System MDM w Jednostkach Samorządu Terytorialnego

Praktyczny poradnik dla samorządowców

CyberKatalog.pl

Wydanie Pierwsze

Czerwiec 2025

Publikacja elektroniczna

O publikacji

Niniejsze opracowanie, przygotowane przez zespół ekspertów CyberKatalog.pl, stanowi kompleksowe kompendium wiedzy poświęcone strategicznym, technicznym i prawnym aspektom zarządzania urządzeniami mobilnymi (Mobile Device Management) w sektorze publicznym.

Celem publikacji jest systematyzacja wiedzy oraz dostarczenie decydentom, menedżerom IT oraz specjalistom do spraw bezpieczeństwa w Jednostkach Samorządu Terytorialnego praktycznego i merytorycznego przewodnika. Mamy nadzieję, że zawarte tu informacje okażą się cennym wsparciem w procesach analizy, planowania, wdrażania i zgodnej z prawem eksploatacji systemów MDM, przyczyniając się do podniesienia poziomu cyberbezpieczeństwa polskiej administracji.

Wydawca: CyberKatalog.pl
Data wydania: Czerwiec 2025
Wydanie: Wydanie Pierwsze
Format: Publikacja elektroniczna

Publikacja jest dostępna w wersji elektronicznej na stronie: CyberKatalog.pl

Spis treści

Rozdział 1

Wprowadzenie

1.1 Zarządzanie Urządzeniami Mobilnymi (MDM) w Administracji Samorządowej

1.1.1 Wyzwania cyfrowej transformacji w sektorze publicznym

Dynamiczna cyfryzacja sektora publicznego, stymulowana przez globalne trendy technologiczne, paradygmat inteligentnego miasta (*smart city*)[1, 2] oraz rosnące oczekiwania obywateli w zakresie jakości i dostępności usług, stawia przed jednostkami samorządu terytorialnego (JST) bezprecedensowe wyzwania[3]. Tradycyjny, stacjonarny model pracy urzędniczej, oparty na scentralizowanej infrastrukturze, ustępuje miejsca elastycznym formom zatrudnienia, w tym pracy zdalnej i hybrydowej. Ta ewolucja modeli operacyjnych, dodatkowo przyspieszona przez globalne kryzysy, takie jak pandemia COVID-19, doprowadziła do masowego wprowadzenia do użytku służbowego urządzeń mobilnych[4].

Skala tego zjawiska jest znacząca. Już w 2020 roku 86,9% jednostek administracji publicznej w Polsce wyposażało swoich pracowników w urządzenia przenośne umożliwiające mobilne łączenie się z internetem w celach służbowych[5]. Chociaż wówczas dotyczyło to 27,8% ogółu pracowników, można z dużą dozą pewności założyć, że odsetek ten dynamicznie wzrósł w kolejnych latach. W rezultacie powstało wysoce heterogeniczne środowisko technologiczne, obejmujące smartfony, tablety i laptopy z różnymi systemami operacyjnymi (np. Android, iOS, Windows) i konfiguracjami[6]. Zarządzanie takim ekosystemem oraz jego efektywne zabezpieczenie stało się kluczowym i złożonym zadaniem dla działów IT w administracji.

Głównym zagrożeniem związanym z tą transformacją jest fundamentalne zwiększenie powierzchni ataku i ryzyka naruszenia bezpieczeństwa danych. Urządzenia mobilne, z natury wykorzystywane poza chronionym obwodem sieciowym urzędu, stają się potencjalnym wektorem ataku (np. poprzez złośliwe oprogramowanie lub phishing) lub punktem wycieku informacji na skutek kradzieży bądź zagubienia[6]. Problem ten nabiera szczególnej wagi w kontekście przetwarzania przez JST danych osobowych milionów obywateli, w tym danych wrażliwych (sensytywnych), a także informacji niejawnych lub kluczowych dla ciągłości funkcjonowania państwa. Skuteczne zarządzanie flotą mobilną nie jest już zatem wyłącznie kwestią optymalizacji operacyjnej, lecz fundamentalnym wymogiem gwarantującym ciągłość świadczenia usług publicznych,

ochronę danych oraz zgodność z obowiązującym porządkiem prawnym.

1.1.2 Systemy MDM jako strategiczne narzędzie zarządcze i gwarant zgodności

Odpowiedzią na opisane wyzwania są systemy klasy **Mobile Device Management (MDM)**. W swej istocie stanowią one scentralizowaną platformę programową, działającą w architekturze klient-serwer, która umożliwia administratorom zdalne zarządzanie, monitorowanie i zabezpieczanie całego cyklu życia urządzeń mobilnych w organizacji – od ich wdrożenia, przez konfigurację i codzienne użytkowanie, aż po bezpieczne wycofanie z eksploatacji[7]. Agent MDM, instalowany na urządzeniu końcowym, komunikuje się z centralnym serwerem, pobierając i egzekwując zdefiniowane polityki bezpieczeństwa.

Należy przy tym zauważyć, że sam termin MDM przeszedł znaczącą ewolucję. Historycznie odnosił się do narzędzi skupionych wyłącznie na kontroli samego urządzenia. Rozwój technologii i modeli pracy, jak *Bring Your Own Device* (BYOD), wymusił powstanie bardziej kompleksowych rozwiązań[7, 8]:

EMM (*Enterprise Mobility Management*) Rozszerzyły one funkcjonalność MDM o zarządzanie aplikacjami (MAM), treścią (MCM) oraz tożsamością i dostępem (IAM), oferując bardziej holistyczne podejście do mobilności[9].

UEM (*Unified Endpoint Management*) Stanowią najnowszy etap ewolucji, pozwalając na zarządzanie z jednej konsoli wszystkimi typami urządzeń końcowych – nie tylko mobilnymi, ale również stacjonarnymi (laptopy, komputery biurkowe), a nawet urządzeniami Internetu Rzeczy (IoT)[10].

Choć współczesne platformy dla sektora publicznego najczęściej należą do kategorii EMM lub UEM, termin MDM jest wciąż powszechnie używany jako synonim dla fundamentalnych funkcji zarządzania mobilnością.

Implementacja systemu MDM pozwala na egzekwowanie jednolitych polityk bezpieczeństwa na wszystkich urządzeniach, niezależnie od ich rodzaju, systemu operacyjnego czy lokalizacji. Kluczowe komponenty funkcjonalne tych systemów obejmują[6, 7]:

- **Zdalną konfigurację i wdrażanie (*Deployment*):** Automatyzacja procesu przygotowania nowych urządzeń do pracy, często w modelu bezdotykowym (tzw. *zero-touch deployment*), co obejmuje automatyczną instalację niezbędnych aplikacji, profili sieciowych i certyfikatów bezpieczeństwa[11].

- **Zarządzanie bezpieczeństwem (*Security Management*):** Wymuszanie stosowania silnych haseł i uwierzytelniania wieloskładnikowego, egzekwowanie szyfrowania pamięci masowej urządzenia (np. BitLocker, FileVault) oraz możliwość zdalnego blokowania lub usuwania danych (*remote wipe*) w przypadku kradzieży lub zgubienia sprzętu[7, 12].

- **Zarządzanie aplikacjami (*Application Management*):** Tworzenie korporacyjnych katalogów aplikacji, egzekwowanie polityk list dozwolonych i zabronionych (*whitelisting/blacklisting*) oraz zarządzanie cyklem życia oprogramowania

(instalacja, aktualizacja, usuwanie). W modelach BYOD kluczowa jest technologia konteneryzacji, tworząca odizolowaną, szyfrowaną przestrzeń na dane służbowe[7, 8].

- **Monitorowanie i raportowanie zgodności (*Compliance Monitoring*):** Ciągła weryfikacja, czy urządzenia spełniają wewnętrzne i zewnętrzne normy bezpieczeństwa, oraz generowanie szczegółowych raportów na potrzeby audytów i wykazania zgodności z regulacjami[6, 7].

Wdrożenie platformy MDM jest nie tylko dobrą praktyką, ale również narzędziem umożliwiającym spełnienie konkretnych wymogów prawnych. Dotyczy to w szczególności dwóch kluczowych regulacji Unii Europejskiej, które fundamentalnie kształtują obowiązki JST w obszarze cyberbezpieczeństwa.

RODO[13] Artykuł 32 RODO nakłada na administratorów danych obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania[14]. System MDM jest jednym z fundamentalnych środków technicznych, pozwalających ten obowiązek zrealizować w odniesieniu do urządzeń mobilnych, wspierając jednocześnie realizację zasady rozliczalności (art. 5 ust. 2 RODO)[7, 15].

Dyrektywa NIS2[16] Nowe przepisy rozszerzają katalog podmiotów objętych regulacją, włączając w to organy administracji publicznej na szczeblu lokalnym i regionalnym[16]. Klasyfikuje je jako „podmioty kluczowe" lub „ważne", co wiąże się z koniecznością wdrożenia rygorystycznych, opartych na analizie ryzyka, środków cyberbezpieczeństwa[17]. System MDM jest nieodzownym elementem strategii mitygacji ryzyka związanego z punktami końcowymi[7].

1.1.3 Strategiczne korzyści z implementacji MDM w samorządzie

Wzmocnienie cyberbezpieczeństwa i ochrona danych. Podstawową korzyścią jest fundamentalne wzmocnienie poziomu bezpieczeństwa danych publicznych i osobowych. Centralne zarządzanie pozwala na proaktywne budowanie wielopoziomowej tarczy ochronnej oraz natychmiastową reakcję na incydenty, minimalizując ryzyko nieautoryzowanego dostępu do danych obywateli i systemów urzędowych[6, 7]. Jest to fundament budowania zaufania publicznego do cyfrowych usług w erze powszechnej cyfryzacji[1].

Optymalizacja operacyjna i finansowa. Automatyzacja procesów związanych z zarządzaniem flotą urządzeń znacząco odciąża działy IT, pozwalając im skupić się na zadaniach o charakterze strategicznym, a nie reaktywnym[18]. Redukcja kosztów wynika nie tylko z mniejszego nakładu pracy, ale również z prewencji – unikania strat finansowych i wizerunkowych związanych z wyciekami danych oraz karami za nieprzestrzeganie przepisów. Wdrożenie MDM wpływa na obniżenie całkowitego kosztu posiadania (*Total Cost of Ownership*, TCO) infrastruktury mobilnej, a bariera inwestycyjna może być dodatkowo zredukowana dzięki programom takim jak „Cyberbezpieczny Samorząd"[19].

Zwiększenie efektywności i mobilności pracowników. Pracownicy samorządowi wyposażeni w bezpieczne i w pełni skonfigurowane narzędzia mobilne mogą wykonywać swoje obowiązki sprawniej, również w terenie lub z domu[18]. Ustandaryzowane środowisko pracy ułatwia współpracę, zapewnia równy i bezpieczny dostęp do zasobów cyfrowych, co bezpośrednio przekłada się na jakość i terminowość obsługi mieszkańców oraz realizacji zadań publicznych[7].

Zapewnienie ciągłości działania i odporności organizacyjnej. W sytuacjach kryzysowych, takich jak awaria sprzętu, jego zagubienie lub konieczność nagłego przejścia na masowy tryb pracy zdalnej, system MDM gwarantuje ciągłość funkcjonowania urzędu. Możliwość błyskawicznego przygotowania nowego urządzenia lub zdalnego zabezpieczenia utraconego sprzętu jest kluczowa dla utrzymania nieprzerwanej realizacji zadań publicznych, co stanowi nadrzędny cel działalności każdej jednostki samorządu terytorialnego i jest filarem jej odporności organizacyjnej[7].

Rozdział 2

Podstawy systemów MDM

2.1 Fundamenty Technologiczne i Ewolucja Paradygmatu

2.1.1 Architektura klient-serwer jako rdzeń systemu

U podstaw każdej platformy klasy **Mobile Device Management (MDM)** leży sprawdzona architektura klient-serwer[7]. Centralnym elementem jest **serwer MDM**, który pełni rolę konsoli administracyjnej i centrum decyzyjnego. Może on być wdrożony w infrastrukturze własnej organizacji (*on-premise*) lub, co jest coraz popularniejszym modelem, świadczony w formie usługi w chmurze (*Software as a Service*, SaaS)[18]. Z poziomu tego serwera administratorzy IT definiują, wdrażają i monitorują polityki bezpieczeństwa oraz konfiguracje dla całej floty urządzeń mobilnych.

Drugim, nierozerwalnym komponentem jest **agent MDM** – specjalistyczne oprogramowanie lub, częściej, natywny profil konfiguracyjny instalowany na każdym zarządzanym urządzeniu końcowym (ang. *endpoint*)[7]. Agent ten pozostaje w stałej, szyfrowanej komunikacji z serwerem, cyklicznie pobierając i egzekwując przypisane mu polityki oraz raportując swój status i stan zgodności[6]. Komunikacja ta opiera się na dedykowanych interfejsach programistycznych aplikacji (API) udostępnianych przez producentów systemów operacyjnych, takich jak *Apple Push Notification service* (APNs) dla iOS/macOS czy *Firebase Cloud Messaging* (FCM) dla Androida[20]. Mechanizmy te pozwalają serwerowi na natychmiastowe wysyłanie poleceń do urządzeń, zapewniając scentralizowaną i zautomatyzowaną kontrolę nad rozproszonym i heterogenicznym środowiskiem mobilnym.

2.1.2 Ewolucja paradygmatu: od MDM przez EMM do UEM

Termin MDM, choć wciąż powszechnie używany, historycznie odnosi się do pierwszej generacji systemów, skupionych wyłącznie na kontroli samego urządzenia[7]. Gwałtowny rozwój technologii mobilnych, a przede wszystkim zmiana modeli pracy – w tym upowszechnienie się polityki *Bring Your Own Device* (BYOD), w której pracownicy wykorzystują prywatny sprzęt do celów służbowych – wymusiły ewolucję tych narzędzi w kierunku bardziej kompleksowych platform zarządczych.

MDM (*Mobile Device Management*) Koncentruje się na fundamentalnym zabezpieczeniu i kontroli sprzętu na poziomie systemu operacyjnego[7]. Jego domeną jest zdalna konfiguracja, egzekwowanie polityk haseł, wymuszanie szyfrowania, a także zdalne blokowanie i czyszczenie danych z urządzenia[6].

EMM (*Enterprise Mobility Management*) Jest naturalnym rozszerzeniem koncepcji MDM[7]. Platformy EMM, oprócz pełnej funkcjonalności MDM, integrują w sobie dodatkowe, kluczowe moduły, takie jak[9]:

- **Zarządzanie aplikacjami mobilnymi** (MAM – *Mobile Application Management*): Pełna kontrola nad cyklem życia aplikacji korporacyjnych, od instalacji po usunięcie[7].
- **Zarządzanie treścią mobilną** (MCM – *Mobile Content Management*): Bezpieczna dystrybucja i dostęp do dokumentów służbowych[7].
- **Zarządzanie tożsamością i dostępem** (IAM – *Identity and Access Management*): Kontrola dostępu do zasobów na podstawie tożsamości użytkownika i stanu (zgodności) urządzenia[7].

UEM (*Unified Endpoint Management*) Reprezentuje najnowszy i najbardziej holistyczny etap ewolucji[10]. Platformy UEM umożliwiają zarządzanie wszystkimi urządzeniami końcowymi w organizacji – smartfonami, tabletami, laptopami, komputerami stacjonarnymi, a nawet urządzeniami Internetu Rzeczy (IoT) – z poziomu jednej, zunifikowanej konsoli. Upraszcza to znacząco administrację i zapewnia spójność polityk bezpieczeństwa w całym, zdywersyfikowanym ekosystemie IT organizacji[7].

Chociaż współczesne, zaawansowane rozwiązania wdrażane w sektorze publicznym najczęściej należą do kategorii EMM lub UEM, termin MDM jest w praktyce nadal powszechnie używany jako synonim dla fundamentalnych funkcji zarządzania mobilnością[7].

2.2 Kluczowe Komponenty Funkcjonalne Platformy Zarządzającej

2.2.1 Zautomatyzowany cykl życia urządzenia: od wdrożenia po wycofanie

Zarządzanie pełnym cyklem życia urządzeń mobilnych jest podstawowym zadaniem systemów MDM[7]. Kluczowym elementem tego procesu jest mechanizm **automatycznego wdrażania** (ang. *zero-touch enrollment*)[21]. Technologie takie jak *Apple Automated Device Enrollment* (dawniej DEP)[22], *Android Zero-Touch*[23] czy *Windows Autopilot*[24] pozwalają na masową, zdalną i bezdotykową konfigurację sprzętu. Proces ten polega na przypisaniu numeru seryjnego urządzenia do serwera MDM organizacji jeszcze na etapie zakupu[22]. Po pierwszym uruchomieniu i połączeniu z internetem, urządzenie automatycznie nawiązuje komunikację z serwerem, pobiera przypisany mu

profil konfiguracyjny, instaluje niezbędne aplikacje, certyfikaty i polityki bezpieczeństwa[20, 21]. Taka automatyzacja eliminuje potrzebę manualnej interwencji działu IT, co gwarantuje spójność i poprawność konfiguracji, a także uniemożliwia użytkownikowi pominięcie procesu rejestracji[11].

Równie istotny jest proces bezpiecznego **wycofania urządzenia** (*decommissioning*)[7]. Platforma MDM automatyzuje go poprzez funkcję zdalnego czyszczenia danych (*remote wipe*)[25]. Może ono przybrać formę[25]:

- **Całkowitego wymazania (full wipe):** Przywrócenie urządzenia do ustawień fabrycznych, stosowane dla sprzętu będącego własnością urzędu[25].
- **Selektywnego wymazania (selective wipe):** Usunięcie wyłącznie danych i aplikacji korporacyjnych z odizolowanego kontenera, z pozostawieniem danych prywatnych użytkownika, co jest funkcją kluczową w modelu BYOD[25, 26].

2.2.2 Zarządzanie aplikacjami i treścią (MAM i MCM)

System MDM/EMM pełni rolę strażnika ekosystemu aplikacyjnego na urządzeniach służbowych[7]. Umożliwia tworzenie i zarządzanie **korporacyjnym katalogiem aplikacji**, zapewniając, że pracownicy korzystają wyłącznie ze zweryfikowanego i bezpiecznego oprogramowania. Funkcjonalność ta obejmuje dystrybucję i automatyczną instalację aplikacji obowiązkowych, zarządzanie ich cyklem życia (w tym krytyczne aktualizacje bezpieczeństwa) oraz egzekwowanie polityk **list dozwolonych i zabronionych** (*whitelisting/blacklisting*)[7].

W scenariuszach BYOD kluczową technologią jest **konteneryzacja**[26]. Polega ona na stworzeniu na urządzeniu zaszyfrowanej, odizolowanej logicznie przestrzeni (kontenera), w której hermetyzowane są wyłącznie dane i aplikacje służbowe. Pozwala to na pełną separację sfery prywatnej od zawodowej, a co za tym idzie, umożliwia selektywne usunięcie tylko danych korporacyjnych bez ingerencji w prywatne pliki użytkownika[25, 26].

2.2.3 Zarządzanie bezpieczeństwem i dynamiczna kontrola zgodności

Możliwość centralnego definiowania i nieprzerwanego egzekwowania polityk bezpieczeństwa jest rdzeniem funkcjonalnym każdego systemu MDM[7]. Platforma pozwala na wdrożenie granularnych reguł, które stanowią techniczną implementację wewnętrznych procedur bezpieczeństwa oraz wymogów prawnych (RODO, NIS2). Kluczowe obszary objęte politykami to m.in. wymagania dotyczące złożoności haseł, obligatoryjne szyfrowanie danych (np. za pomocą technologii BitLocker, FileVault), ograniczenia funkcjonalne (np. blokada aparatu, portów USB, zrzutów ekranu) oraz automatyczna konfiguracja profili sieciowych (Wi-Fi, VPN)[7].

Nowoczesne systemy idą jednak o krok dalej, oferując mechanizmy **dostępu warunkowego** (*Conditional Access*)[27]. Oznacza to, że dostęp do zasobów korporacyjnych (np. poczty elektronicznej, systemów wewnętrznych) jest dynamicznie uzależniony od stanu zgodności (*compliance status*) urządzenia[28, 27]. Jeśli system MDM wykryje naruszenie, takie jak próba złamania zabezpieczeń systemu (*jailbreak/root*) lub brak

zainstalowanych krytycznych poprawek bezpieczeństwa, dostęp do danych służbowych jest automatycznie blokowany do czasu przywrócenia zgodności[27, 26].

2.2.4 Inwentaryzacja, audyt i raportowanie

Platforma MDM pełni funkcję centralnego repozytorium informacji o całej flocie mobilnej[7]. Gromadzi szczegółowe dane inwentaryzacyjne (model, system operacyjny, zainstalowane aplikacje) oraz prowadzi niezaprzeczalny **dziennik zdarzeń (log)** dla wszystkich operacji i incydentów. Dane te są niezbędne do celów audytowych, planowania budżetu oraz analizy bezpieczeństwa. Zdolność do generowania raportów na żądanie jest kluczowa dla wykazania **rozliczalności** w rozumieniu art. 5 ust. 2 RODO. W dojrzałych środowiskach IT, logi z systemu MDM są często integrowane z centralnymi platformami klasy SIEM (*Security Information and Event Management*) w celu korelacji zdarzeń i budowania holistycznego obrazu stanu cyberbezpieczeństwa organizacji[29].

Rozdział 3

Polityki Bezpieczeństwa i Kontrola Zgodności

3.1 Definiowanie i Egzekwowanie Polityk Bezpieczeństwa

Polityki bezpieczeństwa w systemach MDM stanowią fundamentalny mechanizm przekształcenia abstrakcyjnych wymogów prawnych i organizacyjnych w konkretne, techniczne środki ochrony[7]. Polityka MDM (Mobile Device Management policy) to zbiór wytycznych i reguł, które pomagają firmom zarządzać i chronić urządzenia mobilne w sposób spójny i zautomatyzowany[30]. Umożliwiają one narzucenie, egzekwowanie, a tym samym przestrzeganie reguł ustalonych przez organizację lub nałożonych przez uwarunkowania prawne[31].

3.1.1 Hierarchiczna struktura polityk i granularność kontroli

Nowoczesne platformy MDM/EMM oferują zaawansowaną, hierarchiczną strukturę polityk, która pozwala na precyzyjne dostosowanie poziomów restrykcji do różnych grup użytkowników, typów urządzeń czy kontekstów użytkowania[31]. Dostępne polityki są zależne od systemu operacyjnego danego urządzenia, a co za tym idzie, także rodzaju jego aktywacji[31]. Tworząc nową politykę, należy określić jej kompatybilność z jednym wybranym typem aktywacji[31].

Przypisywanie polityk do grup pozwala również na poziomowanie restrykcji, czyli nakładanie większych lub mniejszych ograniczeń, które mogą odzwierciedlać uprawnienia wynikające ze specyfiki konkretnych stanowisk[31]. W przypadku zmiany zasad bezpieczeństwa w organizacji lub pojawienia się nowych dyrektyw prawnych, systemy MDM umożliwiają szybką modyfikację wszystkich polityk jednocześnie[31].

Kluczowe kategorie polityk zabezpieczających. Współczesne platformy MDM oferują kompleksowy katalog kategorii polityk, dostosowanych do różnych systemów operacyjnych i scenariuszy wdrożenia[31]:

Polityki haseł: Dotyczą wszystkich systemów i aktywacji, definiując wymagania dotyczące złożoności, długości i częstotliwości zmiany haseł[31].

Polityki aplikacji: Obejmują aktywacje Android Enterprise, iOS i macOS, kontrolując instalację, aktualizację i korzystanie z oprogramowania[31].

Polityki bezpieczeństwa: Dedykowane dla systemów Android, Windows i iOS, definiujące fundamentalne mechanizmy ochronne[31].

Polityki funkcjonalności: Stosowane w aktywacjach Android Enterprise, iOS, macOS i Windows, ograniczające lub włączające określone funkcje urządzenia[31].

Polityki lokalizacji: Specyficzne dla Android Enterprise Device Owner, umożliwiające geofencing i kontrolę mobilności[31].

Polityki szyfrowania (BitLocker): Dedykowane dla Windows, wymuszające szyfrowanie danych w spoczynku[31].

3.1.2 Automatyzacja egzekwowania i monitoring zgodności

Kluczowym atutem systemów MDM jest zdolność do automatycznego i nieprzerwanego egzekwowania zdefiniowanych polityk[7]. System MDM pozwala administratorom konfigurować urządzenia, wymuszać polityki bezpieczeństwa i chronić dane korporacyjne, zachowując jednocześnie mobilność pracowników[7]. Tego typu rozwiązania umożliwiają egzekwowanie złożonych polityk haseł, w tym wymuszanie użycia PIN-ów, kodów alfanumerycznych o określonym stopniu skomplikowania, metod biometrycznych, a także regularnej zmiany haseł[7].

System automatycznie analizuje aktywność urządzeń, pozwalając na wykrywanie nieprawidłowości – takich jak próby instalacji nieautoryzowanego oprogramowania, łączenie się z niezaufanymi sieciami czy działania typowe dla malware[26]. W przypadku wykrycia naruszenia polityki, platforma może automatycznie podjąć działania naprawcze, od ostrzeżenia użytkownika, przez ograniczenie funkcjonalności, aż po całkowite zablokowanie dostępu do zasobów korporacyjnych[27].

3.2 Kontrola Dostępu Warunkowego i Zarządzanie Tożsamością

3.2.1 Mechanizmy dostępu warunkowego jako fundament Zero Trust

Dostęp warunkowy to zaawansowana funkcja kontroli dostępu, która umożliwia organizacjom definiowanie i egzekwowanie zasad bezpieczeństwa dostępu do danych i aplikacji[32]. Kiedy użytkownik próbuje uzyskać dostęp do zasobów firmowych, system automatycznie ocenia różne "sygnały"(takie jak lokalizacja, urządzenie, aplikacja) i na tej podstawie podejmuje decyzję, czy zezwolić na dostęp, wymagać uwierzytelnienia wieloskładnikowego (MFA) lub całkowicie zablokować dostęp[32].

Systemy kontroli dostępu służą do ograniczenia ilości osób mających dostęp do konkretnych pomieszczeń, stref czy danych, przy czym sprawdzane jest dokładnie kto, co i kiedy zrobił[33]. W kontekście urządzeń mobilnych, mechanizmy te są szczególnie

istotne, gdyż pozwalają na dynamiczną ocenę ryzyka na podstawie aktualnego stanu urządzenia i kontekstu jego użytkowania[27].

Integracja z systemami zarządzania tożsamością. Kontrola dostępu na podstawie ról (RBAC) przyznaje prawa dostępu na podstawie zdefiniowanych funkcji biznesowych, a nie tożsamości czy poziomu w hierarchii poszczególnych użytkowników[34]. Celem jest udostępnianie użytkownikom tylko tych danych, które są im potrzebne do wykonywania ich zadań, bez żadnych innych danych[34]. Kontrola dostępu na podstawie atrybutów (ABAC) umożliwia jeszcze bardziej elastyczne zarządzanie, gdzie dostęp jest udzielany na podstawie kombinacji atrybutów i warunków w środowisku, takich jak czas i lokalizacja[34].

3.2.2 Konteneryzacja i segmentacja danych

Konteneryzacja to jedno z najskuteczniejszych narzędzi pozwalających na bezpieczne współistnienie danych prywatnych i służbowych na jednym urządzeniu[7]. W ramach polityki BYOD system MDM umożliwia stworzenie odseparowanego środowiska roboczego – tzw. profilu służbowego – którego dane mogą być szyfrowane, chronione hasłem i usuwane zdalnie, bez ingerencji w prywatną przestrzeń użytkownika[7].

Rozbudowany mechanizm zarządzania dostępem (IAM) umożliwia definiowanie uprawnień na poziomie aplikacji, grup użytkowników, lokalizacji geograficznych czy sieci, do których podłączone jest urządzenie[7]. W rezultacie możliwe jest precyzyjne zarządzanie ryzykiem, bez utraty komfortu użytkownika[7]. Takie podejście zwiększa bezpieczeństwo aplikacji, które mogą być używane wyłącznie w kontrolowanym środowisku[7].

3.3 Audyt Bezpieczeństwa i Raportowanie Zgodności

3.3.1 Systematyczny audyt jako wymóg prawny i organizacyjny

Zgodność z niektórymi regulacjami (RODO, dyrektywa NIS2) wymaga systematycznego audytu i dokumentowania działań związanych z przetwarzaniem danych, także na urządzeniach mobilnych[7]. Audyt cyberbezpieczeństwa odgrywa kluczową rolę w zapewnieniu zgodności z przepisami RODO, które kładzie duży nacisk na ochronę danych osobowych[35]. Przeprowadzenie takiego audytu pozwala na identyfikację potencjalnych zagrożeń i luk w zabezpieczeniach, które mogą narazić organizację na nieprzestrzeganie przepisów[35].

W tym zakresie MDM musi oferować możliwość wglądu w logi audytowe ze zdarzeń na serwerze oraz wyciągania raportów, które obejmują m.in. kompletną listę urządzeń firmowych, ich status bezpieczeństwa i zastosowane polityki[7]. Administratorzy IT mogą w każdej chwili wygenerować raporty, zarchiwizować logi do celów kontrolnych lub przedstawić dane dowodowe w razie incydentu[7].

Kluczowe obszary audytu bezpieczeństwa mobilnego. W ramach audytu warto uwzględnić kilka istotnych obszarów związanych z bezpieczeństwem mobilnym[35]:

- **Przeszkolenie pracowników:** Szkolenia z zakresu ochrony danych osobowych pomagają zwiększyć świadomość i odpowiedzialność zespołu[35].

- **Ochrona danych w chmurze:** Weryfikacja, jak dane są przechowywane i przetwarzane w chmurze, jest niezbędna dla zgodności z RODO[35].
- **Bezpieczeństwo sieci:** Analiza zabezpieczeń sieciowych, w tym firewalle i systemy detekcji intruzów[35].
- **Procedury reakcji na incydenty:** Opracowanie i testowanie planów działania w przypadku naruszenia danych[35].

3.3.2 Mapowanie zgodności z wymaganiami NIS2

Dokument "Mapowanie zgodności z wymaganiami NIS2"ocenia, jak procesy, polityki i systemy spełniają wymagania NIS2, wskazując luki i obszary do poprawy[36]. Kluczowe elementy mapowania zgodności obejmują analizę wymagań dyrektywy, takich jak zarządzanie ryzykiem bezpieczeństwa cybernetycznego, zgłaszanie incydentów, ochrona sieci i systemów informacyjnych oraz odpowiedzialność kadry zarządzającej[36].

System MDM wspiera realizację zgodności poprzez tworzenie szczegółowej tabeli mapowania, która przedstawia wymaganie NIS2, informację o zgodności (Tak/Nie/Częściowo), dowody zgodności w postaci linków do polityk i procedur, identyfikację luk oraz rekomendacje działań naprawczych[36]. Przykładowo, w obszarze zarządzania ryzykiem, gdzie wymagane jest wdrożenie środków zarządzania ryzykiem, obecne praktyki mogą obejmować polityki ISO 27001, lecz może brakować formalnego planu naprawczego[36].

3.3.3 Automatyzacja raportowania i ciągły monitoring

Funkcja systematycznego raportowania wspiera proces przygotowań do audytów zewnętrznych lub certyfikacji[7]. Oferuje szeroki zakres audytów zgodności (compliance), które stanowią weryfikację i ocenę czy działania organizacji, tj. jej procedury oraz systemy spełniają wymagania wobec określonych standardów i regulacji prawnych[37].

Kluczowe dokumenty, które powinny być generowane automatycznie przez system MDM, obejmują[37]:

- Politykę bezpieczeństwa informacji (Information Security Policy)
- Politykę zarządzania ryzykiem (Risk Management Policy)
- Politykę ochrony danych osobowych (jeśli dotyczy RODO/GDPR)
- Procedurę zarządzania incydentami bezpieczeństwa (Incident Response Plan)
- Rejestr aktywów (Asset Register) dla urządzeń mobilnych
- Rejestr ryzyk związanych z cyberbezpieczeństwem

Regularne generowanie raportów oraz archiwizacja logów stanowią fundament dla wykazania rozliczalności w rozumieniu art. 5 ust. 2 RODO[7], a także umożliwiają organizacji wykazanie spełnienia minimum środków zarządzania ryzykiem wymaganych przez dyrektywę NIS2[36].

Rozdział 4

Wymagania prawne i regulacyjne

4.1 Implikacje Prawne i Regulacyjne dla Zarządzania Mobilnością w Sektorze Publicznym

Wdrożenie i eksploatacja systemów zarządzania urządzeniami mobilnymi (MDM) w jednostkach samorządu terytorialnego (JST) nie jest wyłącznie decyzją o charakterze technologicznym. Stanowi ono fundamentalny element strategii zapewnienia zgodności (ang. *compliance*) z dynamicznie ewoluującym porządkiem prawnym[7]. Zgodność ta nie jest stanem jednorazowym, lecz ciągłym procesem monitorowania, adaptacji i wykazywania należytej staranności w ochronie zasobów informacyjnych[17]. Dwa akty prawne Unii Europejskiej w sposób szczególny determinują obowiązki JST w tym obszarze: ogólne rozporządzenie o ochronie danych (RODO) oraz dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2)[16].

4.1.1 RODO jako fundament ochrony danych na urządzeniach mobilnych

Jednostki samorządu terytorialnego, jako administratorzy danych osobowych milionów obywateli, podlegają rygorystycznym obowiązkom wynikającym z RODO[13, 14]. Centralną zasadą jest tu **podejście oparte na ryzyku**[38]. Kluczowy **art. 32 RODO** nakłada na administratora obowiązek wdrożenia „odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku" naruszenia praw lub wolności osób fizycznych[14, 38]. W kontekście floty mobilnej, gdzie ryzyko utraty lub nieautoryzowanego dostępu jest immanentnie wysokie, system MDM stanowi bezpośrednią i wymierną realizację tego wymogu[7].

Co więcej, platforma MDM jest kluczowym narzędziem do implementacji fundamentalnych zasad RODO, takich jak **ochrona danych w fazie projektowania (*privacy by design*)** oraz **domyślna ochrona danych (*privacy by default*)**, o których mowa w art. 25 RODO[39, 40]. Umożliwia ona bowiem wbudowanie mechanizmów ochronnych w samą architekturę środowiska mobilnego, a nie jedynie ich „doklejenie" na późniejszym etapie[39].

Zapewnienie poufności, integralności i kontroli dostępu

Zgodnie z zasadą integralności i poufności (art. 5 ust. 1 lit. f RODO), dane muszą być przetwarzane w sposób zapewniający ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem[38]. System MDM realizuje ten postulat poprzez szeroki wachlarz mechanizmów technicznych[7]:

- Wymuszanie stosowania silnych, regularnie zmienianych haseł dostępowych do urządzeń.
- Egzekwowanie polityki uwierzytelniania wieloskładnikowego (MFA), które drastycznie podnosi barierę nieautoryzowanego dostępu.
- Definiowanie precyzyjnych ról i uprawnień dostępu do danych z poziomu urządzeń mobilnych, realizując zasadę minimalizacji uprawnień (*principle of least privilege*)[7].

Szyfrowanie danych jako wzorcowy środek techniczny

Artykuł 32 RODO wprost wymienia pseudonimizację i szyfrowanie danych osobowych jako przykładowe, wzorcowe środki techniczne służące zabezpieczeniu przetwarzania[38]. Platforma MDM umożliwia centralne wymuszenie, monitorowanie i zarządzanie szyfrowaniem danych w dwóch stanach[7]:

- **Dane w spoczynku (*data-at-rest*):** Egzekwowanie szyfrowania pamięci masowej urządzenia (np. za pomocą natywnych technologii BitLocker dla Windows czy FileVault dla macOS), co chroni dane w przypadku fizycznej kradzieży sprzętu[7].
- **Dane w tranzycie (*data-in-transit*):** Automatyczna konfiguracja i wymuszanie korzystania z bezpiecznych, szyfrowanych połączeń sieciowych, takich jak VPN (Virtual Private Network), w celu ochrony danych przesyłanych poza zaufaną sieć urzędu[7].

Zdolność do reagowania na incydenty i minimalizacja szkód

W przypadku fizycznej utraty lub kradzieży urządzenia, administrator musi posiadać zdolność do szybkiego i skutecznego reagowania[7]. Funkcja **zdalnego wymazania danych (*remote wipe*)** w systemach MDM jest tu kluczowym narzędziem[25]. Pozwala ona na bezzwłoczne, zdalne usunięcie informacji służbowych, co zapobiega ich wpadnięciu w niepowołane ręce[25]. Jest to niezwykle istotne w kontekście obowiązku zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu (art. 33 RODO)[41]. Skuteczne i udokumentowane użycie funkcji *remote wipe* może stanowić argument, że do naruszenia, które wymaga notyfikacji, w ogóle nie doszło, lub że jego skutki zostały skutecznie zminimalizowane[41].

Realizacja zasady rozliczalności

System MDM, poprzez automatyczne i szczegółowe generowanie dzienników zdarzeń (logów) oraz raportów, dostarcza niepodważalnych dowodów na stosowanie odpowiednich środków ochrony[7]. Dokumentowanie konfiguracji, statusu zgodności urządzeń, prób dostępu oraz przeprowadzonych działań (np. zdalnego wymazania) jest niezbędne do wykazania zgodności z RODO przed organem nadzorczym (Prezesem Urzędu Ochrony Danych Osobowych)[42]. Realizuje to wprost fundamentalną zasadę **rozliczalności** (art. 5 ust. 2 RODO), która wymaga od administratora zdolności do udowodnienia przestrzegania przepisów[42].

4.1.2 Dyrektywa NIS2 i nowy status JST jako podmiotu kluczowego

Dyrektywa NIS2[16], zastępująca swoją poprzedniczkę z 2016 roku, znacząco rozszerza katalog podmiotów objętych obowiązkiem stosowania rygorystycznych środków zarządzania ryzykiem w cyberbezpieczeństwie[17]. Co kluczowe dla sektora publicznego, włącza ona do tego grona **organy administracji publicznej na szczeblu centralnym, regionalnym i lokalnym**, klasyfikując je jako „podmioty kluczowe" lub „ważne"[17].

Implikacje tego faktu są dalekosiężne[17]. Nakłada to na JST obowiązek wdrożenia kompleksowej, proaktywnej i opartej na analizie ryzyka strategii cyberbezpieczeństwa[17]. System MDM/UEM jest nieodzownym komponentem takiej strategii, wspierając realizację co najmniej dziesięciu minimalnych środków zarządzania ryzykiem, o których mowa w art. 21 dyrektywy:

- **Polityki analizy ryzyka i bezpieczeństwa systemów informacyjnych:** MDM pozwala na identyfikację, ocenę i mitygację ryzyk związanych z wykorzystaniem urządzeń mobilnych oraz jest technicznym narzędziem do egzekwowania przyjętych polityk bezpieczeństwa.

- **Obsługa incydentów:** Platforma dostarcza danych telemetrycznych i logów niezbędnych do wykrywania, analizy i reagowania na incydenty bezpieczeństwa dotyczące floty mobilnej, co jest jednym z podstawowych obowiązków.

- **Bezpieczeństwo łańcucha dostaw:** Poprzez restrykcyjną kontrolę instalowanych aplikacji (MAM) i konfiguracji, MDM pomaga w zabezpieczeniu „łańcucha dostaw" oprogramowania i usług, z których korzystają pracownicy na swoich urządzeniach.

- **Higiena cybernetyczna i szkolenia w zakresie cyberbezpieczeństwa:** MDM wymusza podstawowe zasady higieny, takie jak stosowanie silnych haseł czy regularne aktualizacje.

- **Polityki i procedury oceny skuteczności środków zarządzania ryzykiem:** Regularne raporty generowane przez system MDM stanowią kluczowy wkład w procesy audytu i oceny skuteczności wdrożonych środków, czego explicite wymaga dyrektywa.

- **Stosowanie kryptografii i szyfrowania:** Jak omówiono w kontekście RODO, MDM centralnie zarządza politykami szyfrowania.

Szczególnie istotnym zapisem NIS2 jest art. 20, który nakłada **bezpośrednią odpowiedzialność na organy zarządzające** podmiotów kluczowych i ważnych. Muszą one zatwierdzać środki zarządzania ryzykiem oraz nadzorować ich wdrażanie, a także przechodzić specjalistyczne szkolenia. System MDM, dostarczając przejrzystych pulpitów nawigacyjnych (dashboardów) i raportów, jest narzędziem, które pozwala kierownictwu JST wypełnić ten obowiązek nadzorczy[7].

W konsekwencji, implementacja platformy MDM/UEM przestaje być postrzegana jako dobra praktyka czy inwestycja w efektywność, a staje się strategiczną koniecznością[17]. Jest ona warunkiem *sine qua non* zdolności jednostek samorządu terytorialnego do sprostania nowym, rygorystycznym wymogom prawa unijnego i budowy realnej odporności cyfrowej[17].

Rozdział 5

Proces wdrażania systemu MDM

5.1 Proces Wdrożeniowy: Przewodnik Metodyczny dla Sektora Publicznego

Skuteczna implementacja systemu zarządzania urządzeniami mobilnymi (MDM/UEM) jest złożonym projektem o charakterze socjotechnicznym, który wymaga metodycznego i wieloetapowego podejścia, wykraczającego daleko poza samą instalację oprogramowania[7]. Sukces projektu zależy w równej mierze od dojrzałości technologicznej, co od starannego planowania, zarządzania zmianą oraz pozyskania akceptacji użytkowników końcowych[18]. Poniżej przedstawiono czteroetapowy model procesu wdrożeniowego, który może służyć jako ustrukturyzowana mapa drogowa dla jednostek samorządu terytorialnego (JST).

5.1.1 Etap 1: Faza analityczno-strategiczna i definicja zakresu

Szacowany czas trwania: 4–6 tygodni

Celem tej fundamentalnej fazy jest zdefiniowanie zakresu, celów i ram projektu[18]. Błędy lub zaniechania na tym etapie nieuchronnie prowadzą do komplikacji w dalszych fazach[7]. Kluczowe działania obejmują:

Inwentaryzacja i audyt stanu obecnego

Pierwszym krokiem jest dokładna inwentaryzacja wszystkich urządzeń mobilnych wykorzystywanych w organizacji[7]. Należy zebrać dane dotyczące ich liczby, modeli, wersji systemów operacyjnych oraz, co kluczowe, modelu własności[43]. Audyt powinien sklasyfikować urządzenia w ramach następujących modeli[43, 44]:

- **COBO (*Corporate-Owned, Business-Only*):** Urządzenia w pełni służbowe, z zablokowaną możliwością użytku prywatnego[44].
- **COPE (*Corporate-Owned, Personally-Enabled*):** Urządzenia służbowe z dopuszczonym ograniczonym użytkiem prywatnym[43, 44].
- **BYOD (*Bring Your Own Device*):** Urządzenia prywatne wykorzystywane do celów służbowych, co stanowi największe wyzwanie w kontekście ochrony danych i prywatności[43, 44].

Równolegle przeprowadza się audyt obecnego poziomu bezpieczeństwa, identyfikując istniejące polityki (lub ich brak), luki w zabezpieczeniach oraz analizując dotychczasowe incydenty[7]. Celem jest stworzenie mapy ryzyka dla środowiska mobilnego[18].

Definicja wymagań funkcjonalnych, technicznych i organizacyjnych

Na podstawie audytu oraz analizy potrzeb poszczególnych komórek organizacyjnych tworzona jest szczegółowa lista wymagań[7]. Musi ona uwzględniać nie tylko wymogi techniczne (np. wsparcie dla konkretnych platform, możliwości integracyjne), ale również te wynikające z regulacji prawnych (RODO, NIS2) oraz wewnętrznych polityk bezpieczeństwa[17]. Należy zdefiniować **przypadki użycia** (ang. *use cases*) oraz **persony użytkowników** (np. pracownik terenowy, kadra zarządzająca, urzędnik biurowy), aby dostosować polityki do realnych potrzeb, a nie tworzyć jednego, restrykcyjnego szablonu dla wszystkich[18].

Określenie ram projektowych i powołanie zespołu

W tej fazie opracowywany jest wstępny budżet, który musi uwzględniać **całkowity koszt posiadania (TCO)**: koszty licencji, wdrożenia, integracji, szkoleń oraz rocznego utrzymania i wsparcia[45, 46]. Tworzony jest również realistyczny harmonogram projektu z jasno określonymi kamieniami milowymi[7]. Kluczowe jest powołanie interdyscyplinarnego zespołu projektowego, w skład którego powinni wejść przedstawiciele działu IT, bezpieczeństwa, prawnego, kadr oraz kluczowych jednostek biznesowych[18].

5.1.2 Etap 2: Wybór rozwiązania i dostawcy

Szacowany czas trwania: 6–8 tygodni

Etap ten koncentruje się na wyborze technologii i partnera wdrożeniowego, który najlepiej odpowiada zdefiniowanym wymaganiom[7]. Należy pamiętać, że w sektorze publicznym proces ten jest często sformalizowany przez przepisy o zamówieniach publicznych[18].

Analiza rynku i preselekcja kandydatów

Na podstawie publicznie dostępnych informacji, raportów czołowych firm analitycznych (np. Gartner Magic Quadrant for UEM, Forrester Wave) oraz rekomendacji branżowych tworzona jest tzw. **długa lista** potencjalnych rozwiązań MDM[7]. Następnie, poprzez konfrontację ich specyfikacji z kluczowymi, bezwzględnymi wymaganiami projektu (np. model chmurowy z danymi na terenie UE, wsparcie dla konkretnego systemu operacyjnego), lista jest zawężana do kilku (zazwyczaj 3–5) najbardziej obiecujących kandydatów, tworząc tzw. **krótką listę**[18].

Szczegółowa ocena i testy koncepcyjne (Proof of Concept)

Wybrane rozwiązania poddawane są dogłębnej analizie porównawczej, często z wykorzystaniem **matrycy decyzyjnej**[7]. Pozwala ona na obiektywną, ważoną ocenę poszczególnych kryteriów, takich jak funkcjonalność, skalowalność, model licencjonowania i TCO[45]. Kluczowym elementem jest przeprowadzenie testów w formie **Proof**

of Concept (PoC)[47]. Podczas PoC rozwiązanie jest instalowane w ograniczonym środowisku testowym JST w celu weryfikacji jego kluczowych funkcji, wydajności oraz łatwości zarządzania w praktyce, ze szczególnym uwzględnieniem najbardziej złożonych przypadków użycia[47].

Weryfikacja referencji i negocjacje umowy

Równolegle do testów PoC, weryfikowane są referencje dostawców, ze szczególnym naciskiem na udokumentowane, pomyślne wdrożenia w innych podmiotach sektora publicznego[7]. Po wyborze finalnego rozwiązania następują negocjacje warunków umowy[18]. Szczególną uwagę należy zwrócić na zapisy dotyczące **poziomu świadczenia usług (SLA – *Service Level Agreement*)**, które powinny precyzować m.in. czas reakcji na incydenty, gwarancje dostępności usługi oraz kary umowne[48].

5.1.3 Etap 3: Implementacja techniczna i konfiguracja

Szacowany czas trwania: 2–4 tygodnie

Jest to faza technicznego przygotowania systemu do pracy, realizowana w ścisłej współpracy z wybranym dostawcą[7].

Instalacja i przygotowanie infrastruktury

W zależności od wybranego modelu (on-premise vs. chmura), etap ten obejmuje przygotowanie serwerów lub konfigurację instancji usługi w chmurze[7]. Następuje instalacja oprogramowania MDM zgodnie z najlepszymi praktykami (*best practices*) rekomendowanymi przez producenta oraz utwardzenie (*hardening*) konfiguracji serwerów[18].

Integracja z kluczowymi systemami korporacyjnymi

W celu automatyzacji i centralizacji zarządzania, system MDM jest integrowany z istniejącą infrastrukturą IT JST[7]. Najczęściej dotyczy to integracji z[18]:

- **Usługami katalogowymi** (np. Active Directory, Azure AD) w celu synchronizacji tożsamości użytkowników i grup[7].
- **Infrastrukturą klucza publicznego (PKI)** do automatycznej dystrybucji certyfikatów klienckich na urządzenia[7].
- **Systemami SIEM** (*Security Information and Event Management*) w celu przesyłania logów i korelacji zdarzeń bezpieczeństwa[29].

Konfiguracja polityk bezpieczeństwa i profili użytkowników

To merytoryczne serce wdrożenia[7]. Administratorzy, na podstawie wymagań z etapu 1, tworzą i konfigurują polityki bezpieczeństwa[30]. Definiowane są profile dla różnych grup użytkowników i modeli własności (COPE vs. BYOD), konfigurowane są reguły dotyczące haseł, szyfrowania, ograniczeń aplikacji (MAM), dostępu do sieci oraz reguły zgodności (*compliance rules*), które warunkują dostęp do danych służbowych[31].

5.1.4 Etap 4: Wdrożenie, komunikacja i utrzymanie operacyjne

Faza ciągła

Uruchomienie systemu to początek jego cyklu życia w organizacji[7]. Faza ta jest równie krytyczna jak poprzednie i wymaga ciągłego zaangażowania[18].

Komunikacja, szkolenia i zarządzanie zmianą

Kluczowym czynnikiem sukcesu jest pozyskanie akceptacji użytkowników[18]. Należy przeprowadzić transparentną kampanię informacyjną, wyjaśniającą cele i korzyści z wdrożenia MDM, a także jasno komunikującą, jakie dane są monitorowane, a jakie pozostają prywatne (szczególnie w modelu BYOD)[43]. Należy zorganizować dedykowane szkolenia dla pracowników (użytkowników końcowych), personelu helpdesku oraz administratorów systemu[7].

Wdrożenie pilotażowe i weryfikacja

Przed pełnym uruchomieniem systemu w całej organizacji, przeprowadza się wdrożenie pilotażowe na ograniczonej, lecz reprezentatywnej grupie użytkowników[18]. Pozwala to na wychwycenie i usunięcie ewentualnych problemów konfiguracyjnych w kontrolowanym środowisku oraz zebranie cennych informacji zwrotnych od użytkowników[7].

Pełne wdrożenie i stałe monitorowanie

Po sukcesie pilotażu następuje etapowe, kontrolowane wdrożenie systemu dla wszystkich docelowych użytkowników[11, 21]. Od tego momentu rozpoczyna się faza eksploatacji, która polega na bieżącym monitorowaniu stanu zgodności urządzeń, proaktywnym reagowaniu na incydenty, regularnym generowaniu raportów dla kierownictwa oraz okresowym przeglądzie i dostosowywaniu polityk bezpieczeństwa do zmieniających się zagrożeń i potrzeb organizacji[7]. Jest to proces ciągłego doskonalenia, a nie jednorazowe zadanie[18].

Rozdział 6

Analiza Ekonomiczna i Źródła Finansowania

6.1 Całkowity Koszt Posiadania (TCO) Systemu MDM

Decyzja o wdrożeniu systemu klasy **Mobile Device Management (MDM)** jest inwestycją strategiczną, która wymaga starannej i wielowymiarowej analizy ekonomicznej[7]. Podejście oparte wyłącznie na ocenie początkowego kosztu zakupu licencji jest fundamentalnie błędne i nie odzwierciedla rzeczywistego obciążenia finansowego w całym cyklu życia technologii[45, 46]. Prawidłową metryką oceny jest **Całkowity Koszt Posiadania** (ang. *Total Cost of Ownership*, TCO), który uwzględnia zarówno jednorazowe nakłady inwestycyjne, jak i wszystkie bieżące koszty operacyjne[45, 49].

6.1.1 Struktura nakładów: inwestycje (CapEx) a koszty operacyjne (OpEx)

Koszty w modelu TCO można podzielić na dwie główne kategorie, których proporcje zależą w dużej mierze od wybranego modelu wdrożenia: lokalnego (*on-premise*) lub chmurowego (*Software as a Service*, SaaS)[45].

Nakłady inwestycyjne (CapEx)

Obejmują one wszystkie jednorazowe wydatki, ponoszone głównie na początku projektu, niezbędne do jego uruchomienia[45]. Są one dominujące w modelu *on-premise*[7]. Należą do nich[49]:

- **Licencje oprogramowania:** Koszt zakupu wieczystych licencji na oprogramowanie serwerowe i klienckie[7].
- **Infrastruktura sprzętowa:** W przypadku wdrożenia lokalnego, konieczny jest zakup lub modernizacja serwerów, macierzy dyskowych, urządzeń sieciowych oraz ewentualnie systemów do tworzenia kopii zapasowych[45].
- **Usługi wdrożeniowe i profesjonalne:** Koszty związane z pracą wyspecjalizowanych konsultantów zewnętrznych lub wewnętrznych, odpowiedzialnych za

analizę przedwdrożeniową, instalację, konfigurację systemu, integrację z istniejącą infrastrukturą (np. Active Directory, PKI) oraz wsparcie podczas migracji danych[7].

- **Szkolenia inicjalne:** Koszt pierwszych, kompleksowych szkoleń dla administratorów systemu oraz personelu helpdesk[18].

Koszty operacyjne (OpEx)

Są to cykliczne, bieżące wydatki związane z utrzymaniem i eksploatacją systemu[45]. Stanowią one główny składnik kosztowy w modelu SaaS, minimalizując jednocześnie początkowe nakłady CapEx[49]. Do tej kategorii zaliczamy[46]:

- **Opłaty subskrypcyjne lub wsparcie techniczne:** W modelu SaaS są to regularne, najczęściej roczne lub miesięczne, opłaty za korzystanie z usługi, obejmujące dostęp do platformy, wsparcie i aktualizacje[7]. W modelu *on-premise* są to roczne koszty odnowienia pakietu wsparcia technicznego i utrzymania oprogramowania (*maintenance*)[45].

- **Zasoby ludzkie:** Koszty utrzymania (wynagrodzenia) personelu IT odpowiedzialnego za codzienną administrację platformą MDM, monitorowanie bezpieczeństwa, analizę incydentów, zarządzanie politykami i wsparcie użytkowników końcowych[18].

- **Szkolenia ustawiczne:** Wydatki na cykliczne szkolenia personelu w celu utrzymania wysokich kompetencji w obsłudze systemu, poznawania nowych funkcji oraz reagowania na ewoluujące zagrożenia[7].

- **Koszty infrastrukturalne (w modelu on-premise):** Zużycie energii elektrycznej, klimatyzacja serwerowni, koszty odnawiania certyfikatów SSL etc[45].

6.1.2 Zwrot z Inwestycji (ROI) i mitygacja ryzyka

Inwestycja w system MDM, mimo początkowych kosztów, generuje wymierny zwrot z inwestycji (ROI)[50]. Szacunki rynkowe wskazują, że w zależności od skali organizacji i zakresu wdrożenia, zwrot ten może nastąpić w perspektywie 12 do 24 miesięcy. ROI jest generowany na dwóch płaszczyznach[50]:

Oszczędności bezpośrednie (twarde ROI). Wynikają z automatyzacji i optymalizacji procesów, co bezpośrednio przekłada się na redukcję kosztów operacyjnych[50]:

- **Redukcja czasu pracy działu IT:** Automatyczne wdrażanie (*zero-touch deployment*) i konfiguracja urządzeń eliminują czasochłonne, manualne przygotowywanie sprzętu dla pracowników[11, 21].

- **Obniżenie kosztów wsparcia technicznego:** Centralne zarządzanie i możliwość zdalnej diagnostyki problemów redukują liczbę i czas obsługi zgłoszeń serwisowych[7].

- **Optymalizacja zarządzania zasobami:** Dokładna inwentaryzacja sprzętu i oprogramowania pozwala na lepsze planowanie zakupów i unikanie niepotrzebnych wydatków[18].

Uniknięcie strat (miękkie ROI). Jest to kluczowy, choć trudniejszy do bezpośredniego skwantyfikowania, aspekt zwrotu z inwestycji[50]. Polega na mitygacji ryzyka finansowego i wizerunkowego[50]:

- **Uniknięcie kar finansowych:** Zapewnienie zgodności z RODO i NIS2 minimalizuje ryzyko nałożenia wysokich kar administracyjnych za naruszenia bezpieczeństwa (sięgających milionów euro)[14, 17].

- **Redukcja kosztów obsługi incydentów:** Zapobieganie wyciekom danych eliminuje koszty związane z ich usuwaniem – analizą powłamaniową, obsługą prawną, komunikacją kryzysową i ewentualnymi odszkodowaniami[7].

- **Ochrona wizerunku i zaufania publicznego:** Utrata danych obywateli może prowadzić do nieodwracalnego kryzysu zaufania do instytucji, którego koszt jest niemożliwy do oszacowania[7].

6.2 Możliwości finansowania w ramach programu „Cyberbezpieczny Samorząd"

Mając na uwadze strategiczne znaczenie cyberbezpieczeństwa dla funkcjonowania państwa oraz świadomość barier inwestycyjnych, administracja rządowa uruchomiła dedykowane mechanizmy wsparcia dla jednostek samorządu terytorialnego[19]. Kluczowym instrumentem jest tutaj program priorytetowy **„Cyberbezpieczny Samorząd"**, realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy (FERC) przez Centrum Projektów Polska Cyfrowa (CPPC) pod auspicjami Ministerstwa Cyfryzacji[19, 51].

Program ten został zaprojektowany w celu systemowego podniesienia odporności JST na cyberzagrożenia i stanowi bezpośrednią odpowiedź na obowiązki wynikające z dyrektywy NIS2[17, 19]. Co istotne, wdrożenie systemów klasy MDM/UEM jest jednym z kluczowych obszarów, które mogą podlegać dofinansowaniu w ramach tego grantu[19]. Najważniejsze założenia programu to:

Poziom dofinansowania Program oferuje granty pokrywające **do 100% kosztów kwalifikowalnych** projektu[19]. Eliminuje to niemal całkowicie barierę finansową dla JST, przesuwając punkt ciężkości z pytania „czy nas stać?" na „jak to zrobić najlepiej?"[19].

Wysokość wsparcia Maksymalna kwota dofinansowania jest zróżnicowana i uzależniona od typu oraz wielkości JST (gminy, związki międzygminne, powiaty, województwa), wahając się od 200 tys. zł do 850 tys. zł[19]. Zapewnia to sprawiedliwą dystrybucję środków, adekwatną do skali potrzeb[19].

Zakres finansowania Program umożliwia finansowanie szerokiego katalogu wydatków w trzech obszarach: organizacyjnym, technicznym i edukacyjnym[19]. W obszarze technicznym wprost kwalifikuje się zakup oprogramowania i licencji (zarówno w modelu *on-premise*, jak i chmurowym), usług wdrożeniowych oraz niezbędnych szkoleń technicznych dla personelu[19].

Możliwość skorzystania z grantu w ramach programu „Cyberbezpieczny Samorząd" stanowi dla jednostek samorządu terytorialnego unikalną i historyczną szansę na skokowe podniesienie poziomu dojrzałości w zakresie cyberbezpieczeństwa, w tym bezpieczeństwa mobilnego, przy minimalnym obciążeniu własnego budżetu[19, 51].

Bibliografia

[1] Ministerstwo Funduszy i Polityki Regionalnej. *Smart City Forum: wzrasta rola cyfryzacji w procesie rozwoju miast.* URL: https://www.gov.pl/web/fundusze-regiony/smart-city-forum-wzrasta-rola-cyfryzacji-w-procesie-rozwoju-miast (term. wiz. 11. 06. 2025).

[2] Urząd m.st. Warszawy. *Polityka cyfrowej transformacji m.st. Warszawy.* URL: https://um.warszawa.pl/waw/strategia/-/artykul-235 (term. wiz. 11. 06. 2025).

[3] Enova365. *Samorząd terytorialny - funkcje systemu do zarządzania dla samorządów.* URL: https://www.enova.pl/blog/enova365-w-praktyce/samorzad-terytorialny-poznaj-funkcje-zintegrowanego-systemu-do-zarzadzania-dla-samorzadow/ (term. wiz. 11. 06. 2025).

[4] Aleksandra Kowalczyk i Maria Stępień. "Wpływ pandemii COVID-19 na funkcjonowanie urzędów organów administracji publicznej". W: *Studia z Zakresu Prawa, Administracji i Zarządzania UKW* 16.1 (2023), s. 45–60. URL: https://izss.uken.krakow.pl/wp-content/uploads/sites/13/2023/01/Aleksandra-Kowalczyk-Maria-Stepien-Wplyw-pandemii-COVID-19-na-funkcjonowanie-urzedow-organow-administracji-publicznej.pdf (term. wiz. 11. 06. 2025).

[5] Główny Urząd Statystyczny. *Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej w 2023 roku.* Spraw. tech. Główny Urząd Statystyczny, 2023. URL: https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-w-2023-roku,7,6.html (term. wiz. 11. 06. 2025).

[6] IBM. *What is Mobile Device Management (MDM)?* MDM is a proven methodology and toolset used to provide a workforce mobile productivity tools and applications while keeping corporate data secure. URL: https://www.ibm.com/think/topics/mobile-device-management (term. wiz. 11. 06. 2025).

[7] CyberKatalog.pl. *MDM | Mobile Device Management.* URL: https://CyberKatalog.pl/slownik/mdm (term. wiz. 11. 06. 2025).

[8] CyberKatalog.pl. *BYOD | Bring Your Own Device.* URL: https://CyberKatalog.pl/slownik/byod (term. wiz. 11. 06. 2025).

[9] CyberKatalog.pl. *EMM | Enterprise Mobility Management.* URL: https://CyberKatalog.pl/slownik/emm (term. wiz. 11. 06. 2025).

[10] CyberKatalog.pl. *UEM | Unified Endpoint Management*. URL: https://CyberKatalog.pl/slownik/uem (term. wiz. 11. 06. 2025).

[11] Scalefusion. *Jak wdrożenie typu Zero-Touch pomaga administratorom IT?* Scalefusion. URL: https://blog.scalefusion.com/pl/zero-touch-deployment-for-bulk-device-enrollment/ (term. wiz. 11. 06. 2025).

[12] Fortinet. *What Is Mobile Device Management (MDM)? Why is it Important?* MDM means mobile device management, which is a type of software that enables organizations to monitor, manage, and secure their employees' mobile devices. URL: https://www.fortinet.com/resources/cyberglossary/mobile-device-management (term. wiz. 11. 06. 2025).

[13] Parlament Europejski i Rada UE. "Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych". W: *Dziennik Urzędowy Unii Europejskiej* L 119/1 (2016). Ogólne rozporządzenie o ochronie danych (RODO). URL: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679 (term. wiz. 11. 06. 2025).

[14] GDPR-Info.eu. *Art. 32 GDPR – Security of processing*. Artykuł 32 RODO dotyczący bezpieczeństwa przetwarzania danych osobowych. 2018. URL: https://gdpr-info.eu/art-32-gdpr/ (term. wiz. 11. 06. 2025).

[15] CRN. *RODO a cyberbezpieczeństwo mobilne*. URL: https://crn.pl/artykuly/rodo-a-cyberbezpieczenstwo-mobilne/ (term. wiz. 11. 06. 2025).

[16] Parlament Europejski i Rada UE. "Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii". W: *Dziennik Urzędowy Unii Europejskiej* L 333/80 (2022). Dyrektywa NIS2 dotycząca cyberbezpieczeństwa. URL: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555 (term. wiz. 11. 06. 2025).

[17] Atende. *Dyrektywa NIS2 i jej wpływ na jednostki administracji publicznej*. URL: https://atende.pl/pl/blog/sektor-publiczny-dyrektywa-nis2-i-jej-wplyw-na-jednostki-administracji-publicznej/ (term. wiz. 11. 06. 2025).

[18] Apple. *Intro to mobile device management profiles*. Apple Inc. URL: https://support.apple.com/en-gb/guide/deployment/depc0aadd3fe/web (term. wiz. 11. 06. 2025).

[19] Centrum Projektów Polska Cyfrowa. *Cyberbezpieczny Samorząd*. Oficjalna strona programu grantowego. URL: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (term. wiz. 11. 06. 2025).

[20] Apple Support. *Automated Device Enrollment and MDM*. Apple Inc. URL: https://support.apple.com/guide/deployment/automated-device-enrollment-and-mdm-dep73069dd57/web (term. wiz. 11. 06. 2025).

[21] Trio MDM. *Zero-Touch Deployment: Understanding the Key Concepts*. URL: https://www.trio.so/blog/zero-touch-deployment (term. wiz. 11. 06. 2025).

[22] Apple Support. *Use Automated Device Enrollment*. Apple Inc. URL: https://support.apple.com/en-us/guide/apple-business-manager/axm2ad7b203f/web (term. wiz. 11. 06. 2025).

[23] Google. *Android Zero-Touch Enrollment*. Google LLC. URL: https://www.android.com/enterprise/management/zero-touch/ (term. wiz. 11. 06. 2025).

[24] Microsoft. *Windows Autopilot: How It Works & How to Set It Up*. URL: https://www.youtube.com/watch?v=zqwkaWTzsRo (term. wiz. 11. 06. 2025).

[25] TechTarget. *What is a Remote Wipe? | Definition from TechTarget*. Remote wipe is a security feature that allows a network administrator or device owner to send a command that remotely deletes data from a computing device. URL: https://www.techtarget.com/searchmobilecomputing/definition/remote-wipe (term. wiz. 11. 06. 2025).

[26] Trio MDM. *Managing BYOD with MDM Containerization: The Ultimate Guide*. MDM containerization enables companies to separate corporate data from personal data and apps, and follow strict security regulations. URL: https://www.trio.so/blog/mdm-containerization/ (term. wiz. 11. 06. 2025).

[27] Green Eris. *Jak Conditional Access zwiększa bezpieczeństwo firmowych danych?* URL: https://one.greeneris.com/jak-conditional-access-zwieksza-bezpieczenstwo-firmowych-danych/ (term. wiz. 11. 06. 2025).

[28] Reddit r/Intune community. *Entra Registered devices and compliance status*. Dyskusja społeczności technicznej na temat statusu zgodności urządzeń. URL: https://www.reddit.com/r/Intune/comments/1amyzu1/entra_registered_devices_and_compliance_status/ (term. wiz. 11. 06. 2025).

[29] CyberKatalog.pl. *SIEM | Security Information and Event Management*. URL: https://CyberKatalog.pl/slownik/siem (term. wiz. 11. 06. 2025).

[30] Scalefusion. *Czym jest polityka zarządzania urządzeniami mobilnymi (MDM)?* URL: https://blog.scalefusion.com/pl/what-is-an-mdm-policy/ (term. wiz. 11. 06. 2025).

[31] Proget. *Polityki bezpieczeństwa - spójne zasady korzystania z urządzeń*. URL: https://proget.pl/polityki/ (term. wiz. 11. 06. 2025).

[32] Strony Internetowe UK. *Dostęp warunkowy - jak kontrolować dostęp do danych w firmie?* URL: https://stronyinternetowe.uk/dostep-warunkowy-jak-kontrolowac-dostep-do-danych-w-firmie/ (term. wiz. 11. 06. 2025).

[33] Eura-Tech. *Kontrola dostępu w obliczu RODO*. URL: https://eura-tech.eu/blog/kontrola-dostepu-w-obliczu-rodo/ (term. wiz. 11. 06. 2025).

[34] Microsoft. *What is access control?* Microsoft Corporation. URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview (term. wiz. 11. 06. 2025).

[35] Perception Point. "BYOD Security: Threats, Security Measures and Best Practices". W: *Cybersecurity Research* (2024). Comprehensive analysis of BYOD security risks and mitigation strategies in enterprise environments. URL: https://perception-point.io/byod-security-threats-security-measures-and-best-practices/ (term. wiz. 11. 06. 2025).

[36] IEEE. "Systematic Literature Review on Organizational Cyber Security Deficiency in Mitigating Mobile Device Risk". W: *IEEE Conference Proceedings* (2021). Systematic literature review exploring cybersecurity deficiency and mitigating techniques for mobile device risk in organizational IS. URL: https://ieeexplore.ieee.org/document/9791959/ (term. wiz. 11. 06. 2025).

[37] California State University. "An Exploration of Mobile Device Security Artifacts At Institutions Of Higher Education". W: *Journal of Information Technology and Information Management* (2016). Study exploring mobile device security artifacts and compliance requirements in educational institutions. URL: https://scholarworks.lib.csusb.edu/jitim/vol25/iss3/4 (term. wiz. 11. 06. 2025).

[38] GDPR-Info.eu. *Art. 32 GDPR – Security of processing*. Angielska wersja z interpretacją Artykułu 32. URL: https://gdpr-info.eu/art-32-gdpr/ (term. wiz. 11. 06. 2025).

[39] IAPP. *Privacy by Design*. URL: https://iapp.org/resources/article/privacy-by-design/ (term. wiz. 11. 06. 2025).

[40] Intersoft Consulting. *Art. 25 GDPR - Data protection by design and by default*. URL: https://gdpr-info.eu/art-25-gdpr/ (term. wiz. 11. 06. 2025).

[41] GDPR-Info.eu. *Art. 33 GDPR – Notification of a personal data breach to the supervisory authority*. Wytyczne dotyczące obowiązku zgłaszania naruszeń ochrony danych osobowych. 2018. URL: https://gdpr-info.eu/art-33-gdpr/ (term. wiz. 11. 06. 2025).

[42] GDPR-Info.eu. *Art. 5 GDPR – Principles relating to processing of personal data*. Zasada rozliczalności określona w art. 5 ust. 2 RODO. 2018. URL: https://gdpr-info.eu/art-5-gdpr/ (term. wiz. 11. 06. 2025).

[43] DoubleOctopus. *What is Mobile Device Management? - Security Wiki*. Comprehensive overview of MDM technology and device management models including BYOD, COPE, and COBO. 2025. URL: https://doubleoctopus.com/security-wiki/network-architecture/mobile-device-management/ (term. wiz. 11. 06. 2025).

[44] Scalefusion. *What is Unified Endpoint Management (UEM)? Ultimate Guide*. Ultimate guide to Unified Endpoint Management and its evolution from MDM through EMM to UEM. 2013. URL: https://scalefusion.com/unified-endpoint-management-uem/what-is-uem (term. wiz. 11. 06. 2025).

[45] TechTarget. *What is total cost of ownership (TCO)?* URL: https://www.techtarget.com/searchdatacenter/definition/TCO (term. wiz. 11. 06. 2025).

[46] Goodman. *Total Cost of Ownership (TCO) w Zarządzaniu Zakupami*. URL: https://goodman.eu/zarzadzanie-zakupami/total-cost-of-ownership-tco-w-zarzadzaniu-zakupami/ (term. wiz. 11. 06. 2025).

[47] MIT. *Master Data Management: A Proof of Concept*. Spraw. tech. Academic paper presenting implementation of MDM architecture and proof of concept validation methodology. Massachusetts Institute of Technology, 2010. URL: http://mitiq.mit.edu/ICIQ/Documents/IQ%20Conference%202010/Papers/2B3_MDMProofOfConcept.pdf (term. wiz. 11. 06. 2025).

[48] *Service-level agreement*. Wikipedia. URL: https://en.wikipedia.org/wiki/Service-level_agreement (term. wiz. 11. 06. 2025).

[49] Agile Brand Guide. *Total Cost of Ownership (TCO)*. URL: https://agilebrandguide.com/wiki/metrics/total-cost-of-ownership-tco/ (term. wiz. 11. 06. 2025).

[50] Indeed. *What Is Total Cost of Ownership (TCO)? (Tips and Examples)*. Practical guide to understanding and calculating TCO in business decision-making processes. URL: https://www.indeed.com/career-advice/career-development/total-ownership-cost (term. wiz. 11. 06. 2025).

[51] PAP Samorząd. *Będą przesunięcia w budżecie FERC. Dodatkowe 2 mld zł na rozwój e-administracji i cyberbezpieczeństwo*. URL: https://samorzad.pap.pl/kategoria/e-urzad/beda-przesuniecia-w-budzecie-ferc-dodatkowe-2-mld-zl-na-rozwoj-e-administracji-i (term. wiz. 11. 06. 2025).