УДК 004

О.Підлубний, магістр гр. КН-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ З ВИКОРИСТАННЯМ WAN-МЕРЕЖ

У статті розроблено програмне забезпечення, яке призначено для системи віддаленого доступу з використанням WAN-мереж. Метою розробки є дослідження та програмна реалізація системи віддаленого доступу з використанням WAN-мереж. Об'єктом дослідження є процес віддаленого доступу з використанням WAN-мереж. Предметом дослідження є методи віддаленого доступу з використанням WAN-мереж. Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи віддаленого доступу з використанням WAN-мереж. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерні науки, віддалений доступ, WAN-мережі

Постановка проблеми. Сучасний світ тяжко представити без наявності мереж. У тому або іншому вигляді кожна людина на даний момент стикається з мережами: починаючи від роботи та спілкування в Інтернет й закінчуючи роботою з локальною мережею дома, або на роботі. Ще більше проникнення мереж у життя відбулося з введенням електронного документообігу й електронних платежів (у тому числі й отримання грошей через мережу банкоматів).

Таке глибоке проникнення мережевих технологій приводить до того, що доволі часто виникає потреба у віддаленому управлінні ЕОМ через локальну мережу або Інтернет та контролі того, що відбувається на віддаленій ЕОМ.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи віддаленого доступу з використанням WAN-мереж.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи віддаленого доступу з використанням WAN-мереж.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем віддаленого доступу з використанням WAN-мереж.
– Дослідження системи віддаленого доступу з використанням WAN-мереж.
– Програмна реалізація системи віддаленого доступу з використанням WAN-мереж.

Об'єктом дослідження є процес віддаленого доступу з використанням WAN-мереж.

Предметом дослідження є методи віддаленого доступу з використанням WAN-мереж.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Віддалений доступ дозволяє користувачам отримувати доступ до пристрою або мережі з будь-якого місця, що полегшує керування файлами та даними, що зберігаються на віддаленому пристрої . Це сприяє безперебійній співпраці та продуктивності будь-де. Читайте далі, щоб дізнатися більше про основи віддаленого доступу та про те, як він може принести користь вашій організації.

Що таке віддалений доступ і як він працює?

Віддалений доступ передбачає підключення комп'ютера або мережі в одному місці та пристрою в іншому місці.

Є кілька способів досягти цього. Найбільш поширеним є або через віртуальну приватну мережу (VPN), або через спеціальне програмне забезпечення, наприклад інструмент віддаленого доступу. Для організацій зі складними потребами у віддаленому доступі інструменти віддаленого моніторингу та керування (RMM) часто використовуються для спрощення великомасштабного керування.

Щоб використовувати VPN, обидва пристрої повинні мати підключення до Інтернету. VPN створює безпечний тунель, який забезпечує конфіденційність і плавний потік трафіку. Сервер VPN функціонує як шлюз на межі мережі, спрямовуючи трафік до відповідних хостів у мережі.

Для передачі інформації програмне забезпечення VPN бере трафік і загортає його в захисний шар шифрування. Пакети даних надсилаються через Інтернет різними шляхами залежно від доступності мережі. Досягнувши пункту призначення, шлюз надсилає відповідь, також зашифровану, клієнту VPN, завершуючи процес у зворотному порядку.

Тим часом програмне забезпечення віддаленого доступу – це програмне забезпечення, яке можна завантажити на свій пристрій. Він складається з «агента» та «платформи». Ви встановлюєте агента на свої ноутбуки, ПК та інші пристрої, одночасно розгортаючи платформу в мережі, до якої хочете підключитися. Коли інструмент віддаленого доступу активний, вам більше не потрібен VPN, оскільки платформа автоматично розпізнає агента та дозволяє підключитися.

Хоча обидва ці методи відрізняються за застосуванням, вони дозволяють віддалений доступ і зв'язок між пристроями.

З іншого боку, інструмент віддаленого моніторингу та керування (RMM) дозволяє організаціям виконувати операції в масштабі для всіх своїх віддалених пристроїв. Уявіть, що вам доводиться оновлювати тисячі пристроїв по одному віддалено. За допомогою інструментів RMM організації можуть оптимізувати свої IT-операції, автоматизувати рутинні завдання та скоротити час простою, забезпечуючи оптимальну продуктивність і підвищення продуктивності. IT-команди можуть віддалено розгортати оновлення програмного забезпечення, застосовувати політики безпеки та надавати технічну підтримку кінцевим користувачам, незалежно від місця розташування, усуваючи виснажливу роботу.

Чому віддалений доступ до комп'ютерів важливий для бізнесу?

Віддалений доступ до комп'ютерів дуже важливий для бізнесу в цьому сучасному світі. Ось лише кілька важливих способів зв'язку між організаціями та працівниками віддаленого доступу:

– **Підвищує гнучкість –** гнучкість у робочому місці та графіку може підвищити продуктивність співробітників, дозволяючи їм керувати своїм часом і позбавляючи їх виснажливих поїздок.

– **Зменшує витрати –** коли працівникам не потрібно фізично перебувати в офісі, ви можете зменшити витрати, пов'язані з офісним приміщенням, обладнанням і поїздками. Віддалений доступ також добре працює з політикою Bring Your Own Device (BYOD), яка може позбавити підприємства від значних інвестицій у нові комп'ютери для співробітників.

– **Покращує безпеку.** Ви можете уникнути порушень кібербезпеки, обмеживши доступ до даних і програм на сайті лише тим, хто має певні дозволи на віддалений доступ. Зберігання даних за межами об'єкта також може зменшити ризик втрати даних у катастрофічних ситуаціях.

Дев'ять способів можливого віддаленого доступу:

1. DSL (цифрова абонентська лінія)

DSL (цифрова абонентська лінія) використовує телефонну мережу, DSL-модем і високошвидкісне підключення до Інтернету. DSL-модем підключається до мережі DSL і використовує існуючі телефонні лінії для передачі цифрових даних через Інтернет.

DSL забезпечує швидший і надійніший віддалений доступ, ніж стільниковий Інтернет, але це не завжди можливо без надійної інфраструктури.

2. Широкосмуговий кабель

Ймовірно, один із найпоширеніших методів віддаленого доступу включає кабельний модем і високошвидкісне підключення до Інтернету. Для безпечного підключення до цільового пристрою або мережі також потрібне програмне забезпечення VPN або RMM.

Віддалений доступ є відносно швидким і надійним за допомогою кабельного широкосмугового зв'язку, але він обмежений областями, де доступна кабельна інфраструктура.

3. Стільниковий Інтернет

Віддалений доступ можна забезпечити за допомогою стільникового Інтернету, пристрою з підтримкою стільникового зв'язку, наприклад смартфона або планшета, і тарифного плану передачі даних. Послуга стільникового Інтернету добре працює для забезпечення віддаленого доступу, але покладається на стабільне з'єднання.

4. Супутник

Інший спосіб підключення – через супутник із супутниковим модемом, супутниковою антеною або системою VSAT (термінал із дуже малою апертурою). Супутниковий модем використовується для передачі даних на супутник і з нього, тоді як супутникова антена або система VSAT встановлює зв'язок із супутником.

5. Оптоволоконна широкосмугова мережа

Оптоволоконний широкосмуговий доступ є одним із найкращих методів віддаленого доступу, особливо для роботи, яка потребує швидкої реакції та мінімальної затримки. Допомогло б, якби у вас зазвичай був оптоволоконний модем, високошвидкісне підключення до Інтернету та підключення до VPN або програмне забезпечення для віддаленого робочого столу.

Оптоволоконна широкосмугова мережа не зазнає впливу електромагнітних перешкод або втрати сигналу на великих відстанях – на відміну від мідних кабелів, які використовуються в DSL або кабельній широкосмуговій мережі.

6. VPN/ LAN/ WAN

Щоб отримати віддалений доступ через VPN/LAN/WAN, вам потрібна VPN, локальна мережа (LAN) або глобальна мережа (WAN), залежно від вимог. Це безпечна зашифрована мережа, доступ до якої мають лише ті, хто має дозвіл.

З'єднання LAN (локальна мережа) – це мережа, об'єднана в одному місці, наприклад, в офісі, кампусі або вдома.

Глобальна мережа (WAN) – це мережа, яка охоплює кілька місць, наприклад різні офіси або філії компанії.

7. Спільне використання робочого столу

Цей метод працює лише в парі з іншим рішенням, оскільки для нього потрібне підключення до Інтернету. Ви використовуєте програмне забезпечення для віддаленого робочого столу та налаштовуєте головний комп'ютер, щоб дозволити віддалені підключення. Звідти ви можете поділитися своїм робочим столом. Це чудово підходить для обміну презентаціями або для ознайомлення IT-команди з технічними проблемами.

Однак спільний доступ до робочого столу може становити загрозу безпеці, тому важливо налаштувати з'єднання, щоб воно було безпечним і зашифрованим. Перегляньте наш блог, оскільки ми маємо багато інформації про те, як вибрати безпечний інструмент віддаленого доступу.

8. PAM (керування привілейованим доступом)

PAM – це метод безпеки, який допомагає організаціям керувати та захищати привілейовані облікові записи, які мають доступ до конфіденційних систем і даних. PAM забезпечує безпечні шлюзи доступу, які дозволяють віддаленим користувачам підключатися до привілейованих облікових записів, а також дозволяють вказувати індивідуальні рівні доступу.

9. VPAM (керування привілейованим доступом постачальника)

VPAM – це метод безпеки, який дозволяє організаціям керувати та захищати привілейований доступ сторонніх постачальників, яким потрібен віддалений доступ до своїх систем.

Щоб це було ефективним, найкраще попрацювати зі своєю IT-командою, щоб визначити сторонніх постачальників, яким потрібен віддалений доступ постачальників, і обмежити їх необхідними областями.

Що таке протокол віддаленого доступу?

Протокол віддаленого доступу – це набір правил, які регулюють, як користувач або пристрій можуть віддалено отримувати доступ до комп'ютерної системи чи мережі та спілкуватися з ними.

Ці протоколи визначають методи автентифікації та передачі даних.

Протоколи віддаленого доступу зазвичай використовують механізми шифрування та автентифікації, щоб забезпечити безпеку та автентифікацію віддаленого доступу.

6 Типи протоколів віддаленого доступу

1. Інтернет-протокол послідовної лінії (SLIP)

SLIP – це протокол, який працює на каналі даних і фізичному рівнях моделі OSI і, як правило, забезпечує низькі накладні витрати.

Він може транспортувати TCP/IP через послідовні з'єднання, але не має можливості адресації пакетів і перевірки помилок. SLIP можна використовувати лише в послідовних з'єднаннях.

2. Протокол «точка-точка» (PPP)

PPP дає змогу реалізувати TCP/IP за допомогою зв'язків «точка-точка», виділених виділених ліній та комутованих з'єднань. Він в основному використовується для віддаленого підключення до локальних мереж і провайдерів.

PPP використовує протокол керування зв'язком (LCP) для встановлення зв'язку між клієнтом PPP і хостом.

PPP пов'язаний із високими накладними витратами та може бути несумісним із старішими конфігураціями.

3. Протокол тунелювання точка-точка (PPTP)

Створений корпорацією Майкрософт протокол PPTP – це протокол VPN, який забезпечує безпечний зв'язок між віддаленими клієнтами та приватними мережами через Інтернет.

PPTP також підтримує шифрування та стиснення даних, що передаються, забезпечуючи підвищену безпеку зв'язку.

4. Служби віддаленого доступу Windows (RAS)

RAS – це набір функцій і протоколів в операційних системах Microsoft Windows, які дозволяють користувачам віддалено підключатися до мережі або комп'ютера з іншого місця через Інтернет або приватну мережу.

RAS підтримує такі технології віддаленого доступу, як віртуальні приватні мережі (VPN), мережа віддаленого доступу (DUN) і DirectAccess.

5. Протокол віддаленого робочого стола (RDP)

Розроблений корпорацією Майкрософт протокол RDP дозволяє користувачеві віддалено отримувати доступ до іншого комп'ютера або віртуальної машини та керувати ним через мережеве з'єднання. RDP вбудовано в операційні системи Windows і може підключатися до іншого комп'ютера під керуванням Windows або віртуальної машини, що працює на віддаленому сервері.

6. Обчислення віртуальної мережі (VNC)

Подібно до RDP, VNC дозволяє користувачам віддалено керувати іншим комп'ютером. Однак у цьому випадку на віддаленому комп'ютері інстальовано сервер VNC (яким потрібно керувати), а на пристрої встановлено програму перегляду VNC для керування ним.

Це забезпечує більшу гнучкість, оскільки його можна використовувати на кількох пристроях і операційних системах і має можливості спільного використання екрана.

Підвищте ефективність вашої організації за допомогою інструменту віддаленого доступу RealVNC

RealVNC® виводить ефективність вашої організації на новий рівень. VNC Connect дозволяє дистанційно отримувати доступ до комп'ютера та керувати ним, у той час як основний користувач може з ним взаємодіяти. Це робить його ідеальним для віддаленої роботи, навчання та підтримки.

Ця складна технологія віддаленого доступу, створена з урахуванням безпеки, дозволяє вашій команді працювати з будь-якого місця, яке вона вибере, використовуючи розширені інструменти адміністрування, які надають вам повний контроль.

Завдяки вибору варіантів підключення та безпеки корпоративного рівня ви можете бути впевнені, що інструменти віддаленого доступу RealVNC – це ваше рішення для покращення співпраці та продуктивності у всіх сферах.

Опис загальної технології віддаленого керування комп'ютером через Інтернет. Апаратно-програмні вимоги. Отже, що нам буде потрібно, щоб одержати можливість віддаленого керування нашим домашнім комп'ютером:

–По-перше, це, звичайно ж, доступ домашнього комп'ютера в Інтернет, і необхідно, щоб інтернет-провайдер виділив нам пряму (зовнішню) IP-адресу.

–По-друге, необхідно встановити на комп'ютер спеціальне програмне забезпечення для віддаленого адміністрування.

–По-третє, комп'ютер повинен бути включений, із завантаженою операційною системою й всім комплексом програмного забезпечення, необхідного нам для віддаленого керування. Тримати ПК постійно включеним незручно, але проблема розв'язувана. Якщо залишився старий аналоговий dial-up модем, і BIOS материнської плати підтримує технологію Wake-on-Ring, то комп'ютер може залишатися виключеним. Включеним залишиться тільки модем, що при першому ж вхідному дзвінку «розбудить» комп'ютер, і до нього стане можливим звернутися через Інтернет. Головним мінусом даної технології є саме те, що модем спрацює на будь-який вхідний дзвінок, і, відповідно, це може привести до помилкового включення комп'ютера, але адже його потім можна знову відключити.

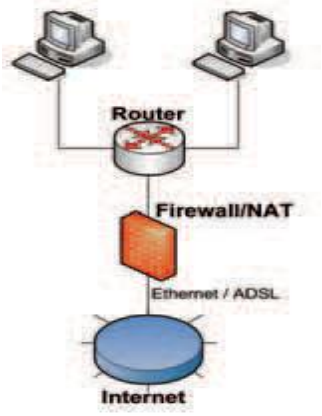

Рисунок 1 – Загальна схема віддаленого керування ПК

Детальніше варто зупинитися на підключенні до Інтернету. Найважливішу роль отут грає IP-адреса. Так, у випадку якщо домашньому комп'ютеру привласнюється пряма IP-адреса, ніяких труднощів виникнути не повинно, а от у випадку підключення через шлюз, і, відповідно, з «сірим» IP усе буде трохи складніше. Якщо підключатися через районну будинкову мережу, то прийдеться домовлятися із провайдером про надання прямої IP-адреси, а от якщо шлюз перебуває в будинку (наприклад, при використанні ADSL-модему в режимі роутера), треба просто забезпечити наскрізне проходження пакетів, адресованих нашому комп'ютеру. Як це зробити?

Для цього існує технологія NAT (Network Address Translation), що транслює запити із внутрішніх IP-адрес у зовнішню мережу, і навпаки. За замовчуванням NAT транслює тільки запити із внутрішньої мережі в зовнішню, а запити, що приходять із зовнішнього миру скидаються, просто тому що подальший маршрут проходження NAT'у невідомий. Для того щоб NAT перенаправляв запити на нашу машину, потрібно жорстко закріпити зовнішні TCP/UDP-порти шлюзу за певним комп'ютером. Для цього NAT'у варто вказати, запити для яких портів необхідно відправляти на адресу нашого ПК.

Підготовка комп'ютера

Отже, необхідно почати підготовку комп'ютера до віддаленого керування. Розглянемо випадок, коли вихід в Інтернет здійснюється через роутер (наприклад, нині популярні роутери CISCO 2801). Тоді схема підключення виходить приблизно така:

Wake-on-Ring

Для початку настроїмо опцію Wake-on-Ring. Якщо в тебе внутрішній модем, то необхідно з'єднати його зі спеціальним рознімання на материнській платі. Із зовнішнім модемом нічого додаткового не потрібно. Заходимо в BIOS материнської плати, у розділ з налаштуваннями живлення, знаходимо щось подібне Resume on Ring або Wake on Ring, і активуємо цю опцію. Тепер після вимикання комп'ютера (у випадку із зовнішнім модемом не забудь залишити його включеним) модем включить комп'ютер при першому ж дзвінку.

Невелике зауваження для тих, у кого будинку АВН. Принцип його функціонування такий, що для визначення номера він знімає трубку (ініціалізує з'єднання з АТМ) і далі дзвінки на телефони/модеми/факси, підключені паралельно АВНу, уже не проходять. Таким чином, у ланцюзі підключення АВН повинен бути першим пристроєм, а всі інші – включатися за ним.

Якщо ти хочеш, щоб комп'ютер автоматично відключався після помилкового дзвінка, необхідно встановити одну із програм, спеціально призначених для цих цілей.

У налаштуваннях програми обов'язково ставимо галочку «автоматично завантажуватися після запуску Windows», створюємо задачу «вимикання живлення», за умови відсутності активності курсору (рухів мишки) протягом десяти мінут (думаю, цього часу сповна вистачить, щоб вийти в Інтернет, зайти RAdmin'ом на комп'ютер і деактивувати цю утиліту) і підтверджуємо додавання задачі. Тепер комп'ютер при надходженні дзвінка ввімкнеться, завантажить Windows, після чого десять мінут буде покірно чекати твоїх вказівок, а після закінчення цього строку знову відключиться до наступного дзвінка.

Wake-on-LAN

Хтось може запитати, а чому б не використовувати для цих цілей технологію включення комп'ютера за допомогою локальної мережі Wake-on-LAN? Вся справа в принципі роботи цієї технології. Wake-on-LAN (а вірніше, її найпоширеніший різновид, Magic Packet) у чомусь схожа на Wake-on-Ring. Тут ключову роль виконує мережева карта, що при включенні функції Wake-on-LAN, продовжує працювати навіть після вимикання комп'ютера, і очікує спеціальний кадр, що будить. Інформація, що перебуває в цьому кадрі, являє собою шість байт синхронізації й шістнадцять разів повторену MAC-адресу мережевої карти-приймача. Послідовність упаковується в UDP, потім у пакет IP із широкомовною адресою, у кадр Ethernet, і адресується приймачу. Як адреса призначення використовується MAC-адреса Ethernet-адаптера, тобто адресація відбувається тільки на канальному рівні моделі OSI. Тому застосовувати технологію можна тільки в локальних мережах, не розділених на сегменти, або усередині одного сегмента. По цій же причині з'являються складності при посилці пакета з послідовністю, що будить, через мережу Internet.

Все це обмежує область застосування даної технології вузьким колом задач. Наприклад, при наявності в будинку декількох комп'ютерів, можно із одного з них включати інші. Для того щоб можна було скористатися цією функцією, її повинні підтримувати й мережева карта, і BIOS материнської плати. Налаштування так само просте, як і налаштування Wake-on-Ring. Заходимо в BIOS материнської плати в той же самий розділ з налаштуваннями живлення й знаходимо щось подібне Resume on LAN або Wake on LAN.

Активуємо цю опцію. Якщо материнська плата має шину PCI специфікації до 2.2 (довідатися, яку специфікацію шини PCI підтримує твоя материнська плати, ти можеш із інструкції до неї), то на ній повинен бути трьохштирьковий роз'єм «Wake On Lan». Аналогічний роз'єм повинен бути на мережевому адаптері. Їх потрібно з'єднати спеціальним кабелем, що входить у комплект поставки мережевого адаптера. Для випадку із шиною PCI 2.2 таке з'єднання вже виконане прямо. Тепер залишається тільки виключити комп'ютер.

Тепер, щоб віддалено включити цей комп'ютер, нам потрібно по мережі послати кадр із послідовністю, що будить. Для цього існує кілька програм, таких як wol.exe або broadc.exe. Всі що нам потрібно знати для запуску програми – це MAC-адреса мережевого адаптера віддаленого комп'ютера. Наприклад, для broadc.exe, що запускається з консолі, вхідний рядок буде така:

broadc.exe (MAC-адреса мережевої карти) 255.255.255.255 67

Допустимо, що MAC-адреса мережевого адаптера – 00:02:B3:D8:B4:E6, тоді рядок прийме вид:

broadc.exe 0002b3d8b4e6 255.255.255.255 67

Інші вхідні параметри змінювати не потрібно. 255.255.255.255 – це широкомовний IP-адреса, завдяки якому сформований кадр пройде через всю мережу, а 67 – номер порту протоколу UDP, у дейтаграмі якого й буде перебувати послідовність, що будить. Використання wol.exe і інших подібних програм повністю аналогічно.

Вибір програмного забезпечення

Наступним кроком є визначення необхідного нам програмного забезпечення, для здійснення функцій віддаленого керування й контролю за системою. Існує множина програм для віддаленого керування комп'ютером.

Принципово можна розділити все це різноманіття на дві групи, що розрізняються по способу керування. Управляти можна через командний рядок/консоль (Telnet, SSH) або за допомогою графічного подання робочого стола віддаленої операційної системи (Remote Desktop, Remote Administrator).

Найбільш зручним і зрозумілим для кінцевого користувача, звичайно, представляється другий спосіб, а найпоширенішою й відомою програмою для такого доступу є Remote Administrator. У якості ftp-сервера можу порекомендувати Bullet Proof або Serv-U – вони досить прості й гнучкі в налаштуванні.

Налаштування NAT

Тепер, перейдемо до підготовки нашого роутера. Отут прийде затурбуватися налаштуванням двох речей: це NAT і вбудований пакетний фільтр (або, як його частіше називають, брандмауер або firewall). І те, і інше зручніше набудовувати за допомогою web-інтерфейсу.

Для початку створимо запис в таблицю статичної NAT-адресації. Залежно від виробника конкретної моделі роутера, ця опція може позначатися по-різному. У роутерах D-link це називається «Virtual Server».

У кожному разі настроюється сам NAT скрізь однаково. Задається зовнішній порт роутера, на який приходить запит, IP-адреса й порт, на який роутер повинен перенаправляти цей запит.

Звичайно номер порту задається в обох випадках однаковий. Усе, що нам треба знати, це те, які порти використовує необхідне нам програмне забезпечення. Так, стандартний порт для Remote Administrator – 4899. З метою безпеки й зменшення ймовірності несанкціонованого доступу, можна замінити в налаштуваннях серверної частини RAdmin'a стандартний порт на будь-який інший.

Для FTP-сервера стандартний порт – 21. Рекомендую також застосовувати нестандартний порт, наприклад 2121. Обумовлено, це тим, що деякі провайдери фільтрують запити, які поступають ззовні, адресовані на стандартний для FTP порт.

Окремо варто поговорити про правильне налаштування FTP. Існують два режими роботи FTP-сервера: пасивний і активний.

Для коректної роботи за NAT'ом, потрібно настроїти сервер на пасивний режим роботи. У такому режимі клієнт, з'єднуючись із сервером, одержує від нього список портів, по яких надалі він повинен ініціювати з'єднання для передачі файлів.

У налаштуваннях самої програми FTP-сервера необхідно вказати зовнішній IP-адресу, на який будуть надсилати запити клієнти, і діапазон портів, по яких їм варто встановлювати з'єднання для передачі даних (наприклад, 47990-48000).

Їх же варто вказати в таблиці статичної NAT-адресації.

Налаштування файрвола

Але настроїти на роутері NAT – недостатньо для повноцінного функціонування цих сервісів. Необхідно ще зконфігурувати пакетний фільтр, реалізований в ADSL-роутері.

Основними правилами завжди повинні бути: пропускати всі запити із внутрішнього інтерфейсу на зовнішній, і скидати всі запити із зовнішнього на внутрішній. Таким чином, ми позбуваємося від зайвого трафіку ззовні, також охороняючи слабкі місця операційної системи від «промацування».

Залишається лише додати правила для пропущення запитів, адресованих FTP-серверу й Remote Administrator'y. Знову таки, налаштування пакетного фільтра схожі в різних виробників роутеров, і завжди містить у собі:

−завдання протоколу передачі інформації (звичайно вибір лежить між TCP, UDP і ICMP; необхідно вказати той або інший набір протоколів, які використовує додаток для передачі свого трафіку);

−завдання маршруту проходження (з якого інтерфейсу/порту на який іде трафік);

−завдання IP-адреси або діапазону IP-адрес відправника (потрібно, тільки якщо ми дозволяємо одержувати ці запити тільки з яких те конкретних IP-адрес);

−завдання номера порту або діапазону портів відправника (для вхідних запитів практичного застосування фактично ні, і в деяких роутерах цей пункт цілком логічно відсутній);

−завдання IP-адреси або діапазону IP-адрес одержувача (потрібно, тільки у випадку наявності в нас декількох зовнішніх IP-адрес, для розмежування функціонального навантаження між ними);

−завдання номера порту або діапазону портів одержувача (цим правилом, ми дозволяємо певним сервісам приймати ззовні запити й обробляти їх);

−завдання розкладу дії правила (другорядний параметр, що рекомендується залишати в значенні за замовчуванням, звичайно – always);

−вибір дії із запитом: пропустити або скинути (вибираємо дія, що буде робити роутер, одержавши пакет, що підходить під ці параметри).

Так, для Remote Administrator'a необхідно дозволити вхідні запити по протоколі TCP, з будь-яких IP-адрес, на будь-які IP-адреси, на порт 4899. Для FTP-сервера варто дозволити вхідні запити по протоколі TCP, з будь-яких IP-адрес, на будь-які IP-адреси, на порт 21 (2121) і на діапазон портів 47990-48000.

Отже, що маємо в підсумку. Ми настроїли комп'ютер, що включається по нашому телефонному дзвінку й відключається через десять мінут, у випадку якщо це був помилковий дзвінок. Ми одержали можливість віддалено включати цей комп'ютер з локальної або домашньої мережі, настроїти на роутері NAT і пакетний фільтр так, що до комп'ютера стало можливим звертатися через Інтернет.

І тепер у нас з'явилася повноцінна можливість діагностувати й віддалено управляти повною мірою домашнім комп'ютером.

Internet Server API фірми Microsoft

Коли застосовується інтерфейс Internet Server API (ISAPI) фірми Microsoft, то взаємодія між сервером і прикладною програмою організується через спеціальну структуру даних, іменовану ECB (Extension Control Block). У ній утримується інформація про те, як прикладній програмі варто обробляти поточний запит клієнта. Спочатку сервер завантажує

прикладний модуль і передає йому ECB-блок. За допомогою функцій GetServerVariable і ReadClient модуль зчитує передані клієнтом вхідні дані.

Обробивши їх, модуль звертається до функції WriteClient і відправляє дані обернено клієнтові. Після цього він викликає функцію ServerSupportFunction, щоб повідомити сервер про закінчення обробки запиту. Інсталяція прикладних ISAPI-модулів виробляється за допомогою Internet Service Manager.

Існують два типи ISAPI-програм для нарощування можливостей сервера: фільтри й прикладні модулі. Фільтри виконують, задають або змінюють запити клієнта до початку їхньої обробки сервером. Звертання до фільтрів відбувається при надходженні будь-якого запиту від клієнта. Відомості про наявні DLL-фільтри втримуються в системному Реєстрі Windows, і сервер звертається до них при своїй ініціалізації. На відміну від фільтрів прикладні модулі повинні запитуватися самим клієнтом.

Крім ISAPI існує ще інтерфейс OLEISAPI, що дозволяє вашої допоміжної API-програмі взаємодіяти із серверами OLE Automation (автоматизація OLE). У результаті можна буде створювати програми в середовищі Visual Basic, що працюють із ISAPI. (Для розробки ISAPI-модулів необхідно використовувати Visual C++ або Delphi.) Специфікація OLEISAPI містить тільки частина ISAPI і офіційно ще не прийнята фірмою Microsoft.

Розробка структурної схеми

Проаналізувавши, всі досліджені технології віддаленого керування комп'ютером, движок розробленого програмного забезпечення виконує наступні дії. Спершу відбувається з'єднання через Інтернет або локальну мережу із клієнтською частиною, що встановлена на комп'ютері який буде віддаленно управлятися. Після цього клієнтом, за допомогою функцій API, грабую весь екран і передаю його серверу, той, у свою чергу, відтворює його у своїй робочій області й там можна рухати мишею й робити довільні дії; все це програма-сервер відслідковує, перехоплює й посилає клієнтові, а той їх відтворює.

Перераховані вище дії утворюють основне ядро програми. На рисунку 2 зображена структурна схема віддаленого управління ЕОМ у загальному випадку. З цієї схеми ми бачимо, що усі віддалені користувачі зв’язуються один з одним за допомогою RAS (серверів віддаленого управління доступом), модемів та маршрутизаторів.

При цьому для доступу у мережу підприємства, сервер віддаленого управління доступом використовує файрвол, для надання взаємного захисту між внутрішньою мережею підприємства, яку можно моніторити за допомогою, розробленого, у результаті виконання магістерського проектування, програмного забезпечення, з однієї сторони та сервером віддаленого управління доступом з іншої сторони.

Схеми віддаленого керування наведені на рисунку 2, відрізняються типом взаємодіючих систем:

(1) – термінал-комп'ютер;

(2) – комп'ютер-комп'ютер;

(3) – комп'ютер-мережа;

(4) – мережа-мережа.

Відповідно при реалізації різних типів взаємодіючих систем використовується різне апаратне обладнання.

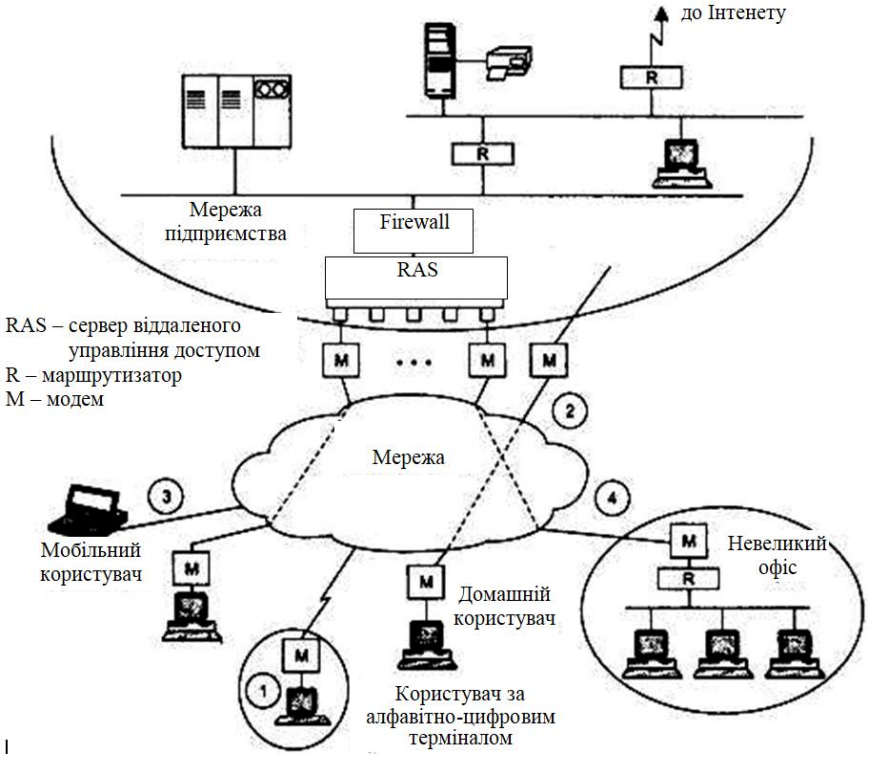

Рисунок 2 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віддаленого доступу з використанням WAN-мереж. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем віддаленого доступу з використанням WAN-мереж. Досліджена система віддаленого доступу з використанням WAN-мереж. На основі отриманих результатів досліджень створена програмна реалізація системи віддаленого доступу з використанням WAN-мереж. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання віддаленого доступу з використанням WAN-мереж. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

Список літератури

1. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645. (Scopus).
2. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660., (Scopus).
3. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407. (Scopus).
4. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019. (Scopus).
5. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019. (Scopus).

6. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629. (Scopus).
7. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 873-884. (Scopus).
8. Smirnov, O., Kuznetsov, A., Prokopovych-Tkachenko, D. «Hiding Data in Images Using a Pseudo-Random Sequence». ISCI'2020: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko, Victor A. Krasnobayev and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2020. pp. 46-59. – ISBN: 978-1-7362833-0-1 (Hardback), ISBN: 978-1-7362833-1-8 (Ebook).
9. Smirnov, O., Kuznetsov, A., Shekhanin, K., Chepurko, I. Detecting Hidden Information in FAT. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 412-429. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).
10. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).
11. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
12. Смірнов О.А., Дрєєва Г.М., «Метод генерування фрактального трафіку за допомогою моделі генератора на графі» у Інформаційна безпека та інформаційні технології: монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139.
13. Смирнов А.А., Коваленко А.В. Комплекс математических моделей технологии тестирования web-приложений. Інформаційні технології: сучасний стан та перспективи: монографія / За загальною редакцією В.С. Пономаренка. – Х.: ТОВ «ДІСА ПЛЮС», 2018. – 461 с.
14. Смирнов А.А., Коваленко А.В. Разработка метода управления рисками разработки программного обеспечения. Інформаційні технології: проблеми та перспективи: монографія / За загальною редакцією В.С. Пономаренка. – Х.: Видавець Рожко С.Г., 2017. – 447 с.
15. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98. 2022. (Фахове видання. Категорія «Б»)
16. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
17. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
18. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
19. Смирнов А., Кузнецов А., Кузнецова Т. «Шумоподобные дискретные сигналы для асинхронных систем кодового разделения радиоканалов». Радиотехника, № 2(205), 175–183. 2021.
20. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». CEUR Workshop Proceedings Volume 2732, 2020, Pages 214-227.