Архітектура засобів захисту IPSec

План

- Рівні архітектури IPSec
- Асоціації захисту (SA)
- Автентифікаційний заголовок (Протокол AH)
- Протокол інкапсулюючого захисту (ESP)
- Транспортний та тунельний режими
- Протокол обміну ключами

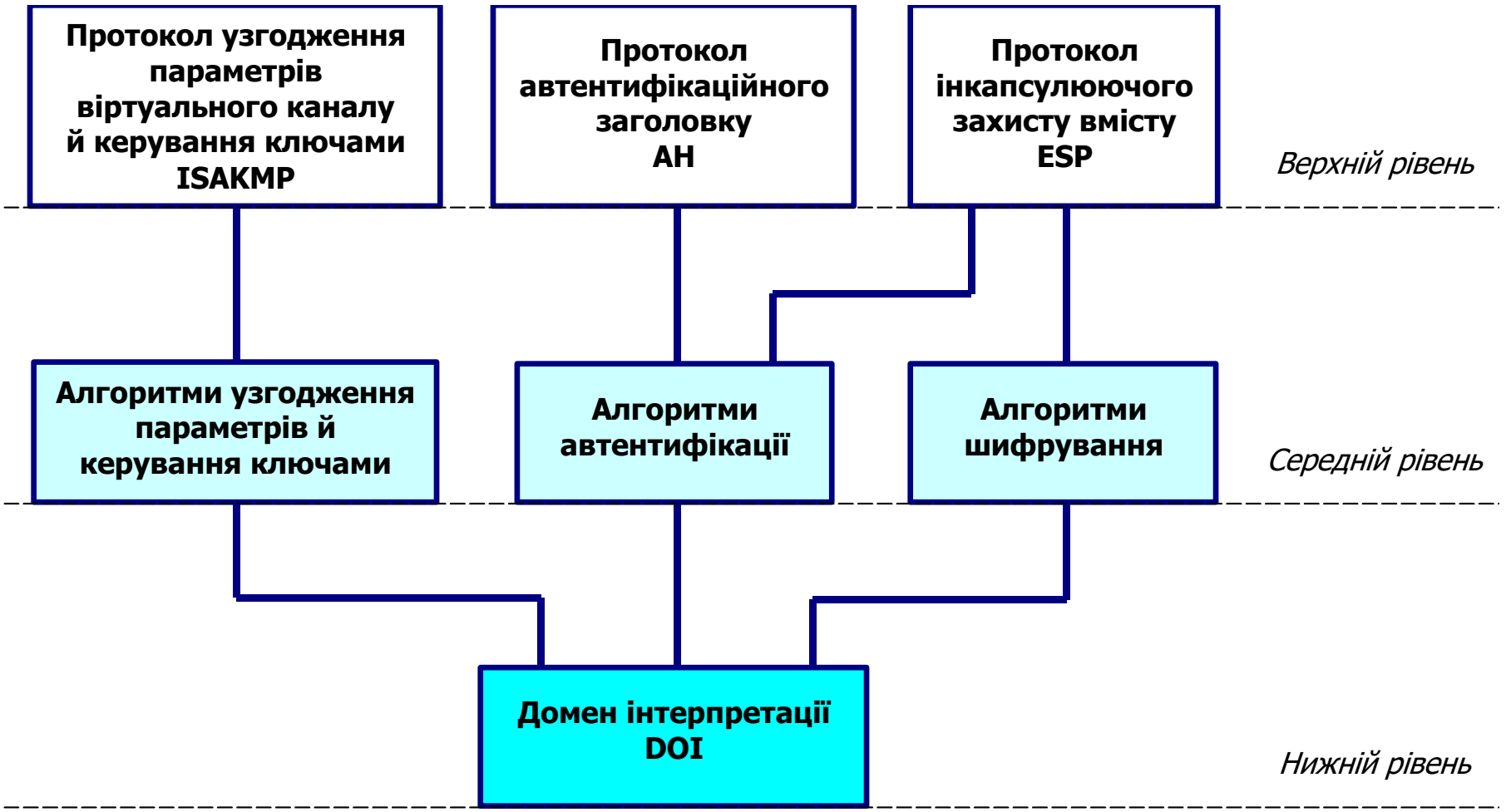
Архітектура засобів захисту IPSec

- 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



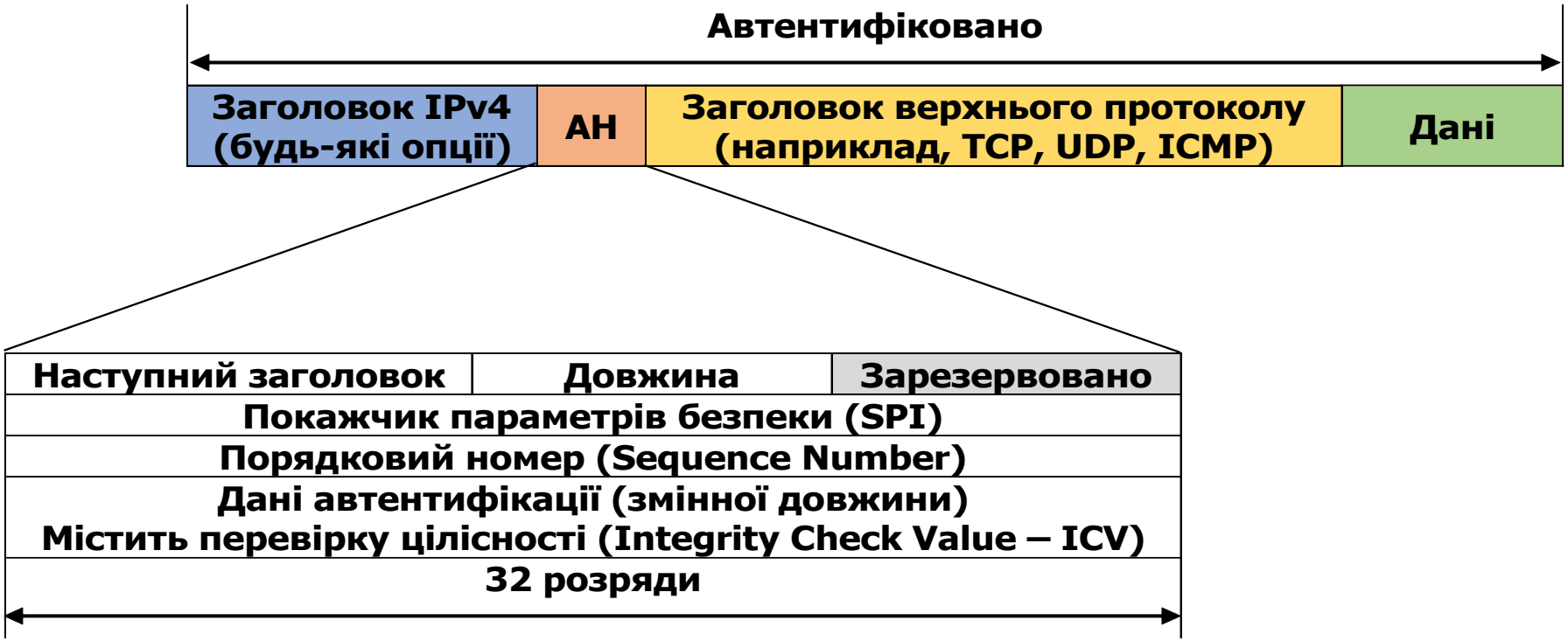
Верхній рівень IPSec

- 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)

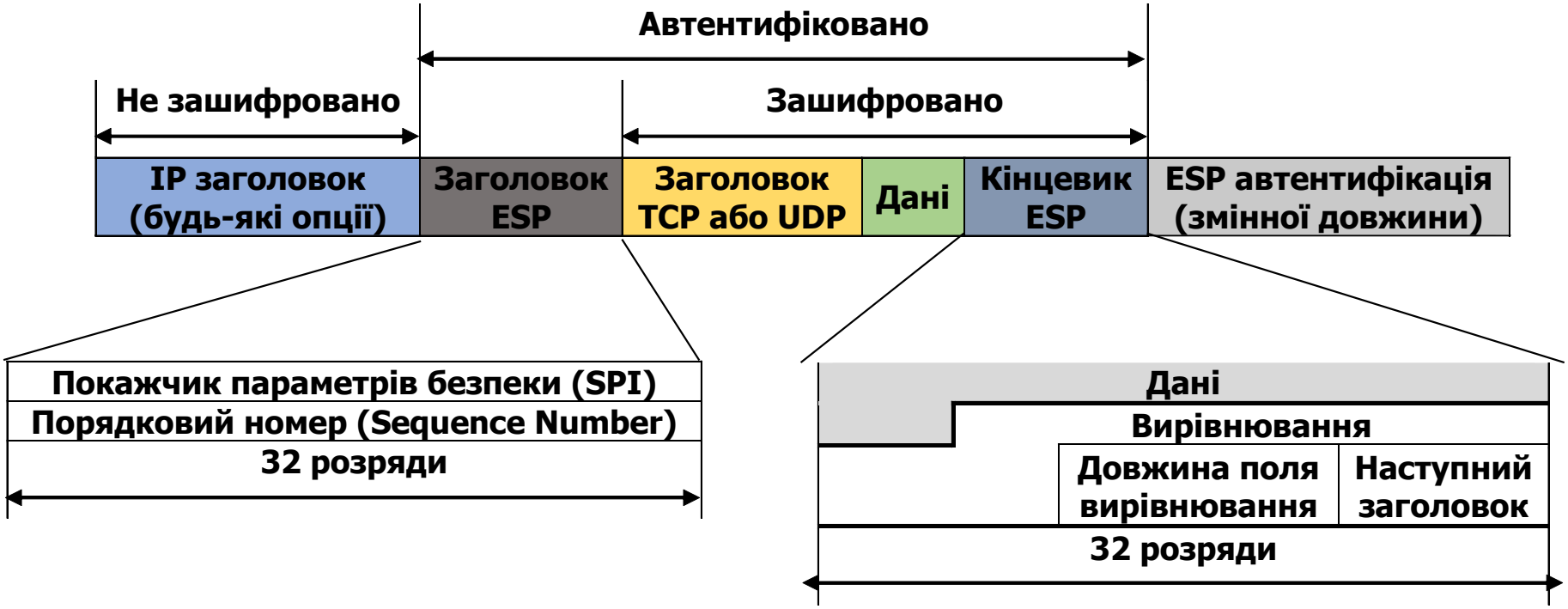
- Контекст, у якому взаємодіють сторони, що використовують технологію IPSec, визначають терміном “асоціація захисту” (*Security Association*, SA)
- Асоціація захисту функціонує на основі угоди, що складається сторонами
- Елементами асоціації захисту є
  - Учасники зв’язку: IP-адреси відправника й одержувача
  - 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)

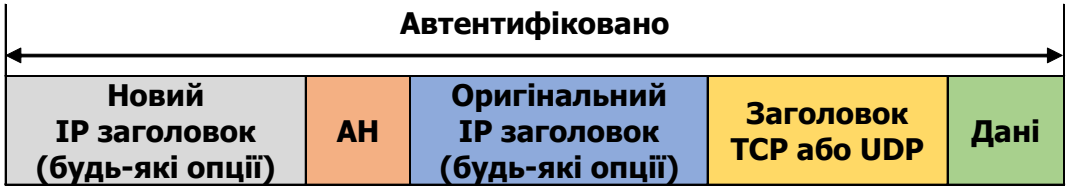
- Протокол ESP забезпечує шифрування IP-інформації на рівні пакетів
  - Передбачено використання різних алгоритмів шифрування
- Протокол ESP забезпечує автентифікацію даних із застосуванням різних алгоритмів автентифікації
- Слід звернути увагу на таке
  - Заголовок ESP розташований між заголовком IP 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

Транспортний та тунельний режими

- 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



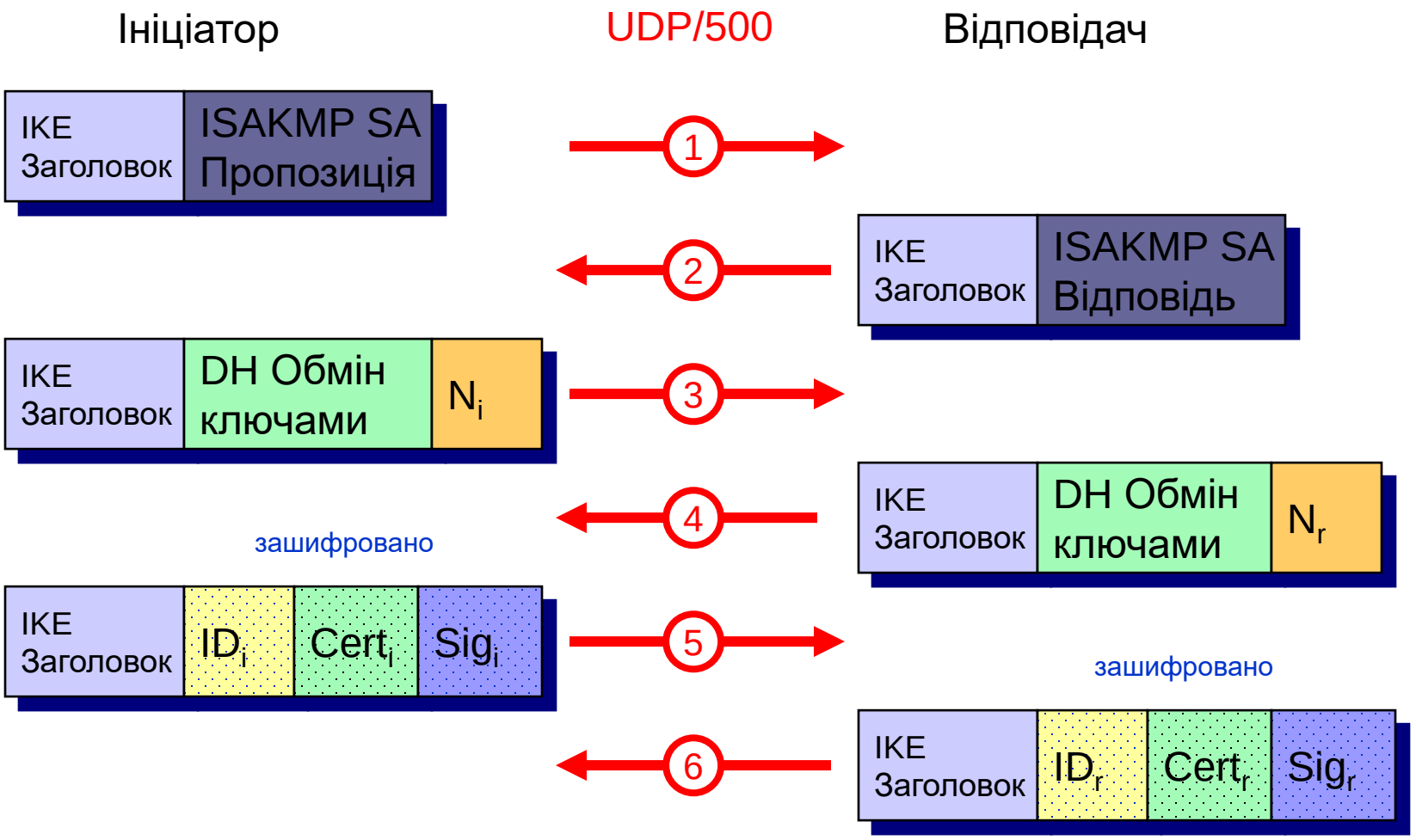
Обмін ключами

- 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

Internet Key Exchange – IKEv1 (Основний режим)



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