Воротніков В.В., д.т.н., доцент
Мисюк Є.Ю., магістрант
Державний університет «Житомирська політехніка»

АЛГОРИТМИ ОПТИМІЗАЦІЇ ТА АВТОМАТИЗАЦІЯ ФОРМУВАННЯ СПИСКІВ КОНТРОЛЮ ДОСТУПУ ДЛЯ МІЖМЕРЕЖЕВИХ ЕКРАНІВ

У сучасних умовах забезпечення кібербезпеки складність управління мережевими політиками стає критичною проблемою для великих організацій. Основою багатьох політик безпеки є списки контролю доступу, які визначають правила дозволу або заборони трафіку між мережевими сегментами. Однак традиційні методи ручного формування списків доступу часто виявляються неефективними через низку причин:

1. Надмірна кількість правил. Великі організації, що використовують сотні мережевих пристроїв, зіштовхуються з проблемою дублювання правил, коли схожі або ідентичні правила прописуються для різних міжмережевих екранів. Це не лише ускладнює адміністрування, а й збільшує ризики виникнення конфліктів між правилами.

2. Помилки через людський фактор. Ручне внесення змін у складні списки контролю доступу вимагає значних зусиль і може призводити до помилок, таких як неповне видалення застарілих правил або некоректне налаштування портів і IP-адрес.

3. Зниження продуктивності мережі. Чим більше правил у списку, тим більше часу потрібно пристроям для їх обробки, що негативно впливає на продуктивність мережі.

Для подолання зазначених проблем розроблено алгоритми автоматизації та оптимізації списків доступу. Одним з ефективних підходів є застосування агрегації правил, що дозволяє об'єднувати схожі правила в одне, зменшуючи їх кількість без втрати функціональності. Наприклад, правила з однаковими джерелами

трафіку, але різними портами призначення, можна об’єднати в одне правило із зазначенням діапазону портів.

Автоматизація формування списків доступу за допомогою таких інструментів, як Tufin Orchestration Suite, AlgoSec або FireMon, забезпечує централізоване управління політиками безпеки. Ці інструменти дозволяють:

- Аналізувати конфлікти між правилами;
- Оптимізувати наявні списки доступу через видалення надлишкових записів;
- Забезпечувати відповідність стандартам безпеки.

Такі підходи ефективно працюють у великих корпоративних мережах з гібридною інфраструктурою, де поєднуються локальні сервери та хмарні сервіси.

Дослідження [Qian et al., 2001] показують, що впровадження алгоритмів оптимізації списків доступу може скоротити їх обсяг на 30- 50%, що суттєво спрощує адміністрування мережі. Інший підхід, представлений [Al-Shaer, 2014], акцентує на автоматизації управління політиками безпеки, що дозволяє скоротити час на внесення змін у політику на 60%.

Таким чином, оптимізація та автоматизація формування списків контролю доступу є критично важливими для сучасних мережевих систем. Застосування алгоритмів агрегації правил та автоматизованих платформ управління забезпечує зменшення обсягу списків доступу, мінімізує ризик помилок та підвищує ефективність використання міжмережевих екранів. Подальші дослідження мають адаптувати ці інструменти до потреб хмарних і гібридних мереж.

Список використаних джерел

1. Qian J., Hinrichs S., Nahrstedt K. ACLA: A Framework for Access Control List (ACL) Analysis and Optimization // У кн.: Communications