

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАТИКА, МАТЕМАТИКА,
АВТОМАТИКА

ІМА :: 2017

**МАТЕРІАЛИ
та програма**

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 17–21 квітня 2017 року)



Суми
Сумський державний університет
2017

Мережева безпека на основі протоколів IPsec і SSL VPN

Павленко Є.Р., студент; Великодний Д.В., старший викладач
Сумський державний університет, м. Суми

Історично склалося, що багатьом організаціям важко знайти вдале співвідношення між ступенем захисту інформації в комп'ютерній мережі і витратами, що необхідно здійснити на підтримку такого захисту. Для вирішення проблеми захисту, на сьогодні існує велика кількість можливих рішень. Найактуальнішими серед них є стек протоколів IPsec та SSL VPN. Кожен з них зайняв свою нішу, та має високу популярність у своєму сегменті.

Технологію IPsec використовують для створення захищеної мережі середніх на великих компаній. Вона дозволяє безпечно передавати будь які повідомлення через IP-протокол на мережевому рівні.

Для дослідження протоколу IPsec використовувався мережевий емулятор GNS3. Модель комп'ютерної мережі являла собою поєднання, за допомогою маршрутизаторів, двох окремих офісів на комп'ютерах яких був налаштований чат. Оскільки клієнтська чат-програма передавала повідомлення без шифрування, то перехоплення пакетів за допомогою WireShark відкривало можливість повного аналізу та обробки незахищеної інформації. Після налаштування IPsec перехоплені повідомлення прочитати було не можливо.

SSL VPN найчастіше використовують для захищеного з'єднання з веб-клієнтом. SSL VPN створює захищене сесійне з'єднання, що дозволяє не турбуватися про важливу, конфіденційну інформацію.

Практична реалізація та дослідження проводилися за допомогою стимулятора Cisco Packet Tracer 7.0. Роль мережевого екрану виконував Cisco ASA. Було створено декілька груп користувачів з обмеженням доступу на певні веб-сайти. Доступ до інформації можна було отримати лише після успішної авторизації на Cisco ASA завдяки встановленню безпечного з'єднання https, що фактично і є SSL VPN.

Отже, на сьогодні безпечна передача даних є надзвичайно важливою задачею. Проте існує багато методів вирішення цієї проблеми. Знання особливостей таких методів дозволить ефективно використовувати їх у залежності від поставленої задачі.