Колісник О.Є., Колісник М.О. (УкрДАЗТ)

ДОСВІД ВИКОРИСТАННЯ IP ТЕЛЕФОНІЇ ДЛЯ ПОБУДОВИ МЕРЕЖІ ТЕХНОЛОГІЧНОГО ЗВ'ЯЗКУ

На сьогоднішній час продовжується впровадження апаратури передачі даних у мережах зв'язку ДК «Укртрансгаз». До недавнього часу IP-телефонія, як частина уніфікованих комунікацій, не могла надати прийнятну для широкомасштабного впровадження якість інформації (недостатня розбірливість мови і затримка при передачі). Зростання продуктивності цифрової техніки дозволило використовувати кодеки, що гарантують обмін повідомленнями з заданою якістю, і не поступаються традиційним видам телефонії. Збільшення швидкості передачі даних в мережах зв'язку та впровадження в обладнання оцінки якості обслуговування (QoS) сприяло зменшенню затримок. Оскільки протокол UDP, часто використовуваний для передачі голосових повідомлень, не гарантує доставку пакетів, завдання надійності вирішується шляхом вибору надійних маршрутів передачі мови, що реалізується за допомогою маршрутизаторів, та їх резервуванням.

Побудова мережі телефонного зв'язку на основі IP-телефонії (VoIP терміналів (програмних або апаратних) і IP-АТС) дає значні переваги для організації безпечної передачі мови перед багатьма цифровими АТС. Розглянемо практичну реалізацію мережі IP-телефонії. Серверна частина IP-телефонії передбачає можливість взаємодії між оператором і IP-АТС (IP PBX) за допомогою інтернет браузера (HTTP сервер), білінгу через веб-інтерфейс (HTTP сервер), організацію зберігання голосових повідомлень (Voice Mail) і факсограм (Fax storage) на поштовому сервері (SMTP-сервер). Наявність TFTP (простий протокол передачі файлів) сервера обумовлено необхідністю оновлення програмного забезпечення (ПЗ) обладнання, інтегрованого в мережу, а також зберіганням статистичних даних.

Для апробації побудови мережі IP-телефонії в мережі Ethernet (всі комп'ютери знаходилися під управлінням операційної системи Windows) був використаний програмний IP-телефон X-Lite в якості клієнтської програми, на комп'ютер, що виконував роль сервера, була встановлена програма Asterisk, яка виконувала роль програмної АТС (IP-АТС), а також програмний термінал X-Lite. В реалізованій мережі використано наступне обладнання - маршрутизатор DSL-2600U (D-link corp.) з портом ADSL, портом Ethernet та портом 802.11g. В якості сервера виступала ПЕОМ зі встановленим ПЗ Asterisk, в якості абонентських пристроїв - комунікатор, сервер зі встановленим термінальним ПЗ і ПЕОМ зі встановленим термінальним ПЗ. Побудована мережа підтвердила можливість реалізації якісних телефонних каналів за допомогою мережі передачі даних, показала здатність до легкого масштабування мережі.

Кондратюк В.А. (УкрДАЗТ)

ЗАСТОСУВАННЯ КОНТРОЛЛЕРІВ У СУЧАСНИХ СИСТЕМАХ ЗАХИСТУ

У сучасному світі для багатьох організацій і приватних осіб стало характерним те, що збільшилася кількість крадіжок особистого і громадського майна. Особливо ця проблема стала актуальною для великих організацій де порушення безпеки може завдати величезної матеріальної шкоди, як самим організаціям, так і її клієнтам. Тому ці організації змушені особливу увагу приділяти гарантіям безпеки. В наслідок чого виникла проблема захисту та контролю доступу в приміщення. І зараз ця проблема є сукупність тісно пов'язаних проблем в областях права, організації, управління, розробки технічних засобів, програмування і математики.

У сучасних системах існує багато варіантів систем захисту та контролю доступу. Але як правило, вони є дорогими, складними, мають недостатню кількість функціональних можливостей і використовують застарілу елементну базу. Для розширення функціональних можливостей і для зниження вартості при розробці охоронних систем необхідно використовувати контролери, що дозволить реалізувати апаратуру з покращеними технічними і споживчими характеристиками.

При виробленні підходів до вирішення проблем безпеки підприємства, виробники як правило виходять з того, що кінцевою метою будь-яких заходів протидії загрозам є захист власника і законних користувачів системи від нанесення їм матеріального або морального збитку в результаті випадкових або навмисних впливів на неї. Для побудови системи захисту потрібно вирішити завдання:

- ідентифікація - процес распознанія визначених компонентів системи, зазвичай за допомогою унікальних, сприйманих системою імен(ідентіфікаторов);
- аутентифікація - перевірка ідентифікації користувача, зазвичай для прийняття рішення про дозвіл доступу до ресурсів системи;
- авторизація - надання доступу користувачеві.
- Призначення проектованої системи, це забезпечення безпеки, створення перешкод для будь-якого несанкціонованого втручання, спроб розкрадання. Система крім виконання функції захисту повинна бути сама захищена.
- Виходячи з вищесказаного можна зробити