УДК 621.326
Климчук Г. – ст. гр. ПКмпз-61
Тернопільський державний технічний університет імені Івана Пулюя

КОРПОРАТИВНА МЕРЕЖА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Науковий керівник: к.т.н., доцент Березовська І.Б.

На сучасному етапі розвитку інформаційних систем та в умовах, коли філіали одного підприємства знаходяться на відстані один від одного, потреба в оперативному і надійному обміні інформацією стала найгострішою, оскільки принцип побудови Internet не забезпечує надійного захисту від проникнення зловмисників в корпоративні мережі і відкриває можливості для крадіжки або навмисного спотворення інформації. Як наслідок, компанія може зазнати суттєвих збитків від втрати цінної інформації. Ефективно ж вирішити завдання, пов'язані з циркуляцією конфіденційної інформації по каналах зв'язку, дозволяє технологія віртуальних приватних мереж (VPN).

VPN - це метод підключення до приватної мережі (наприклад, офісної мережі) за допомогою загальнодоступної мережі (наприклад, Інтернету). Підключення VPN через Інтернет працює як канал глобальної мережі (WAN).

В основі концепції побудови захищених віртуальних приватних мереж лежить проста ідея: якщо в глобальній мережі є два вузли, між якими здійснюється обмін інформацією, то для забезпечення передачі конфіденційної і цілісної інформації по відкритій мережі, “прокладаємо” між цими вузлами віртуальний тунель, щоб унеможливити доступ усім можливим активним і пасивним зовнішнім спостерігачам. При цьому передача даних здійснюється по захищеному каналі (secure channel), який будується за допомогою системних засобів, реалізованих на різних рівнях еталонної моделі взаємодії відкритих систем (OSI).

Від вибраного рівня OSI багато в чому залежить функціональність реалізовуваної VPN і її сумісність з програмами інформаційної системи, а також з іншими засобами захисту. По ознаках робочого рівня моделі OSI розрізняють наступні групи VPN:

– VPN другого (канального) рівня;
– VPN третього (мережного) рівня;
– VPN п'ятого (сеансового) рівня.

За видом технічної реалізації розрізнюють такі групи VPN:

– VPN на основі мережної операційної системи;
– VPN на основі міжмережних екранів;
– VPN на основі маршрутизаторів;
– VPN на основі програмних рішень;
– VPN на основі спеціалізованих апаратних засобів з вбудованими апаратними засобами криптографічних перетворень.

Переваги, отримані компанією при формуванні захищених віртуальних тунелів, на відміну від використання швидкісних каналів зв'язку, полягають, перш за все, в значній економії коштів. Крім того концепція захищених віртуальних приватних мереж дозволяє організовувати необхідний обмін інформацією всередині компанії і з віддаленими користувачами та клієнтами при найкращому поєднанні продуктивності, оперативності, захищеності і вартості. Відтак такі технології, як VPN, з урахуванням всіх їх переваг, надалі будуть активно розвиватися, удосконалюватися і набувати все більш масового характеру.