УДК 681.3:614.842.86

Т.В. Рак, Я.С. Парамуд
Національний університет “Львівська політехніка,
кафедра ЕОМ

ЗАСТОСУВАННЯ ВІРТУАЛЬНИХ МЕРЕЖ В ПОЖЕЖНІЙ ОХОРОНІ

Розглянуто віртуальні приватні мережі (VPN) та їх застосування в пожежній охороні для побудови комп’ютеризованої системи управління (КСУ ПО). Показано, що VPN є одним з найефективніших рішень для побудови КСУ за критерієм "мінімальна вартість – достатня якість".

In this article are considered virtual private networks and probability of using of them in fire service for computer dispatch systems. Is shown that the virtual private networks are one of the optimal decision for development of the computer dispatch systems proceeding from criterion "low price – allowable quality".

Сьогодні в Україні актуальним є створення комп’ютеризованої системи управління пожежною охороною. Основні задачі, які розв'язуються в службі пожежної охорони за допомогою КСУ, можна умовно розділити на такі групи [4, 6]: управління адміністративно-господарською діяльністю; управління профілактичною роботою; оперативне управління силами і засобами пожежної охорони.

Однією з проблем при створенні КСУ є мінімізація затрат на розробку, впровадження та експлуатацію цієї системи при заданому рівні функціональних можливостей. Для зменшення витрат при створенні системи можна звернутись до вже готових продуктів та технологій, використати раніше створену базу. За структурним складом в кожному обласному управлінні пожежної охорони функціонує ЦААСЗ – центр автоматизованих агрегатизованих систем зв’язку, який призначений для забезпечення автоматизації розв'язування задач управління та прийняття рішень, розв'язування задач в оперативно-тактичній, профілактичній, наглядовій та адміністративно-господарській галузях роботи пожежної охорони [2, 3], створені локальні комп’ютерні мережі. Використовується електронна пошта на базі програмного пакета ASTRA, який призначений для передавання файлів між комп'ютерами телефонними лініями зв'язку в автоматичному режимі між підрозділами пожежної охорони в межах країни [5]. Практично у всіх обласних управліннях є підключення до Internet по комутованих лініях зв’язку, а в багатьох інших пожежних підрозділах виділеними телефонними лініями.

У другій половині 90-х років з'явилося декілька близьких за методами реалізації технічних рішень, які можуть бути використані для створення КСУ ПО. Вони об'єднані однією назвою VPN (Virtual Private Networks). Всі ці рішення зводяться до забезпечення інформаційної безпеки в корпоративних мережах, побудованих на принципах Інтернет-технологій.

Поява віртуальних мереж обумовлена певними причинами, зокрема вимогами сучасної економіки, яка припускає наявність географічно розподілених підприємств і відповідної їм інформаційної інфраструктури. VPN – черговий крок на цьому шляху, вони покликані замінити більш дорогі і менш надійні технології організації розподілених систем, що використовують виділені лінії, модемні пули, технологію Frame Relay та ін.

Побудова корпоративних інформаційних систем з використанням VPN має сенс як з фінансової, так і з експлуатаційної точки зору. Впроваджуючи VPN для передачі конфіденційної інформації, підприємство чи організація заощаджує значні засоби, оскільки може відмовитися від невластивих йому комунікаційних функцій, передати їх компаніям, що надають послуги зв'язку (ISP – сервіс-провайдерам Internet). Тим самим воно відмовляється від непрофільної для себе діяльності, відпадає необхідність у наявності власної комунікаційної апаратури, сервісної служби тощо. Треба врахувати, що професійне обслуговування не тільки знижує витрати на експлуатацію, але й підвищує якість послуг та їхню надійність, що підтверджується широко відомими прикладами, коли передача даних через Інтернет виявлялася більш надійною, ніж спеціалізовані мережеві рішення. Так було, наприклад, з американськими системами передачі даних під час війни в Перській затоці.

Про те, які реальні вигоди обіцяють VPN, можна судити за матеріалами аналітичної компанії Forrester Research. Вона порівняла річні витрати при використанні виділеного сервера віддаленого доступу Remote Access Server (RAS) і VPN (таблиця) [8]. Виявилося, що сумарні витрати з використанням VPN у 2,5 разів менші порівняно із використанням технології RAS.

Ці та багато інших фактів, що підтверджують економічну ефективність нової технології, стимулюють підприємства до якнайшвидшого впровадження VPN. Про те, наскільки VPN виявилися привабливими, свідчать дані ще декількох аналітиків ринку. Так, компанія Infonetics Research вважає, що в 2001 р. більше 70 % компаній, що використовують Інтернет у корпоративних цілях, перейдуть на VPN. Інший відомий аналітик – Gartner Group – прогнозує, що кількість таких фірм досягне 90 % до 2002 р. [8].

Річні витрати компаній при використанні технологій RAS і VPN з розрахунку на 1000 користувачів, млн. дол.

Затрати	**RAS**	**VPN**
Оплата послуг провайдерів	1,08	0,54
Витрати на експлуатацію	0,30	0,30
Капіталовкладення	0,10	0,02
Інші витрати	0,02	0,03
Разом	1,50	0,59

Усе це, разом узяте, дало змогу Міжнародній асоціації комп'ютерної безпеки (International Computer Security Association) в одному з останніх звітів стверджувати, що VPN входить у кращу десятку тих продуктів, які компанії мають намір придбати найближчим часом.

В основу віртуальних мереж усіх модифікацій покладено ідею використання відкритих каналів для передачі закодованої конфіденційної інформації так званими віртуальними тунелями. VPN можна порівняти зі звичайними захисними екранами. Функції екранів полягають у тому, щоби відбивати неавторизований трафік і передавати через тунель тільки авторизований. У VPN роль зовнішніх стінок тунелю виконують додаткові оболонки, усередину яких інкапсулюються вихідні передані пакети. Ці вторинні пакети і роблять безпечною “подорож” мережею. Кожен тунель має входи і виходи. Вхідними порталами тунелів є шлюзи вузлів, що входять до VPN, вони обробляють вхідні і вихідні пакети. У результаті поза віртуальною мережею можна бачити тільки входи і виходи тунелю і циркулюючі між ними захищені пакети. Звичайно говорять, що тунель поділяє простір на захищену (червону) і незахищену (чорну) зону.

Тунель може складатися з декількох оболонок, їх кількість залежить від конкретної реалізації VPN. Внутрішня оболонка утворюється засобами криптозахисту, вся інформація внутрішніх пакетів (основна і допоміжна) кодується відповідно до прийнятого в даній VPN алгоритму.

Типи VPN. Найпростіше класифікувати віртуальні мережі залежно від їхньої конфігурації, виділяючи три елементарні типи [9]:

- інтранет-VPN для організації взаємодії між підрозділами усередині підприємства або між групою підприємств, об'єднаних корпоративними зв'язками;
- Internet-VPN для забезпечення віддаленого доступу мобільним клієнтам;
- екстранет-VPN для зв'язку зі стратегічними партнерами, користувачами і постачальниками.

Ще можна класифікувати VPN за способами реалізації на базі:

- спеціалізованих пристроїв, що працюють під керуванням систем реального часу й апаратних засобів, що використовуються для криптографічної підтримки;
- чисто програмних рішень на універсальних апаратних платформах, звичайних ПК або Unix-станціях;
- гібридів, де додатки VPN працюють на стандартних комп'ютерах, але з використанням додаткових криптографічних процесорів;
- захисних екранів і маршрутизаторів, яким можуть бути додані додаткові функції, що забезпечують VPN.

Основні функції VPN. Незалежно від реалізації віртуальна мережа виконує три основні комунікаційні функції [9]:

1. Ідентифікація (Authentication). Для того, щоб “відкрити” тунель, шлюз, що приймає, повинен розпізнати вхідне повідомлення як своє. Він робить це на підставі перевірки ряду вкладених секретних ознак.

2. Інкапсуляція (Encapsulation). Після того, як тунель відкритий, за прийнятим в даній мережі протоколом починається обмін захищеними пакетами з вкладеннями.

3. Шифрування (Encryption). Вкладені пакети кодуються за прийнятими у мережі правилами.

VPN створюється між ініціатором тунелю і термінатором тунелю. Звичайна маршрутизована мережа IP (вона не обов'язково містить загальнодоступну мережу Internet) визначає маршрут між ініціатором і термінатором. Ініціатор тунелю інкапсулює пакети в новий пакет, що містить поряд з вихідними даними новий заголовок з інформацією про відправника й одержувача. Хоча всі передані тунелем пакети є пакетами IP, у принципі інкапсульовані пакети можуть належати до протоколу будь-якого типу, включаючи пакети немаршрутизованих протоколів, – таких, як NetBEUI. Термінатор тунелю виконує процес, зворотний інкапсуляції, видаляючи нові заголовки і направляючи вихідний пакет у локальний стек протоколів або адресата в локальній мережі.

Сама по собі інкапсуляція ніяк не підвищує конфіденційності або цілісності даних. Конфіденційність забезпечується за допомогою шифрування. Оскільки методів шифрування даних існує безліч, дуже важливо, щоб ініціатор і термінатор тунелю використовували той самий метод. Крім того, для успішного дешифрування даних вони повинні мати можливість обміну ключами. Щоби тунелі створювалися тільки між уповноваженими користувачами, кінцеві точки потрібно ідентифікувати. Цілісність даних можна забезпечити за допомогою певної форми вибірки повідомлення для виявлення змін або видалень.

Безліч альтернативних підходів до організації VPN можна розрізняти залежно від того, протокол якого рівня відповідно до моделі відкритих систем OSI використовується.

Для реалізації уніфікованого способу інкапсуляції трафіка третього рівня (і більш високих рівнів) на клієнтах і серверах Windows розроблено тунельний протокол між двома точками (Point-to-Point Tunneling Protocol, PPTP), що являє собою розширення протоколу PPP. У PPTP не специфікується конкретний метод шифрування.

Для пересилання на другому рівні моделі OSI розроблено протокол L2F (Layer-2 Forwarding), за допомогою якого віддалені клієнти можуть зв'язатися каналами провайдера Internet і бути ідентифікованими. При цьому ISP не потрібно здійснювати конфігурацію адрес і виконувати ідентифікацію.

Ці тісно зв'язані один з одним протоколи в 1996 р. вирішили об'єднати. Результуючий протокол називається протоколом тунелювання другого рівня (Layer-2 Tunneling Protocol, L2TP) [7, 9]. Як і попередні протоколи другого рівня, специфікація L2TP не описує методи ідентифікації і шифрування.

Специфікацією, де описані стандартні методи для всіх компонентів VPN, є протокол Internet Protocol Security, або IPSec (іноді його називають тунелюванням третього рівня - Layer-3 Tunneling) [7, 9]. IPSec передбачає стандартні методи ідентифікації користувачів або комп'ютерів при ініціації тунелю, стандартні способи використання шифрування кінцевими точками тунелю, а також стандартні методи обміну і керування ключами шифрування між кінцевими точками.

Деякі постачальники VPN використовують інший підхід за назвою "посередники каналів" (circuit proxy), або VPN п'ятого рівня. Цей метод функціонує над транспортним рівнем і ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet для кожного сокета окремо. (Сокет IP ідентифікується комбінацією TCP-з'єднання і конкретного порту або заданим портом UDP.)

Наведені особливості технології VPN можна легко використати як основу для побудови КСУ пожежною охороною. Підрозділи служби пожежної охорони є значно розкидані територіально. Для того, щоб об'єднати їх загальною спільною мережею, можна використати виділені телефонні лінії між підрозділами або технологію RAS через комутовані лінії зв'язку. Перший варіант є дорогим через відносно високу вартість прокладання і оренди виділених ліній зв'язку між всіма підрозділами. Другий варіант є відносно дешевшим, але не забезпечує необхідної надійності та оперативності. В обох випадках виникають значні труднощі при підключенні абонентів, які знаходяться в різних населених пунктах.

Поряд з цими варіантами технологія VPN має такі переваги. По-перше, відпадає необхідність прокладання додаткових ліній зв'язку, що веде до значної економії коштів. По-друге, забезпечується підключення абонентів, які знаходяться в різних населених пунктах. По-третє, паралельно можна використовувати можливості мережі Internet. Зрозуміло, що кожен абонент повинен мати надійне підключення до Internet.

Технології VPN застосовуються для вирішення завдань керування адміністративно-господарською діяльністю та профілактичною роботою, які вимагають створення розподілених баз даних та значного документообігу. При вирішенні цих задач основним є забезпечення надійних та захищених каналів зв’язку. Для цього можуть використовуватись VPN на основі програмних рішень на універсальних апаратних платформах, звичайно ПК

або Unix-станціях. При вирішенні третьої задачі – оперативного управління силами і засобами пожежної охорони – критичними є швидкість і надійність зв’язку.

Як видно з вищесказаного, технології VPN в першу чергу орієнтуються на захист інформації. Однак багато останніх розробок в області технологій VPN були спрямовані на вирішення питань продуктивності. Зусилля сюди спрямували і ISP, і виробники. Наприклад, послуга ConcentricQOS компанії Concentric Networks передбачає 100-процентну гарантію доступності мережі для замовника і гарантію, що максимальна затримка для з'єднання VPN не буде перевищувати 80 мс [1]. VPN Advantage компанії GTE Internetworking передбачає окремі угоди для виділеного і віддаленого доступу. У випадку виділеного доступу компанія надає 99,9-процентну гарантію доступності і гарантію, що максимальна затримка не буде перевищувати 125 мс [1]. У випадку віддаленого доступу сигнал «вільно» буде доступний у 97 % випадків при мінімальній швидкості з'єднання по модему 26,4 Кбіт/с [1]. Оскільки в моменти надходження викликів про пожежу між пожежними підрозділами передається незначна кількість інформації (адреса, назва об'єкта, маршрут руху тощо – до декількох сотень Кбайт, решта інформації може бути отримана в момент руху до місця або в процесі роботи на пожежі, при цьому затримка в декілька секунд не є критичною), то вказаної швидкості встановлення зв'язку та передачі інформації при використанні технологій VPN буде достатньо для вирішення завдань оперативного керування. При цьому для забезпечення надійності та швидкості при вирішенні завдань оперативного керування на обласному рівні необхідно, щоб кожна пожежна частина мала надійний доступ до Internet за виділеними лініями зв'язку або радіоканалами. Наведені матеріали показують, що застосування VPN дозволяє вирішувати значну частину задач КСУ ПО, забезпечуючи при цьому досить високу якість її функціонування.

Переважна більшість провайдерів Internet в Україні підтримують протокол PPTP і IPSec і забезпечують послуги VPN. Тому на сучасному етапі застосування технологій VPN є одним з найефективніших варіантів для застосування при побудові КСУ пожежної охорони, при якому досягається значна економія коштів на впровадження та експлуатацію і забезпечується достатня якість виконання всього переліку функціональних задач, які ставляться перед КСУ. Отже, застосування VPN для побудови КСУ ПО може забезпечити високу ефективність розв‘язання функціональних задач за критерієм "мінімальна вартість - достатня якість".

1. Кларк Е. Виртуальные частные сети, версия 2.0 // Журн. сетевых решений. 1999. – № 12. 2. Наріжний В. ЦААСЗ – мозок управління пожежною охороною./ Пожежна безпека. 2000. № 2. – С. 16-17. 3. Настанова по службі зв’язку і АСУ пожежної охорони України. 4. Рак Т. Особливості побудови комп’ютеризованої системи управління регіональною пожежною охороною / Вісн. НУ “Львівська політехніка”. 1997, – № 322. 5. Скомарський В. Зв’язок в Державній пожежній охороні МВС України та перспективи його розвитку // Пожежна безпека. 1997. – № 6. – С. 9–10 6. Скомарський В. Інформаційно-керуюча система пожежної безпеки України. // Пожежна безпека. 1997. № 4. – С. 9-11. 7. Хендерсон Т. Частные виртуальные сети становятся реальностью // Журн. сетевых решений. 1998. – № 6. 8. Черняк Л. VPN – первое знакомство // Net Week. 2000. – № 9. 9. Штайнке С. VPN между локальными сетями // Журн. сетевых решений. 1998. – № 10.