УДК 004.7

Макарик А.С., магістрант,
Фальковський І., Г., ст. викладач
Державний університет «Житомирська політехніка»

ОБҐРУНТУВАННЯ ПІДХОДІВ ДО ОПТИМІЗАЦІЇ ЗАСТОСУВАННЯ GPO З УРАХУВАННЯМ АРХІТЕКТУРИ ТА МАСШТАБУ ДОМЕНУ МЕРЕЖІ

У сучасних корпоративних інформаційних системах на базі Windows Server служба каталогів Active Directory є основним засобом централізованого управління мережевими ресурсами. Важливою складовою її функціонування є Group Policy (GPO), ефективність яких визначається архітектурою домену, масштабом мережі та кількістю об'єктів, що безпосередньо впливають на продуктивність і стабільність системи. У зв'язку з цим актуальним є обґрунтований вибір та оптимізація моделі застосування GPO і механізмів їх впровадження з урахуванням характеристик мережевого середовища [1].

Таким чином, метою дослідження є розробка та обґрунтування підходів до оптимізації застосування GPO з урахуванням архітектури та масштабу доменної мереж.

Безпосереднє застосування політик на рівні домену або сайту є недоцільним, оскільки такі політики автоматично успадковуються всіма організаційними одиницями (OU) в межах ієрархії GPO, що призводить до застосування параметрів до невідповідних користувачів або комп'ютерів. Замість цього доцільним є створення окремої кореневої OU, на яку застосовуються політики доменного рівня, що потребують контрольованого розповсюдження.

Важливим аспектом є структурування налаштувань у межах самих GPO. Зокрема, GPO доцільно класифікувати на монолітні та функціональні. Монолітні GPO являють собою об'єднання значної кількості налаштувань в одному об'єкті, як правило, згрупованих за спільною функціональною ознакою (наприклад, забезпечення журналювання або реалізація політик безпеки). Це спрощує візуалізацію за допомогою інструментів адміністрування, зокрема Group Policy Management Console (GPMC), та полегшує призначення політик на відповідні ієрархічні рівні. Водночас монолітні GPO можуть негативно впливати на керованість системи: при великій кількості налаштувань ускладнюється делегування прав та діагностика помилок, хоча вплив на продуктивність залежить від конкретної конфігурації мережі та механізмів фільтрації.

Функціональні GPO формуються за принципом розподілу налаштувань між окремими об’єктами за їхнім призначенням, при якому кожен GPO відповідає за реалізацію конкретної функціональної задачі. Такий підхід підвищує гнучкість адміністрування та спрощує діагностику та підтримку системи.

Вибір механізмів фільтрації GPO є критичним етапом, оскільки забезпечує цільове застосування політик і зменшує їх надлишковий вплив у мережах різного масштабу та топології. Найпоширенішими методами є WMI-фільтрація та блокування успадкування політик [2]. Доцільним є підхід, за якого GPO прив’язуються максимально близько до цільових організаційних одиниць із використанням фільтрації за принципом винятків лише за необхідності, що зменшує складність адміністрування та обчислювальні витрати, підвищуючи продуктивність системи. Надмірне застосування фільтрації, навпаки, збільшує час обробки GPO через додаткові перевірки на клієнтських системах .

Окремо варто загати використання механізму зациклення GPO (Loopback processing), котрий змінює порядок обробки користувацьких політик. Зокрема, у режимі злиття (merge mode) де відбувається послідовна обробка політик користувача і комп’ютера, що призводить до подвійного аналізу посилюючи тим самим навантаження на систему, особливо у великих мережах. У зв’язку з цим використання даного механізму повинно бути обмеженим і застосовуватися лише у випадках, коли це обґрунтовано специфікою конфігурації середовища.

Результати теоретичного дослідження підтверджують доцільність оптимізації застосування GPO шляхом раціонального вибору моделі впровадження, структурування та механізмів фільтрації з урахуванням архітектури доменної мережі. Застосування запропонованих підходів підвищує продуктивність системи, знижує складність адміністрування та забезпечує ефективне й цільове використання політик.

Список використаних джерел

1. Group Policy processing for Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/%20windows-server/identity/ad-ds/manage/group-policy/group-policy-processing.

2. Active Directory and Group Policy Management Best Practices / B. Hennings et al. CIS Center for Internet Security. URL: https://learn.cisecurity.org/CIS-Benchmarks-Active-Directory-Guide.