РОЗРОБКА ТА ДОСЛІДЖЕННЯ МЕРЕЖІ З ВИКОРИСТАННЯМ IPSEC ТЕХНОЛОГІЇ

канд. техн. наук, доц. М.В. Мезенцев, магістр Є.Р. Шпортько
Національний технічний університет "Харківський політехнічний інститут", м. Харків

У сучасному світі скрізь використовуються різні VPN-технології. Деякі (наприклад, PPTP) з часом визнаються небезпечними і поступово відмирають, інші (OpenVPN), навпаки, з кожним роком нарощують оберти. Але незмінним лідером і найбільш пізнаваною технологією для створення і підтримки захищених приватних каналів як і раніше залишається IPsec VPN [1].

Технологія IPSec була розроблена для підвищення безпеки IP протоколу. Це досягається за рахунок додаткових протоколів, що додають до IP-пакету власні заголовки. При цьому специфічним для IPsec є те, що вона реалізується на мережевому рівні, доповнюючи його таким чином, щоб для наступних рівнів все відбувалося непомітно. Весь процес встановлення з'єднання включає дві фази: перша фаза застосовується для того, щоб забезпечити безпечний обмін ISAKMP-повідомленнями вже в другій фазі. ISAKMP (Internet Security Association and Key Management Protocol) – це протокол, який служить для узгодження і поновлення політик безпеки (SA) між учасниками VPN-з'єднання. У цих політиках якраз і вказано, за допомогою якого протоколу шифрувати (AES або 3DES) і за допомогою чого аутентифікувати (SHA або MD5).

В роботі розроблена модель мережі в пакеті GNS3 [2] для аналізу роботи VPN з використанням IPSec. Проведено дослідження розробленої мережі та зроблено висновок про вибір найбільш підходящої реалізації IPSec з точки зору безпеки та швидкодії.

Список літератури: 1. IPSec – протокол защиты сетевого трафика на IP-уровне [Електронний ресурс]. – Режим доступу: https://www.ixbt.com/comm/ipsecure.shtml.