

Що таке брандмауери і для чого вони використовуються?

Загальний захист мережного підключення здійснюють так звані *брандмауери* (або міжмережеві екрани, програма файрвол -firewalls), які являють собою або окремий пристрій, або спеціальну програму. Програмні ж брандмауери для більшості користувачів є достатньо надійним засобом від зазіхань із боку *хакерів* і від проникнення багатьох вірусів і хробаків.

В загальних рисах принцип дії файрволів полягає у наступному: кожна програма, що вимагає мережевого підключення, використовує один із 64 тисяч доступних портів. Деякі програми і протоколи жорстко прив'язані до своїх портів, так наприклад, веб-браузери використовують 80 або 81 порт, поштові програми – 25 для відправлення або 110 для одержання. Кілька десятків портів відведено під службові потреби, інші «багато тисяч» не мають жорсткої прив'язки та використовуються різними мережевими програмами, наприклад Інтернет-пейджерями.

Програми-брандмауери відслідковують всі підключення і можуть при необхідності відкривати\закривати доступ до вибраних портів. Для того, щоб відділити корисні дані від спаму, файрвол за допомогою користувача, створює правила, за якими тій чи іншій програмі дозволено звертатися до мережевих ресурсів, використовуючи вибраний порт. При цьому враховуються звернення як зовні так із середини. При цьому в більшості випадків сигнал від файрволу про те, що зовнішня програма намагається встановити з'єднання, означає те, що вами зацікавився хакер.

Брандмауер підключення до Інтернету блокує певні типи потенційно небезпечних даних, які можуть передаватися по Мережі. Разом з тим він також блокує корисний обмін даними (наприклад при спільному використанні файлів або принтерів, передаванні файлів у моментальних повідомленнях або іграх з багатьма учасниками). І все-таки при підключенні до Інтернету рекомендується користуватися міжмережевим екраном, оскільки це допомагає захистити комп'ютер. А корисний обмін даними можна розблокувати, коли ресурси Всесвітньої мережі будуть не потрібні.

В офісних мережах як правил встановлюється корпоративний брандмауер у точці з'єднання локальної і глобальної мереж, і пробитися через таку перегороджу хакеру проблематично.

Перш ніж підключати комп'ютер до Інтернету, необхідно встановити брандмауер, вбудований в операційну систему Windows XP засіб захисту досить ефективний.

Щоб включити брандмауера підключення до Інтернету, спочатку потрібно натиснути кнопку **Пуск** і клацнути на пункті **Панель керування**. Далі у вікні, що відкрилося, слід вибрати категорію **Мережа й підключення до Інтернету** й клацнути на значку **Мережеві підключення**.

Після цього в групі **Віддалений доступ або ЛВС або високошвидкісний Інтернет** потрібно клацнути правою кнопкою миші на значку мережевого підключення, що потрібно захистити, і в контекстному меню вибрати команду **Властивості**. У вікні, що з'явилося, на вкладці **Додатково** в групі Брандмауер підключення до Інтернету варто встановити прапорець **Захистити моє підключення до Інтернету** (Рис.).

Потім потрібно натиснути на кнопку **ОК** — як результат для обраного мережевого підключення захист буде включеним.

Після встановлення між мережевого екрану при кожному першому запуску мережевих програм файрвол видаватиме вікно з попередженням, що деякий додаток намагається одержати доступ до мережевого ресурсу, використовуючи деякий конкретний порт. Користувачеві пропонується на вибір: одноразово або назавжди дозволити\заборнити доступ в мережу для обраного додатку.

Крім брандмауера, убудованого в Windows XP, є безліч аналогічних засобів, що мають більш гнучкі параметри налагодження.