УДК 004.056:004.7

ІНТЕГРАЦІЯ MDM ТА DLP В АРХІТЕКТУРІ ЗАХИСТУ КОРПОРАТИВНИХ ДАНИХ МОБІЛЬНИХ ІФОРМАЦІЙНИХ ІНФРАСТРУКТУР

Санжарова А. К.
e-mail: alina.sanzharova@nure.ua
Науковий керівник – старший викладач Ликова Г.О.
Харківський національний університет радіоелектроніки, каф.КРіСТЗІ
м. Харків, Україна

The work examines the convergence of MDM and DLP systems in mobile BYOD infrastructures. Sandboxing in iOS and Android prevents content-aware DLP, shifting protection to a context-aware model via containerization. MDM is positioned within a multi-layered security architecture alongside NGFW, EDR, and SIEM, and its integration with server-side DLP is proposed as the optimal mobile data protection approach.

Зростання мобільності корпоративного середовища та поширення концепції BYOD (Bring Your Own Device) змінюють традиційний підхід до захисту інформації. Якщо у стаціонарній інфраструктурі системи запобігання витоку даних (DLP) та управління мобільними пристроями (MDM) розвивалися як самостійні класи рішень, то у мобільній екосистемі відбувається їхня функціональна конвергенція, зумовлена архітектурними особливостями сучасних операційних систем.

Системи DLP (Data Loss Prevention) традиційно реалізують захист на трьох рівнях: Data-at-Rest – дані у стані зберігання, Data-in-Motion – дані під час передачі мережею, та Data-in-Use – дані у процесі обробки користувачем [1]. Ключовим принципом класичного DLP є контентний аналіз: система перевіряє вміст файлів та потоків даних на відповідність заданим шаблонам – персональним даним, платіжній інформації, грифам секретності. Однак на мобільних платформах iOS та Android повноцінна реалізація DLP-агентів архітектурно обмежена механізмом «пісочниці» (sandboxing): застосунок ізольований від даних інших застосунків і не може аналізувати їхній вміст [2]. Це унеможливлює роботу класичного Content-Aware DLP безпосередньо на мобільному пристрої.

Системи MDM (Mobile Device Management) еволюціонували від інструментів базового адміністрування пристроїв до платформ уніфікованого управління безпекою (UEM). В умовах зазначених архітектурних обмежень MDM перебирає на себе функції DLP, реалізуючи захист через контроль контексту, а не вмісту [2]. Заборона знімків екрана, блокування буфера обміну між корпоративним і особистим профілями, примусове шифрування даних у контейнері, умовний доступ до корпоративної пошти при невідповідності пристрою політикам безпеки – все це є прикладами Context-Aware DLP засобами MDM. Таким чином, ізоляція даних у захищеному контейнері замінює собою інспекцію їхнього

вмісту. MDM-системи є лише одним рівнем багаторівневої архітектури кібербезпеки. Мережевий периметр захищають міжмережеві екрани нового покоління (NGFW), що здійснюють контроль трафіку на рівні застосунків із глибокою інспекцією пакетів [3]. Системи виявлення та запобігання вторгненням (IDS/IPS) аналізують мережевий трафік на наявність сигнатур відомих атак. Захист кінцевих точок забезпечують рішення класу EDR, орієнтовані на виявлення складних загроз через поведінковий аналіз [4]. Централізований аудит усіх подій безпеки виконують SIEM-платформи, що корелюють інциденти з різних компонентів інфраструктури в реальному часі [4]. MDM у цій архітектурі забезпечує рівень кінцевої мобільної точки, доповнюючи периметровий захист контролем стану пристрою та реалізацією мобільного DLP.

Компенсація архітектурної неможливості повноцінного Content-Aware DLP на мобільних пристроях досягається на серверному рівні: DLP-сканування здійснюється на поштовому шлюзі та в корпоративному хмарному сховищі, де обмежень пісочниці не існує. MDM при цьому гарантує безпеку кінцевого пристрою-отримувача: навіть якщо шкідливий файл надійшов із зовнішнього джерела, ізоляція робочого контейнера не дозволяє даним вийти за його межі. Така комбінація серверного DLP та мобільного MDM є найбільш ефективною моделлю захисту для BYOD-середовища [1-2].

Таким чином, в архітектурі захисту корпоративних даних мобільних інфраструктур MDM виконує подвійну роль: управління відповідністю пристрою політикам безпеки та реалізація мобільного DLP через контейнеризацію і контроль контексту. Ефективний комплексний захист вимагає інтеграції MDM із серверним DLP для контентного аналізу, MTD-рішенням (Mobile Threat Defense) для виявлення мобільних загроз та SIEM для централізованого аудиту – що формує цілісну багаторівневу архітектуру безпеки корпоративної мобільної інфраструктури.

Список використаних джерел:

1. Market Guide for Data Loss Prevention / Gartner. URL: https://www.gartner.com/en/documents/4005391 (дата звернення: 10.03.2026).

2. What Is Data Loss Prevention (DLP)? / IBM. URL: https://www.ibm.com/topics/data-loss-prevention (дата звернення: 10.03.2026).

3. What Is a Next-Generation Firewall (NGFW)? / Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-next-generation-firewall (дата звернення: 11.03.2026).

4. What is SIEM and SOAR? / Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem (дата звернення: 11.03.2026).

5. OWASP Mobile Top 10 Vulnerabilities / OWASP Foundation. URL: https://owasp.org/www-project-mobile-top-10/ (дата звернення: 11.03.2026).