Григорусь А. М., магістрант,
Фальковський І. Г., ст. викладач,
Державний університет «Житомирська політехніка»

АНАЛІЗ ТИПІВ МІЖМЕРЕЖЕВИХ ЕКРАНІВ ЗА ЇХ ПРИЗНАЧЕННЯМ І РОЗМІЩЕННЯМ В МЕРЕЖІ

Міжмережеві екрани (брандмауери) є невід'ємною складовою забезпечення кібербезпеки в сучасних інформаційних системах. Вони виконують роль бар'єра між сегментами мережі контролюючи трафік на основі встановлених правил і тим самим запобігають несанкціонованому доступу та забезпечують захист від зовнішніх і внутрішніх загроз. Сучасні брандмауери класифікуються за призначенням, методами контролю та розташуванням у мережі, що дозволяє вибирати оптимальне рішення для конкретного середовища. Тому в даній роботі буде наведено аналіз основних типів міжмережевих екранів з урахуванням їх функціонального призначення та розміщення в мережі.

За способом реалізації вони поділяються на [1]:

- Апаратні – це фізичні спеціалізовані пристрої з вбудованим програмним забезпеченням для виконання функцій брандмауера. Вони забезпечують високу продуктивність, надійність і стабільність, підходять для корпоративних мереж.
- Програмні – це програмне забезпечення, що встановлюються на компю’тер або мережевий пристрій. Даний тип екранів забезпечують високу гнучкість і доступність, зокрема за рахунок низької вартості. Однак їхня ефективність залежить від апаратного забезпечення, і вони можуть бути менш продуктивними при високих навантаженнях.

За функціональними можливостями розрізняють наступні типи:

- Пакетні фільтри (Packet Filters). Ці брандмауери працюють на мережевому та транспортному рівнях моделі OSI, аналізуючи заголовки пакетів (IP-адреси, порти, протоколи). Вони швидкі та ефективні, але мають обмежену функціональність, оскільки не аналізують вміст пакетів. Пакетні фільтри зазвичай використовуються для базового контролю доступу.
- Міжмережеві екрани стану (Stateful Firewalls). Забезпечують аналіз стану з'єднань, дозволяючи моніторити та фільтрувати пакети на основі контексту попередніх взаємодій. Вони є більш гнучкими, ніж прості фільтри і широко використовуються в корпоративних мережах.
- Брандмауери додатків (Application Layer Firewalls). Працюють на рівні додатків, що дозволяє їм аналізувати конкретні протоколи та забезпечувати захист від цільових атак. Вони ефективні для запобігання атакам на веб-додатки та служби.
- Шлюз сеансового рівня (Circuit-level Gateways) – це брандмауери, що працюють на рівні сесії в мережі, контролюючи з'єднання між клієнтами та серверами. Вони перевіряють, чи є запит на з'єднання від легітимного користувача, і дозволяють лише пакети, що належать до активної сесії.
- NGFW (брандмауери нового покоління). Поєднують функції традиційних брандмауерів із додатковими можливостями, такими як аналіз трафіку на рівні додатків, захист від шкідливого програмного забезпечення та інтеграція з системами виявлення вторгнень (IDS/IPS).

За розміщенням в мережі міжмережеві екрани поділяють на наступні типи [2]:

- Периметрові брандмауери. Розташовуються на межі між корпоративною мережею та зовнішнім інтернетом. Їх основна мета – запобігати несанкціонованому доступу ззовні.
- Внутрішні брандмауери. Використовуються для сегментації мережі та захисту критично важливих зон від внутрішніх загроз. Це важливо для великих організацій, де існує ризик внутрішніх атак.
- Хмарні брандмауери. Розміщуються в інфраструктурі провайдерів хмарних послуг. Вони забезпечують захист даних і додатків, розгорнутих у хмарі.
- Гібридні брандмауери. Поєднують фізичні та хмарні компоненти для забезпечення комплексного захисту в мережі.

Отже, міжмережеві екрани є ключовими для забезпечення кібербезпеки, контролюючи трафік і захищаючи мережу від загроз [3]. Їх класифікація за призначенням та розміщенням дозволяє підібрати оптимальний тип для конкретних потреб користувача чи організації.

Список використаних джерел

1. What Is a Firewall? URL: https://www.techtarget.com/searchsecurity/definition/firewall

2. The 5 different types of firewalls explained. URL: https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls

3. IETF RFC 2979. Behavior of and Requirements for Internet Firewalls. URL: https://datatracker.ietf.org/doc/html/rfc2979