УДК 004.056.5

ПРОБЛЕМИ МІЖМЕРЕЖЕВИХ ЕКРАНІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Янголь А., студ. гр. МКБп-191
Науковий керівник: **Ткач Ю. М.,** д.пед.н., доцент
Національний університет «Чернігівська політехніка»

Переваги, які отримує сучасне підприємство, маючи доступ до глобальної мережі Internet важко перерахувати. Поряд з тим використання інтернету має і негативні наслідки. Глобальна мережа Internet створювалася як відкрита система, призначена для вільного доступу до інформації. Разом з цим, питання про проблеми захисту мереж і її компонентів стали досить важливими та актуальними в наш час, час прогресу і комп'ютерних технологій.

Міжмережеві екрани можуть працювати на різних рівнях протоколів моделі OSI.

На мережевому рівні виконується фільтрація вхідних і вихідних пакетів по IP–адресам (наприклад, не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено).

На транспортному рівні фільтрація відбувається ще й за номерами портів TCP і прапорців, що містяться в пакетах (наприклад, запити на встановлення з’єднання).

На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь–яких типів файлів: рекламної інформації або виконуваних програмних модулів).

Один зі способів визначити результат спроби злому брандмауерного захисту - перевірити стан речей в так званих зонах ризику. Якщо мережа підключена до Internet без брандмауера, об'єктом нападу стане вся мережа. Така ситуація сама по собі не передбачає, що мережа стає вразливою для кожної спроби злому. Однак якщо вона приєднується до загальної незахищеної мережі, адміністраторові доведеться забезпечувати безпеку кожного вузла окремо. Більш ефективним було б не тільки блокування, але і попередження атак.

Міжмережевий екран не в змозі вирішити всі проблеми безпеки корпоративної мережі. Крім описаних вище переваг міжмережевих екранів є ряд обмежень у їхньому використанні, а також існують загрози безпеки, від яких міжмережеві екрани не можуть захистити. Також не зайвим буде використання захищених віртуальних приватних мереж, в доповнення до міжмережевих екранів, коли декілька локальних мереж, підключених до глобальної мережі, поєднуються в одну. Передача даних між цими локальними мережами є невидимою для користувачів, а конфіденційність і цілісність переданої інформації повинні забезпечуватися за допомогою засобів шифрування, використання цифрових підписів і т.і. При передачі даних може шифруватися не тільки вміст пакета, але й деякі поля заголовка.

Список використаних джерел

1. Міжмережевий екран (МЕ) [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/zahistlokalnoiemerezi/zahist/mizmerezevij-ekran.

2. Безпека Internet [Електронний ресурс] – Режим доступу до ресурсу: http://ua-referat.com/%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_Internet.

3. Проблеми безпеки та критерії оцінки міжмережевих екранів [Електронний ресурс] – Режим доступу до ресурсу: http://ni.biz.ua/4/4_5/4_54680_personalnie-raspredelennie-setevie-ekrani.html.