

УДК 004.72

М.І. Шоцький, В.В. Федина

Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ ПРОЦЕСУ ОРГАНІЗАЦІЇ ЗОНОВОЇ БЕЗПЕКИ У КОМП'ЮТЕРНІЙ МЕРЕЖІ

M.I.Shotskyi, V.V. Fedyna

RESEARCH OF THE PROCESS OF ZONE SECURITY ORGANIZATION IN A COMPUTER NETWORK

Захист інформації та інформаційних ресурсів набуває все більш вагомого значення при проектуванні нових мереж та модернізації роботи існуючих. Таким чином, актуальною задачею є дослідження організації зоновної безпеки для ефективної та безпечної роботи мереж різного призначення. При дослідженні проектування безпеки в мережах потрібно враховувати низку факторів, що визначають особливості роботи організації, наборів обладнання та потоків трафіку, що мають бути захищені.

Аналіз літературних джерел дав змогу сформулювати ряд задач, що потребують вирішення при організації зоновної безпеки, а саме:

- дослідити розмір мережі для визначення правильного підходу до організації мережевої безпеки;
- визначити набори обладнання, їх тип та можливості для впровадження спроектованих рішень;
- провести аналіз потоків даних з визначенням рівнів важливості для забезпечення роботи організації;
- провести зонування мережі з використанням зон безпеки другого рівня, третього рівня або їх поєднання.

Дослідження розмірів мережі дасть змогу визначити чи створення зональної безпеки не буде приводити до ускладнення її роботи та подальшого обслуговування адмініструючим персоналом. В маленьких мережах, в багатьох випадках, достатнім рішенням є використання списків контролю доступу для організації контролю трафіку. При невеликих кількостях типів потоків даних процес написання таких списків не потребує особливих затрат часу та в подальшому спрощує керування мережею при зміні адміністратора. У мережах з динамічними потоками даних такий підхід працювати не буде або його робота буде неефективною.

Аналіз наборів обладнання дасть змогу провести аудит мережевих ресурсів з визначенням версій операційних систем, апаратних можливостей нести додаткові навантаження щодо аналізу потоків даних, сумісності різного обладнання між собою при розгортанні єдиної політики безпеки мережі.

Для різних мереж не всі потоки даних є однаковими. Створення правильної політики безпеки мережевих ресурсів організації вимагає чіткого розуміння точок входу та виходу трафіку, переходів трафіку між різними сегментами мережі, класифікації наборів даних та ін. Створення зональної безпеки базується на створенні правил роботи з даними чітко визначеними у політиці безпеки мережі організації.

Створення зонування потребує визначення на яких рівнях у мережі буде застосовуватись дана технологія. Використання зон безпеки другого рівня буде акцентувати увагу на інтерфейсах другого рівня і включатиме списки інтерфейсів в зоні, активні політики безпеки, що будуть застосовувати правила до трафіку який проходить через інтерфейс. Зональна безпека, що базується на третьому рівні використовує для організації інтерфейси третього рівня.