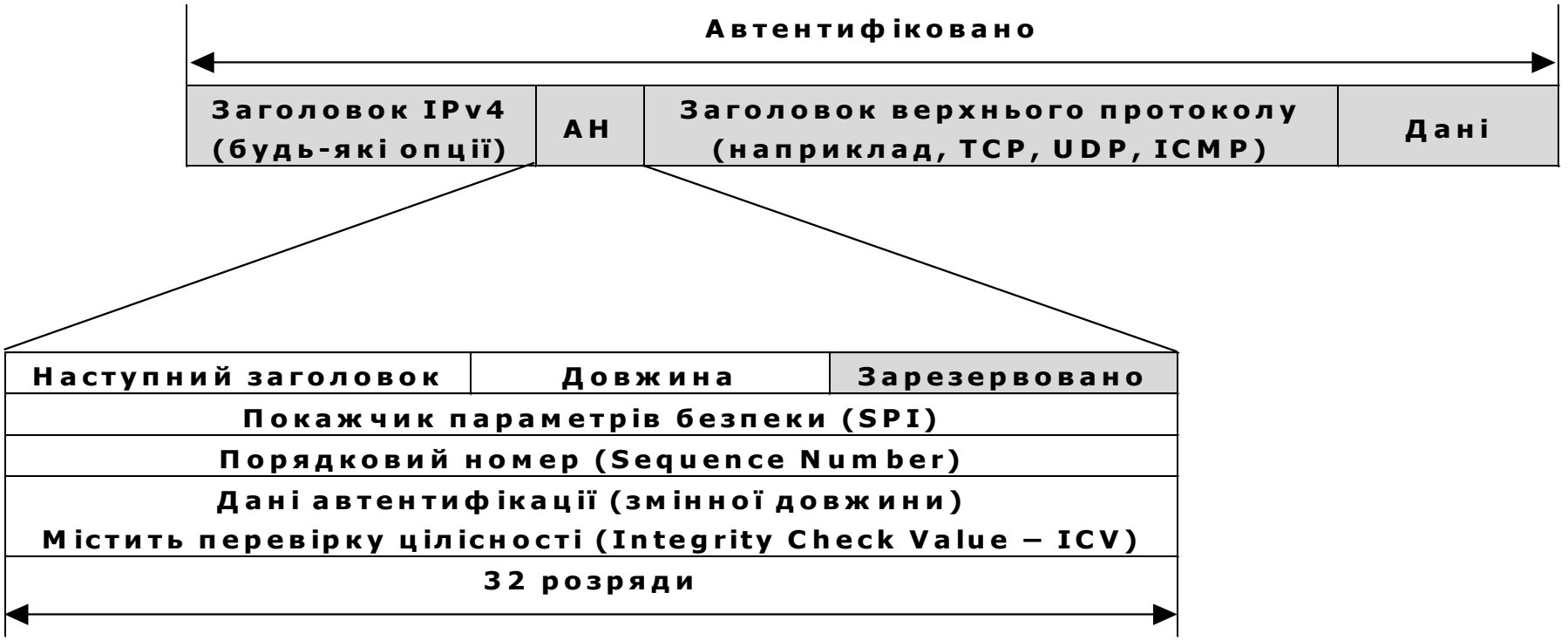
# Верхній рівень IPSec

- Протокол автентифікаційного заголовку (*Authentication Header*, AH)
  - RFC-4302, IP Authentication Header / S. Kent. – December 2005
  - Протокол AH передбачає
    - Автентифікацію джерела даних
    - Перевірку їхньої цілісності і справжності після одержання
    - Захист від нав'язування повторних повідомлень
- Протокол інкапсулюючого захисту вмісту (*Encapsulating Security Payload*, ESP)
  - RFC-4303, IP Encapsulating Security Payload (ESP) / S. Kent. – December 2005
  - Протокол ESP крім усіх функцій протоколу AH забезпечує ще й криптографічне закриття пакетів повідомлень
- Протокол узгодження параметрів віртуального каналу й керування ключами (англ. – Internet Security Association Key Management Protocol, ISAKMP)
  - RFC-4306, Internet Key Exchange (IKEv2) Protocol / C. Kaufman, Ed. – December 2005
  - Призначений для попереднього узгодження алгоритмів та їхніх параметрів сторонами, що взаємодіють за протоколами AH та ESP
  - Забезпечує створення сторонами, що взаємодіють, спільного контексту, елементи якого в подальшому вони можуть вільно використовувати.

# Асоціації захисту (SA)

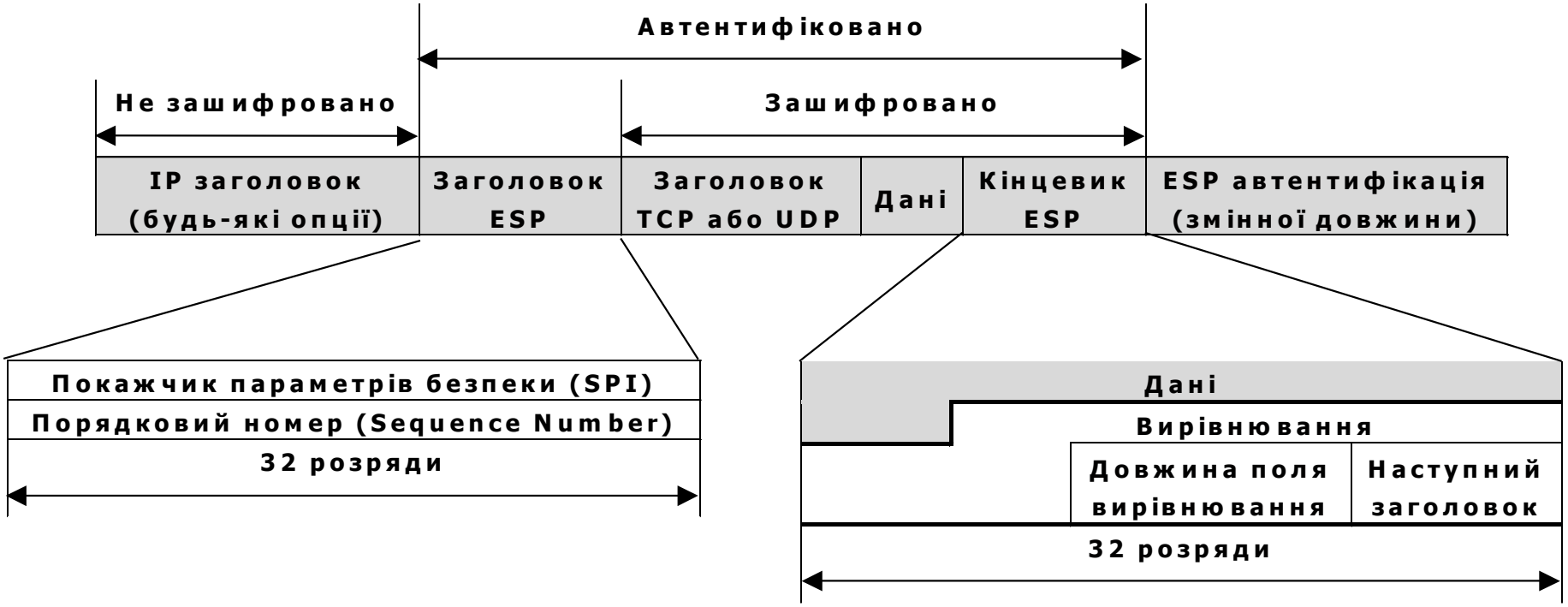
- Контекст, у якому взаємодіють сторони, що використовують технологію IPSec, визначають терміном “асоціація захисту” (*Security Association*, SA)
- Асоціація захисту функціонує на основі угоди, що складається сторонами
- Елементами асоціації захисту є
  - Учасники зв’язку: IP-адреси відправника й одержувача
  - Криптографічний алгоритм
  - Порядок обміну ключами
  - Розміри ключів
  - Термін дії ключів
  - Алгоритм автентифікації
- Асоціації захисту утворюються відповідно до протоколу ISAKMP

# Автентифікаційний заголовок (AH)




- Поле SPI (*Security Parameters Index*) – це “покажчик параметрів безпеки”
  - 32-розрядне число, що вказує на протоколи захисту, що використовуються
  - В це поле включені індекси алгоритмів і типи ключів
  - Фактично, воно визначає асоціацію захисту
- Порядковий номер (*Sequence Number*) – це ідентифікатор пакету, що забезпечує захист від повторного відправлення даних

# Протокол інкапсулюючого захисту (ESP)



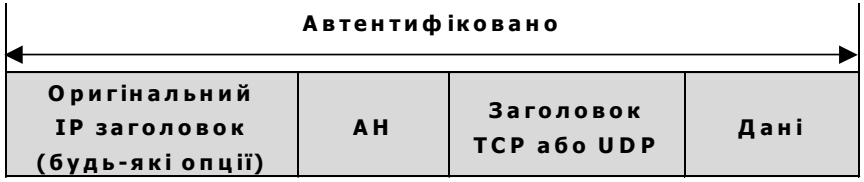
# Протокол інкапсулюючого захисту (ESP)

- Протокол ESP забезпечує шифрування IP-інформації на рівні пакетів
  - Передбачено використання різних алгоритмів шифрування
- Протокол ESP забезпечує автентифікацію даних із застосуванням різних алгоритмів автентифікації
- Слід звернути увагу на таке
  - Заголовок ESP розташований між заголовком IP та рештою вмісту пакета
  - Поля покажчика SPI та порядкового номера виконують ту ж функцію, що й у заголовку AH
  - Поле заголовку TCP (або UDP, або іншого протоколу), дані та кінцевик (трейлер) ESP зашифровані
  - Поле вирівнювання має змінну довжину в діапазоні 0-255 біт, і забезпечує, по-перше, що поле “Наступний заголовок” закінчується на межі 32-розрядного слова, а по-друге, що розмір зашифрованої частини кратний розміру блоку застосованого алгоритму шифрування
  - ESP забезпечує автентифікацію даних у тому ж порядку, що й AH

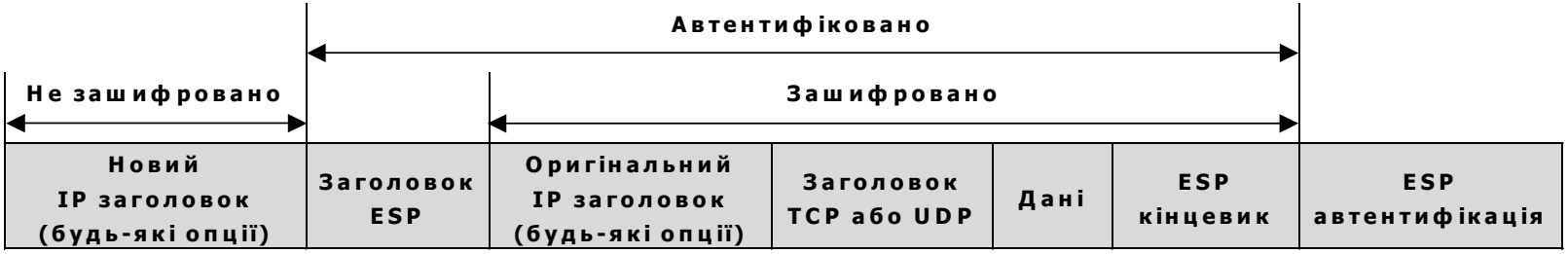
# Режим тунелювання та транспортний режим

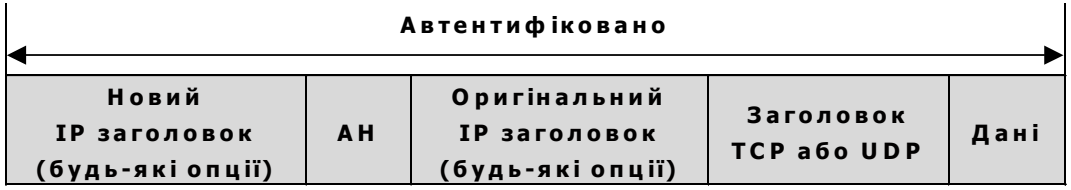
- Як для AH, так і для ESP існують два режими
- Транспортний режим (*Transport Mode*)
  - Призначений для забезпечення зв'язку між двома вузлами
  - Не передбачає інкапсуляції IP-пакета в інший пакет
  - У випадку прослуховування трафіка, зловмисник зможе прочитати справжні IP-адреси відправника й одержувача
- Режим тунелювання (*Tunnel Mode*)
  - Весь IP-пакет поміщається в поле даних пакета IPSec. Далі для пакета вказується нові IP-адреси відправника та одержувача, і додаються захисні заголовки та автентифікаційні трейлери
  - В новому заголовку адреси відправника й одержувача відрізняються від тих, що вказані у вихідному пакеті
  - Зловмисник, який перехопив пакет, не зможе встановити, які саме вузли спілкуються між собою
  - Заголовок ESP не шифрується, щоби вузол, що приймає повідомлення, мав змогу зрозуміти, що одержаний пакет є пакетом IPSec ESP
  - Вихідний IP-заголовок, дані TCP, інформація, яку передають, та кінцевик ESP шифруються. Ці елементи складають вміст поля даних зовнішнього пакета

# Транспортний режим


# Режим тунелювання



# Обмін ключами

- В IPSec застосовуються два способи передачі ключів:
- Вручну
  - Ключі вручну завантажуються у відповідні пристрої IPsec безпосередньо на об’єктах
  - Шифруванню ці ключі не піддаються, вони або передаються системному адміністратору особисто, або надсилаються через захищені канали
  - Введення ключів вручну виправдано лише у невеликій мережі
- Шляхом обміну через IP-мережу (*Internet Key Exchange, IKE*)
  - Коли масштаби мережі зростають, виникає потреба в механізмі створення асоціацій захисту за вимогою (SA on Demand)
  - За створення асоціацій захисту відповідає протокол ISAKMP, який описує базові технології, але не специфікує конкретні алгоритми
    - Для обміну ключами можуть застосовуватись окремі протоколи
    - Був обраний протокол Oakley, що використовує алгоритм Діффі-Хелмана
  - Поєднання протоколів ISAKMP та Oakley було відомо як специфікації ISAKMP/Oakley, тепер воно отримало назву протоколу IKE

# Протокол IKE

- Призначений для узгодження параметрів асоціацій захисту, що створюються, і для автентифікованого обміну ключами, якими будуть користуватись учасники цих асоціацій
- Дозволяє утворити між двома учасниками обміну (IKE SA) автентифікований захищений тунель, за яким будуть узгоджуватись параметри асоціації захисту, що створюється для IPSec
- Протокол на базі UDP, передбачає використання порту 500
- Може функціонувати у трьох режимах:
  - Основний режим (*Main Mode*)
    - Застосовується, коли дві сторони вперше встановили зв'язок, щоби узгодити параметри асоціації захисту, яка забезпечить конфіденційність їх подальшого обміну
  - "Активний" режим (*Aggressive Mode*)
    - Є скороченою версією основного режиму, має те ж призначення, що й основний режим, і може використовуватись замість нього
  - Швидкісний режим (*Quick Mode*)
    - Застосовується, коли асоціація захисту вже створена в результаті використання основного або активного режиму, але існує необхідність в узгодженні функцій захисту або обміну новими ключами
    - Оскільки захищений канал був утворений ще до застосування швидкісного режиму, останній забезпечує надійний захист без додаткових витрат, які притаманні основному або активному режиму

# Автентифікація у протоколі IKE

- Протокол IKE передбачає кілька способів автентифікації
  - Коли спільно використовуються одні й ті ж ключі
    - Всі хост-системи (або шлюзи VPN) володіють одними й тими ж таємними ключами
    - IKE автентифікує різних учасників обміну по гешу ключа
  - При використанні криптографії з відкритим ключем
    - Кожна сторона генерує випадкове число і шифрує його відкритим ключем іншої сторони
    - Автентифікація відбувається, коли інша сторона може розрахувати геш-функцію цього випадкового числа і надіслати результат першій стороні
  - Технології цифрового підпису
    - Кожний пристрій “підписує” набори даних, що відсилає іншій стороні
    - Цей метод подібний до шифрування відкритим ключем, але додатково забезпечує захист від відмовлення від авторства
- При використанні асиметричної криптографії (цифровий підпис, шифрування відкритим ключем), необхідно використання цифрових сертифікатів, що підтверджують взаємну відповідність і справжність відкритих та секретних ключів
  - Протокол IKE дозволяє отримати доступ до сертифікату в односторонньому порядку або у формі обміну при виконанні сторонами процедури IKE