УДК 004.459

Фальковський І.Г., ст. викладач
Карп'юк І.В., магістрант
Державний університет «Житомирська політехніка»

МОДЕЛЬ ОПТИМІЗАЦІЯ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ НА БАЗІ MECM У WINDOWS-ІНФРАСТРУКТУРІ

Стрімке масштабування сучасних IT-інфраструктур та перехід до гібридних моделей роботи формують нові виклики для системних адміністраторів. Зі збільшенням кількості робочих станцій у корпоративній мережі, побудованій на базі Windows, критичного значення набуває проблема ефективного управління кінцевими точками. Ручне виконання рутинних операцій, таких як інсталяція операційних систем, розгортання прикладного програмного забезпечення та встановлення оновлень безпеки, стає не лише економічно недоцільним через високі часові витрати, але й створює суттєві ризики для інформаційної безпеки підприємства. Затримка в оновленні навіть одного вузла може призвести до компрометації всієї системи.

Вирішення цієї проблеми полягає у переході від децентралізованого до повністю автоматизованого централізованого керування. У даній роботі досліджується підхід до побудови такої системи на основі Microsoft Endpoint Configuration Manager у тісній інтеграції зі службами каталогу Active Directory. Цей інструментарій дозволяє розглядати інфраструктуру не як набір розрізнених пристроїв, а як єдиний керований організм, де політики безпеки та конфігурації застосовуються глобально або до цільових груп.

Ключовим технічним аспектом, що дозволяє вирішити проблему навантаження на мережеві канали при масовому розгортанні "важкого" контенту, є впровадження та налаштування Boundary Groups. У роботі продемонстровано, що правильна конфігурація цих параметрів дозволяє локалізувати трафік та оптимізувати маршрути отримання оновлень клієнтськими машинами. Це вирішує проблему "вузьких місць" у мережі під час планових оновлень, забезпечуючи стабільність бізнес-процесів навіть у періоди пікового навантаження на IT-інфраструктуру.

Практична реалізація запропонованої моделі у тестовому середовищі довела свою ефективність. На прикладі автоматизованого розгортання програмного забезпечення, зокрема медіаплеєра VLC та агентів управління було показано, як застосування сценаріїв MECM мінімізує людський фактор та гарантує уніфікацію програмного

середовища на всіх робочих станціях. Впровадження автоматизованих політик оновлення сприяє зменшенню обсягу ручної роботи, дозволяючи фахівцям зосередитися на стратегічних завданнях. Крім того, інтеграція засобів моніторингу дозволяє адміністраторам отримувати превентивні сповіщення про технічні проблеми, такі як нестача дискового простору для баз даних SQL, що забезпечує проактивне реагування на інциденти.

У перспективі модель може бути масштабовано шляхом інтеграції з Microsoft Defender for Endpoint та впровадження багатофакторної автентифікації, що посилить загальний контур безпеки корпоративної мережі .

Отже, впровадження MECM із застосуванням розроблених сценаріїв налаштування Boundary Groups та політик оновлення дозволяє досягти якісно нового рівня керованості інфраструктурою. Це забезпечує баланс між оперативністю обслуговування користувачів та дотриманням суворих стандартів корпоративної безпеки .

Список використаних джерел:

1. Microsoft. Microsoft Endpoint Configuration Manager Documentation. URL: https://learn.microsoft.com/en-us/mem/configmgr/

2. Smith J. Practical Guide to Integrating MECM with Active Directory. IT Pro Publishing, 2020. 450 с.

3. Microsoft. Automatic Deployment of Software Updates. URL: https://learn.microsoft.com/en-us/intune/configmgr/sum/deploy-use/automatically-deploy-software-updates