УДК 004.375

О. Ф. ЛАНОВИЙ,
кандидат технічних наук
начальник кафедри інформаційних систем і технологій в діяльності ОВС
Харківського національного університету внутрішніх справ.
І. В. КОБЗЕВ,
кандидат технічних наук, доцент
доцент кафедри інформаційних систем і технологій в діяльності ОВС
Харківського національного університету внутрішніх справ.
О. І. ПЕТРОВА,
кандидат фізико-математичних наук, доцент
доцент кафедри фізики
Харківського національного аерокосмічного університету «ХАІ»

ВИКОРИСТАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЛЯ ДИСТАНЦІЙНОЇ ОСВІТИ ДЕРЖАВНИХ СЛУЖБОВЦІВ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ

Однією з найважливіших проблем функціонування системи державного управління Україні є підвищення ефективності системи підготовки кадрів та підвищення кваліфікації персоналу у сфері державного і муніципального управління. Одним із шляхів розв'язання цієї проблеми є використання системи заочного навчання.

Класична заочна освіта з самого початку свого існування включала дистанційне навчання, тому що основну частину навчального часу слухач-заочник проводить на великій відстані від викладача. Основними засобами комунікації між слухачем і викладачем є письмові матеріали незалежно від форми носія (папір, магнітні диски тощо) або електронні засоби зв'язку (телефон, електронна пошта, інтернет тощо).

Дистанційне навчання (distance education, e-learning) як інновація прийшло на український ринок навчальних послуг декілька років тому і до сьогодні не має законодовчо-нормативного визначення. Протягом цього часу тривали активні дискусії стосовно стратегії, перспективності та можливості впровадження e-learning в освітню сферу України.

Зараз виділяють два шляхи впровадження дистанційних технологій:

1) впровадження розподілених дистанційних технологій у навчальний процес існуючих навчальних закладів;

2) створення віртуальних навчальних закладів із використанням нових комунікаційних й інформаційних технологій (віртуальних університетів, коледжів і гімназій).

Традиційна технологія заочної освіти без використання досягнень у галузі інформаційних і телекомунікаційних технологій не є достатньо ефективною. Без застосування сучасних інформаційних і телекомунікаційних технологій неможливо забезпечити в процесі підготовки фахівця такі інноваційні складові процесу навчання, як:

– інтерактивна взаємодія у діалоговому режимі між викладачем і слухачем, а також між студентами;

– швидка доставка студентові навчальних матеріалів в електронному вигляді;

– оперативний доступ до баз даних та знань, розміщених на сайті навчального закладу;

– тестування знань слухачів у дистанційному режимі.

При використанні вищеперелічених технологій у процесі підготовки державних службовців із використанням заочної форми навчання студенти мають бути забезпечені можливістю доступу до ресурсів вузу в режимі реального часу шляхом

асинхронної комунікації за допомогою різних інформаційно-технічних засобів: телефон, електронна пошта, програмні засоби взаємодії в середовищі www-серверів, комп'ютерний відео конференц-зв'язок тощо. Крім того, в процесі взаємодії слухача з освітніми ресурсами має бути забезпечено безумовне дотримання законодавства в галузі авторських прав, тобто рівень безпеки каналу передачі інформації повинен бути достатньо високим.

VPN – основа телекомунікаційної мережі. Найраціональніше використовувати для організації обміну інформацією з видаленим комп'ютером слухача віртуальні приватні мережі (VPN).

Віртуальна приватна мережа (VPN) – це логічна мережа, що створюється поверх іншої мережі, наприклад, інтернет. Незважаючи на те, що комунікації відбуваються через публічні мережі з використанням незахищених протоколів, за рахунок шифрування створюються закриті від сторонніх канали обміну інформацією. VPN дозволяє об'єднати декілька філіалів організації в єдину мережу з використанням непідконтрольних їй каналів зв'язку.

VPN використовується для організації прямого, безпечного з'єднання через загальнодоступний інтернет між клієнтами або між двома локальними обчислювальними мережами (ЛОМ). Завдяки VPN віддалені слухачі можуть звертатися до серверів навчальних закладів [1].

Для VPN не потрібні виділені лінії, тому користуватися нею може кожен, хто має в своєму розпорядженні доступ до інтернету. Після того, як з'єднання встановлене, слухачам може надаватися доступ до всіх ресурсів мережі – так, ніби вони були присутні в аудиторії. Найбільша перевага цієї технології полягає в тому, що, незважаючи на загальнодоступну інфраструктуру, пряме з'єднання VPN, яке іноді називають «тунелем», захищено настільки надійно, що вкрасти дані або дістати несанкціонований доступ до територіально-розподіленої мережі стає дуже важко.

Мережі VPN мають ряд економічних переваг перед іншими методами дистанційного доступу. Користувачі VPN мають можливість звертатися до корпоративної мережі, не встановлюючи комутоване з'єднання, що дозволяє скоротити кількість модемів або взагалі відмовитися від них. Можна обійтися і без виділених ліній, що з'єднують віддалені підрозділи. Крім того, підвищується продуктивність праці, тому що слухачі можуть користуватися надшвидкісними лініями зв'язку, які є в їх розпорядженні, замість того щоб витрачати час на встановлення комутованого з'єднання через банк модемів. Переваги технології викликали бум на ринку засобів VPN. За даними недавнього дослідження, проведеного журналом CIO Insight, понад 56 % компаній з кількістю співробітників до 1000 чоловік і 70 % більших підприємств уже розміщують VPN або інсталюють їх [1].

Захист інформації у VPN-мережах. Для побудови VPN необхідно мати на обох кінцях лінії зв'язку програми шифрування вихідного і дешифровки вхідного трафіку. Програми можуть працювати на спеціалізованих апаратних пристроях або на ПК з універсальною операційною системою, такою, як Linux, NetWare або Windows.

Доступ слухача до освітніх ресурсів вузу і комп'ютерів інших студентів групи може надаватися як через сервер освітньої установи, так і децентралізовано. Така організація обміну інформацією вимагає:

– швидкості передачі інформації, яка аналогічна швидкості передачі в локальній мережі навчального закладу;

– заборону потрапляння переданих даних до мережі загального користування;

– низької вартості обміну даними.

При достатньому рівні реалізації і використанні спеціального обладнання та програмного забезпечення й технологій, таких, як SSL та IPSec, мережа VPN може забезпечити високий рівень шифрування інформації, що передається через неї.

Порівняно з існуючими технологіями передачі даних у традиційних інтернет-мережах, мережі VPN мають такі переваги:

– при підключенні до мережі нового студента, якому дозволено користуватися віддаленим доступом, не потрібно жодних додаткових витрат на комунікації;

– у мережі VPN окремо взятий слухач може працювати вдома, з корпоративного сервера, перебувати в іншій державі; надалі виникає можливість використовувати т. зв. мобільні офіси, які не мають прив'язки до певної місцевості.

Організувати таке підключення до сервера вузу можна з допомогою т. зв. Extranet VPN. Дана організація мережі, що надає доступ через безпечні канали, останнім часом набула широкого поширення у зв'язку з розвитком електронної комерції. В цьому випадку віддалені користувачі мають дуже обмежені можливості щодо використання корпоративної мережі: фактично їх доступ обмежується тими ресурсів вузу, які необхідні при вивченні дисциплін навчального плану, а VPN використовується в цьому випадку для безпечної пересилки конфіденційних даних, які використовують протоколи шифрування.

Безпека VPN досягається за рахунок застосування таких механізмів, як тунелювання, шифрування, аутентифікація, управління доступом, а також служб, які використовуються для передачі трафіку через інтернет або будь-яку іншу небезпечну мережу на базі протоколів TCP/IP. IPSec – одна з найважливіших технологій забезпечення безпеки, яка використовується у VPN.

Гарантії цілісності та конфіденційності даних у протоколі IPSec забезпечуються за рахунок використання механізмів аутентифікації та шифрування. Застосування цих механізмів базується на попередньому погодженні сторонами порядку інформаційного обміну – т. зв. «контексту безпеки» – криптографічних алгоритмів, алгоритмів управління ключовою інформацією та конфігурації параметрів цих алгоритмів.

Управління доступом, аутентифікація і шифрування – найважливіші елементи захищеного з'єднання. Протокол PPP (Point-to-Point Protocol) давно є універсальним канальним рівнем інтернету для прокладення тунелів між пристроями, але останніми роками широкого поширення набули протоколи PPTP (Point-to-Point Tunneling Protocol) і L2TP (Layer 2 Tunneling Protocol) [2]:

а)·PPTP – тунельний протокол «крапка – крапка» – є вбудованим у клієнта віддаленого доступу таких ОС, як Windows XP і Microsoft 2003 Server. При стандартному виборі даного протоколу компанія Microsoft пропонує використовувати метод шифрування MPPE (Microsoft Point-to-Point Encryption). Можна передавати дані без шифрування у відкритому вигляді;

б)·L2TP (Layer Two Tunneling Protocol) надає більш захищене з'єднання, ніж перший варіант. Шифрування відбувається засобами протоколу IPSec (IP-security). Він також є вбудованим у клієнта віддаленого доступу ОС Windows XP і Microsoft 2003 Server, більше того, при автоматичному визначенні типу підключення клієнт спочатку намагається з'єднатися з сервером саме за цим протоколом, який є кращим у плані безпеки.

Висновки. Дану організацію телекомунікаційної мережі пропонується використовувати в системі забезпечення навчально-методичними матеріалами слухачів заочної форми навчання в міжсесійний період у навчальних закладах із підготовки та підвищення кваліфікації держслужбовців.

Література

1. Коннолли Т. Базы данных: проектирование, реализация и сопровождение. Теория и практика : учеб. пособ. / Коннолли Т., Бегг К., Страчан А. – 2-е изд. – [пер. с англ.]. – М. : Изд. дом «Вильямс», 2000. – 1120 с., ил.

2. Ульман Дж. Основы систем баз данных / [пер. с англ. М. Р. Когаловского и В. В. Когутовского ; под ред. М. Р. Когаловского]. – М. : Финансы и статистика, 1983. – 334 с.; ил.

3. Чаудхари С. Методы оптимизации запросов в реляционных системах / С. Чаудхари // Системы управления базами данных – 1998. – № 3. – С. 22.

4. Кузнецов С. Методы оптимизации выполнения запросов в реляционных СУБД / Центр информационных технологий [Електронний ресурс]. – Режим доступу : http://www.citforum.ru\database\articles\art_26.shtml.htm

Надійшла до редколегії 22.06.2009

Анотації

У статті розглядаються питання побудови телекомунікаційної мережі для проведення дистанційного навчання державних службовців. Висвітлюються питання заочного навчання і використання нових інформаційних технологій при проведенні навчання. Як базова технологія передбачається використовувати віртуальні приватні мережі. Описані основні параметри і переваги таких мереж.

В статье рассмотрены вопросы построения телекомуникационной сети для проведения дистанционного обучения государственных служащих. Рассмотрены вопросы заочного обучения и использования новых информационных технологий при проведении обучения. В качестве базовой технологии предполагается использовать виртуальные частные сети. Описаны основные параметры и преимущества таких сетей.

In the article the questions of construction of telecommunication network are considered for the leadthrough of the controlled from distance teaching of civil servants. The questions of the extra-mural teaching and use of new information technologies are considered during the leadthrough of teaching. As base technology it is assumed to utillize virtual private networks. Basic parameters and advantages of such networks are described.

УДК 681.3

А. Л. ЄРОХІН,
доктор технічних наук, професор,
начальник кафедри інформатики
Харківського національного університету внутрішніх справ
В. О. РОМАНОВ,
магістрант
Харківського національного університету радіоелектроніки

РОЗРОБКА ДОДАТКІВ ЗАСОБАМИ БІБЛІОТЕКИ WXWIDGETS

Постановка завдання. При створенні віконних додатків на будь-якій платформі використовується певний інструментарій для зручного створення графічних інтерфейсів. З огляду на вирівнювання популярності різних операційних систем, у розробників виникає потреба в крос-платформному інструменті для розробки додатків, включаючи як графічну складову, так і інші елементи узагальненої взаємодії з операційною системою, що не вимагають від розробника переписування коду під час міграції на іншу платформу. Прикладом таких елементів є керування багатопотоковістю, взаємодія через мережу, мультимовні інтерфейси, а також робота з файловою системою.

У даній статті розглядається бібліотека wxWidgets, основною метою якої є створення крос-платформних графічних інтерфейсів. Бібліотека розповсюджується з вільною ліцензією і набуває популярності як серед невеликих колективів розробників, так і серед великих корпорацій. Використання бібліотеки варіюється від наукових досліджень до клієнтських графічних додатків і візуалізації статистики.

Бібліотека розбита на модулі; деякі з них є обов'язковими для використання в будь-якому додатку, що працює з wxWidgets, інші ж допомагають розробникові в конкретних ситуаціях.

До обов'язкових базових модулів належать wxBase і wxCore.

Додаткові модулі надають інтерфейси для роботи з базами даних, мережами (сокетами), потоками, XML (включаючи можливість динамічного створення інтерфейсів з XML-файлів), візуалізацією HTML-документів, базовою роботою з