

# Katarzyna Ciach

---

## Zarządzanie mobilnością cyfrową

---

Ekonomiczne Problemy Usług nr 112, 259-267

---

2014

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej [bazhum.muzhp.pl](http://bazhum.muzhp.pl), gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

*KATARZYNA CIACH*  
Uniwersytet Łódzki

## ZARZĄDZANIE MOBILNOŚCIĄ CYFROWĄ

### Streszczenie

W artykule skoncentrowano się na przybliżeniu problematyki związanej z technologiami mobilnymi, a w szczególności problemami z zarządzaniem tymi technologiami w przedsiębiorstwach, w kontekście zmian, jakie niesie ze sobą stosowanie nowoczesnych technologii i trendów mobilnych, takich jak przetwarzanie w chmurze czy konsumeryzacja IT.

**Słowa kluczowe:** technologie mobilne, konsumeryzacja, BYOD.

### Wprowadzenie

Koniec XX w. i początek XXI w. to okres rewolucji technologicznej w życiu gospodarczym i społecznym. Zapoczątkowało ją pojawienie się na początku lat osiemdziesiątych ubiegłego wieku komputerów osobistych, które przyczyniły się do rozwoju społeczeństwa informacyjnego. Pierwsza połowa lat dziewięćdziesiątych to bardzo dynamiczny rozwój Internetu, który nieodwracalnie zmienił sposób komunikowania się, pozyskiwania informacji, prowadzenia działalności gospodarczej czy odpoczynku. Ostatnie lata zaś to era post PC, w której rozwój technologii informacyjnych doprowadził do masowego upowszechnienia się w społeczeństwie przenośnych urządzeń mobilnych, które znacząco wpłynęły również na sposoby funkcjonowania przedsiębiorstw, gwarantując nieprzerwany i niezależny od miejsca oraz czasu dostęp do korporacyjnych informacji.

Szczególne uwagę autorka zwróciła na przybliżenie problematyki związanej z technologiami mobilnymi, a w szczególności problemami z zarządzaniem tymi

technologiami w przedsiębiorstwach, w kontekście zmian, jakie niesie ze sobą stosowanie nowoczesnych technologii i trendów mobilnych, takich jak przetwarzanie w chmurze czy konsumeryzacja IT.

## 1. Technologie i urządzenia mobilne w biznesie

Technologie i urządzenia mobilne funkcjonują na rynku od wielu lat. Pierwsze smartfony pojawiły już w latach dziewięćdziesiątych. Jednak dopiero w ostatnich latach, i to głównie za sprawą producentów telefonów komórkowych, technologie mobilne weszły w fazę dynamicznego rozwoju, przez co radykalnie zmieniły sposób prowadzenia działalności gospodarczej i komunikowania się wszystkich przedsiębiorstw funkcjonujących na rynku.

Podstawowym zastosowaniem technologii mobilnych jest komunikacja. Korzystanie z firmowej poczty na smartfonie uważane jest za coś naturalnego, wygodnego i wręcz niezbędnego. Ale komunikacja w biznesie wykracza poza e-mail, kontakty i kalendarz. Komunikacja to również udostępnianie danych, np. inwestorom, klientom zarówno obecnym i potencjalnym (Synergizer, 2013).

Rosnące zapotrzebowanie na dostęp do danych w czasie rzeczywistym doprowadziło w firmach z różnych branż do szybkiego upowszechnienia się urządzeń i technologii mobilnych, które upraszczają prowadzenie firmy, maksymalizują dochody przez minimalizowanie wydatków i ulepszają jakość świadczonych usług.

Do mobilnych technologii w biznesie zaliczamy: bluetooth, mobilne aplikacje WWW, software as a service, mobilne widżety, platformy independent, GPS, komórkowy dostęp szerokopasmowy, ekrany dotykowe oraz uniwersalne systemy bezpieczeństwa (*Mobilne technologie*).

Rozwój techniczny tych technologii powoduje, że przestają istnieć bariery związane z miejscem i czasem, przez co znajdują zastosowanie w wielu branżach, m.in. w produkcji, handlu, usługach finansowych czy opiece zdrowotnej. W analizie przeprowadzonej przez firmę AT&T wskazano na podstawową korzyść z zastosowania urządzeń i aplikacji mobilnych (AT&T, 2006), jaką jest znaczące zwiększenie wydajności organizacji oraz indywidualnej efektywności poszczególnych pracowników. Dodatkowo do zalet rozwiązań mobilnych należy zaliczyć (Synergizer, 2013b):

- dostępność do danych i przepływ informacji wszędzie i o każdej porze,
- integrację z systemami informatycznymi firmy i automatyzację wymiany danych,
- ciągłą kontrolę wskaźników istotnych dla działalności firmy,
- stały kontakt z klientami oraz pracownikami,
- oszczędność czasu i pieniędzy – natychmiastowy przepływ informacji,

- natychmiastowy i łatwy dostęp do najaktualniejszych zasobów firmowych – większa efektywność pracy,
- większe zyski związane z usprawnieniem organizacji pracy, ograniczeniem procedur, dostępnością informacji.

## 2. Konsumeryzacja i BYOD

Szybkość działania oraz umiejętność reagowania w zmieniającym się otoczeniu firmy są obecnie jednymi z najważniejszych elementów w prowadzeniu biznesu. Konsekwencją tego jest przenikanie się życia osobistego z zawodowym. Pracownicy na co dzień korzystają z firmowych komputerów i aplikacji w pracy, ale coraz częściej wykorzystują prywatne notebooki, tablety, czytniki czy telefony do zadań związanych z pracą zawodową. Dlatego też obserwuje się, że prywatne doświadczenia zmieniają oczekiwania pracowników w stosunku do rozwiązań stosowanych w firmie.

Konsumeryzacja to zjawisko charakterystyczne dla współczesnych technologii informacyjnych i oznacza podporządkowanie tych technologii konsumentom (Niedbał 2013). Jest to zatem proces, w ramach którego pracownicy mają możliwość wyboru urządzeń i aplikacji (przeznaczonych dla konsumentów), za których pośrednictwem realizują zadania związane z pracą zawodową.

Podstawowym przejawem konsumeryzacji jest BYOD. Skrót ten pochodzi od angielskiej frazy *Bring Your Own Device* i odnosi się do coraz powszechniejszego wykorzystywania prywatnych urządzeń przez pracowników do celów służbowych. Mowa oczywiście o smartfonach, tabletach oraz przenośnych komputerach.

Zjawisko to związane jest z jednej strony z większą dostępnością tańszych i łatwiejszych w obsłudze urządzeń elektronicznych, z drugiej zaś – z podejmowaniem pracy przez tzw. pokolenie Y, czyli młodych ludzi w wieku 20–29 lat, dla których posiadanie urządzeń mobilnych jest „chlebem powszednim”, którzy aktywnie korzystają z nich w życiu codziennym i chcą mieć dostęp do informacji, również służbowych, o każdej porze i w każdym miejscu.

O popularności trendu BYOD świadczy badanie przeprowadzone na zlecenie firmy Fortinet<sup>1</sup>, według którego 74% respondentów na świecie i 69% w naszym kraju wykorzystuje prywatne urządzenia mobilne w celach służbowych, np. odbierając e-maile, korzystając z sieci korporacyjnej będąc domu czy w podróży służbowej.

---

<sup>1</sup> Badanie zostało przeprowadzone na zlecenie firmy Fortinet przez firmę Vision Critical w październiku 2013 r. u ponad 3200 aktywnych zawodowo mężczyzn i kobiet w wieku od 21 do 32 lat (tzw. „Generacja Y”), w tym 151 osób z Polski. Badania prowadzono równolegle w 20 krajach na całym świecie, m.in. w Polsce, USA, Japonii, Chinach, Chile, Kolumbii, Meksyku, Brazylii, Francji, Niemczech czy Rosji (Fortinet, 2013).

Prywatne urządzenia mają często lepsze parametry niż sprzęt służbowy, ponieważ zostały wybrane bezpośrednio przez samych użytkowników, są dobrze dopasowane do ich potrzeb, co bezpośrednio wpływa na jakość pracy i motywację osób zatrudnionych w firmie. Dzięki możliwości dostępu do danych firmowych, z każdego miejsca i o każdej porze, zwiększa się produktywność pracowników, co przekłada się na zadowolenie klientów przedsiębiorstwa. Jednocześnie minimalizuje się ryzyko odpływu specjalistów do konkurencji (Aiperos Technologies, 2013).

Na zjawisko BYOD należy jednak spojrzeć z dwóch perspektyw: firmy i pracownika, które często są ze sobą w sprzeczności (Niedbał 2013). Dla pracowników model BYOD to przede wszystkim komfort pracy na własnym, nierzadko lepszym sprzęcie i większe możliwości pracy mobilnej, co przekłada się na ich produktywność i zaangażowanie. Jednak model BYOD dla pracowników to nie tylko same korzyści, ale również pełna odpowiedzialność za sprzęt i dane firmowe zapisane w pamięci prywatnego urządzenia, ponieważ utrata takiego sprzętu będzie równoważna z utratą sprzętu służbowego, a więc możliwością nieuprawnionego dostępu do firmowych danych. Natomiast z punktu widzenia przedsiębiorstwa model BYOD to z jednej strony oszczędności związane z kosztami nabycia nowoczesnych urządzeń, z drugiej zaś problemy z zachowaniem bezpieczeństwa danych firmowych, zarządzaniem urządzeniami mobilnym i zachowaniem ich kompatybilności z infrastrukturą istniejącą w firmie.

Różnorodność urządzeń i aplikacji mobilnych istniejąca na rynku, w połączeniu z różnym zakresem obowiązków pracowników, wymusza na przedsiębiorstwach konieczność opracowania i ciągłej aktualizacji polityki BYOD, która powinna być dopasowywana do indywidualnych profili użytkowników. Powinien zostać przeprowadzony audyt ról pracownika w firmie i jego potrzeb w zakresie wykorzystania własnych urządzeń do celów zawodowych.

### **3. Zarządzanie mobilnością w firmie**

Do niedawna firmy miały pełną kontrolę nad tym, jakich urządzeń mobilnych używają ich pracownicy. To firma decydowała o systemie operacyjnym i modelu kupowanych urządzeń – zarówno laptopów czy notebooków, jak i smartfonów. Rozwiązanie takie było gwarancją kompatybilności zakupionych urządzeń z rozwiązaniami systemowymi funkcjonującymi w firmie i dawało możliwość efektywnego i scentralizowanego administrowania nimi. Jednak w ostatnich latach coraz popularniejszy trend BYOD zmienił ten obraz.

Praktycznie w każdym obszarze gospodarki firmy pozwalają swoim pracownikom na używanie prywatnych urządzeń, takich jak telefony komórkowe czy tablety, do celów służbowych. Z jednej strony jest to korzystne rozwiązanie dla firmy, ponieważ pozwala na redukcję wydatków związanych z zakupem urządzeń

przenośnych, ale z drugiej strony stanowi poważny problem związany z bezpieczeństwem danych firmowych.

W prywatnych urządzeniach mobilnych, których używają pracownicy do zadań służbowych, stosowane są systemy operacyjne, które nie zostały stworzone do profesjonalnych zastosowań, np. Apple iOS czy Android, dlatego też firmowe oprogramowanie do zarządzania infrastrukturą na ogół nie jest z nimi kompatybilne.

Powstaje zatem pytanie, jak administrować tymi urządzeniami, aby zapewnić bezpieczeństwo danych.

Rozwiązaniem tego problemu jest wdrożenie EMM (Enterprise Mobility Management), czyli modelu zarządzania mobilnością na poziomie firmy. Model ten powinien obejmować zarządzanie zarówno dostępem do danych za pomocą laptopów, tabletów, smartfonów, fabletów, jak i oprogramowaniem oraz dostępem do sieci internetowej i intranetowej.

Stworzenie i wdrożenie sprawnie działającego modelu zarządzania mobilnością przedsiębiorstwa nie jest rzeczą prostą. Należy zwrócić uwagę na następujące problemy (*Zarządzanie mobilnością...*, 2013):

#### ***Bezpieczeństwo danych firmowych.***

Urządzenia przenośne potencjalnie narażone są na utratę poufnych danych, m.in. wiadomości e-mail, danych klientów oraz danych niezbędnych do dostępu do wewnętrznych baz danych i firmowych aplikacji, w wyniku kradzieży lub zagubienia. Przedsiębiorstwa zezwalające na korzystanie z zasobów informacyjnych firmy za pomocą prywatnych urządzeń mobilnych tracą wtedy kontrolę nad tym, kto może uzyskać dostęp do tych danych. Wdrażany model zarządzania mobilnością powinien zatem obejmować systemy ochrony przed nieuprawnionym dostępem do aplikacji korporacyjnych i/lub danych firmowych na tychże urządzeniach. Mogą one obejmować ochronę hasłem, szyfrowanie oraz technologie zdalnego czyszczenia, które pozwalają administratorowi na usunięcie wszystkich danych z utraconego urządzenia.

#### ***Zarządzanie oprogramowaniem***

Ważnym zagadnieniem w kontekście EMM jest zarządzanie oprogramowaniem zainstalowanym na prywatnych urządzeniach przenośnych, posiadających różne systemy operacyjne. Każde takie urządzenie posiada unikalne wymagania w zakresie zarządzania, a administracja nimi wykonywana jest na ogół zdalnie. Dlatego też tradycyjne zadania administracyjne tracą na znaczeniu, gdyż wiele z nich zostało przerzuconych na użytkownika, np. takie jak aktualizacja oprogramowania czy personalizacja ustawień. Systemy zarządzania mobilnością powinny zatem udostępnić oprogramowanie pośredniczące (middleware), które umożliwi administratorom zdalne wykonywanie zadań związanych z zarządzaniem oprogramowaniem i obsługą urządzeń mobilnych.

***Kwestie prawne związane z modelem BYOD***

EMM powinien również uwzględniać kwestie prawne związane z modelem BYOD, tak aby pracodawca mógł legalnie monitorować prywatne urządzenia mobilne pracowników, choćby w ograniczonym zakresie.

***Koszty związane z wdrożeniem EMM***

Nie bez znaczenia są również koszty wdrożenia modelu EMM. W każdej firmie będą one różne w zależności od sektora gospodarki. W sektorach, gdzie mamy do czynienia z wrażliwymi danymi, np. finansowymi czy osobowymi, koszty wdrożenia zaawansowanych rozwiązań EMM będą duże, zaś w przedsiębiorstwach niekorzystających z danych wrażliwych aplikacje zapewniające bezpieczeństwo nie będą musiały spełniać wygórowanych wymogów restrykcyjnych, przez co wdrożenie tych rozwiązań będzie tańsze.

Na wysokość kosztów wdrożenia mają również wpływ takie czynniki, jak: koszty związane z pracą specjalistów, którzy będą zarządzać wdrożonym modelem EMM, niezależnie od tego czy firma będzie korzystała z własnych zasobów (zatrudni wykwalifikowany personel), czy też zdecyduje się na rozwiązanie outsourcingowe oraz koszty związane z usługami przesyłu danych, co jest konsekwencją zastosowania rozwiązań chmurowych.

Wdrożenie EMM powinno być zatem przeprowadzone w sposób świadomy i kontrolowany.

Według badań przeprowadzonych na zlecenie Samsunga<sup>2</sup> ponad połowa (57%) dużych polskich firm utraciła lub obawia się utraty danych klientów wskutek używania przez pracowników prywatnych urządzeń przenośnych. Pomimo tego tylko 37% przedsiębiorstw już wdrożyło bądź zamierza wdrożyć politykę BYOD pod kątem bezpieczeństwa.

Wdrożenie EMM wiąże się z zastosowaniem systemów oferujących funkcje do zarządzania urządzeniami (Mobile Device Management – MDM), aplikacjami (Mobile Application Management – MAM) oraz treściami Mobile Content Management – MCM) pozwalającymi na integrację z innymi systemami wykorzystywanymi w przedsiębiorstwie. Wśród korzyści ze stosowania ww. systemów należy wymienić przede wszystkim (Niedbał 2013):

- scentralizowaną kontrolę urządzeń mobilnych w czasie rzeczywistym, od chwili aktywacji usług mobilnych, poprzez cały cykl życia urządzenia;
- redukcję kosztów dzięki możliwości zarządzania różnymi urządzeniami (smartfony, tablety) niezależnie od systemu operacyjnego, jaki posiadają;
- bezpieczeństwo informacji i danych przechowywanych na urządzeniach mobilnych;

---

<sup>2</sup> Badanie przeprowadzono w maju i czerwcu wśród dyrektorów i osób podejmujących decyzje w sprawach informatyki w firmach zatrudniających ponad 1000 osób (Pasałowski 2013).

- usprawnienie procesów administracyjnych i serwisowych oraz wdrażania nowych rozwiązań mobilnych w firmie.

Na rynku obecnie dostępnych jest wiele systemów do zarządzania mobilnością w firmie oferujących (*Integrated Solutions*, 2013):

- zarządzanie zasobami mobilnymi – rozpoznawanie, przechowywanie i raportowanie danych o urządzeniach mobilnych;
- zarządzanie konfiguracjami – zdalną konfigurację połączeń sieciowych;
- zarządzanie aplikacjami – centralne repozytorium aplikacji, zdalną dystrybucję i instalację aplikacji;
- automatyczny backup danych – tworzenie kopii zapasowych najważniejszych danych dostępnych na urządzeniu mobilnym;
- zarządzanie bezpieczeństwem – definiowanie, aktualizowanie i zdalne przysyłanie polityk bezpieczeństwa na urządzenia mobilne;
- zarządzanie certyfikatami – centralny system dystrybucji certyfikatów;
- zdalne wsparcie – bezpieczne przejście kontroli nad urządzeniem mobilnym;
- system profili administracyjnych – elastyczne definiowanie ról, uprawnień i zakresu kompetencji dla pracowników mających dostęp do systemu;
- konsolę dla użytkowników końcowych – panel, dzięki któremu użytkownicy samodzielnie lokalizują swoje urządzenie, zgłaszają jego kradzież, zdalnie mogą wyczyścić dane, zainstalować aplikacje i zrobić backup danych.

Według Gartnera w magicznym kwadrancie liderów EMM znajdują się AirWatch, MobileIron, Citrix, SAP, Good Technology oraz Fiberlink. Mimo iż polska firma FancyFon nie znalazła się w analizie Gartnera, to także jej rozwiązanie z zakresu EMM cieszy się na rynku dużym uznaniem (Jakubowski 2013).

Oferta dostawców EMM jest szeroka i dopasowana do potrzeb firm różnej wielkości. Szczególnie przydatne w przypadku małych i średnich firm mogą być usługi EMM świadczone za pomocą rozwiązań chmurowych. Takie rozwiązania mogą być po prostu dla nich przystępniejsze cenowo.

## Podsumowanie

Ogromne znaczenie technologii mobilnych w dzisiejszych czasach jest nie do podważenia. Dzięki nim możemy szybciej kontaktować się z klientami, podnosić tempo cykli biznesowych, zwiększać produktywność, obniżać koszty operacyjne, a także rozszerzać zasięg oddziaływania organizacji.

W związku z tym, że w firmach coraz częściej urządzenia mobilne wykorzystywane są jako narzędzia pracy, potrzebna stała się kompleksowa ochrona gwarantująca bezpieczeństwo tych urządzeń. Zarządzanie i ochrona urządzeń mobilnych



musi zaczynać się od momentu aktywacji usługi, aż do końca cyklu życia urządzenia. Dlatego też zagadnienia związane z Enterprise Mobility Management (EMM) są coraz częściej przedmiotem rozważań nie tylko w największych korporacjach, ale także dużych i średnich firmach.

Rosnąca popularność BYOD oraz trendy związane z wykorzystaniem urządzeń i aplikacji mobilnych wymagają od organizacji wypracowania kompleksowych strategii w tym zakresie. Strategia ta, ze względu na szybko zachodzące zmiany w zakresie potrzeb biznesowych i wprowadzania na rynek nowych technologii, powinna mieć charakter procesu i być regularnie aktualizowana.

## Literatura

- Aiperos Technologies (2013), *Wyzwania konsumeryzacji*, <http://www.aiperos.pl/?p=18>.
- AT&T (2006), *The Wireless Advantage. Business Scenarios for Mobile Solutions*, <http://www.att.com/Common/merger/files/pdf/Wirelesscasestudies.pdf>.
- Fortinet (2013), Badanie Fortinet na temat BYOD i rozwoju nowoczesnych technologii mobilnych, <http://www.telix.pl/images/sprawozdania/FORTINET-BYOD-2013.pdf> [dostęp 28.01.2014].
- Integrated Solutions (2013), Oferta firmy w zakresie Mobile Device Management, <http://www.integratedsolutions.pl/oferta/it-infrastructure-application/mobile-device-management> [dostęp 3.02.2014].
- Iskierka S., Krzemiński J., Weźgowiec Z. (2012), *Przetwarzanie w chmurze obliczeniowej w warunkach polskiej edukacji*, w: N. Starik, A. Zduniak, *Podmiotowość w edukacji wobec odmienności kulturowych oraz społecznych zróżnicowań*, Zakopane, t. 1, [http://www.konferencja.21.edu.pl/uploads/6/3/9/9/6399009/1.2.1.\\_iskierka\\_krzemiski\\_wegowiec.pdf](http://www.konferencja.21.edu.pl/uploads/6/3/9/9/6399009/1.2.1._iskierka_krzemiski_wegowiec.pdf) [dostęp 6.01.2014].
- Jakubowski R. (2013), *Jak zapanować nad mobilnością?*, <http://it-manager.pl/jak-zapanowac-nad-mobilnoscia/> [dostęp 31.01.2014].
- Mell P., Grance T. (2009), *The NIST Definition of Cloud Computing*, <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf> [dostęp 6.01.2014].
- Mobilne technologie w biznesie*, <http://listaplac.net.pl/mobilne-technologie-w-biznesie> [dostęp 1.02.2014].
- Niedbał R. (2013), *Konsumeryzacja technologii IT w organizacjach gospodarczych*, E-wydawnictwo, [http://www.e-wydawnictwo.eu/Document/Document Preview/3757](http://www.e-wydawnictwo.eu/Document/Document%20Preview/3757) [dostęp 28.01.2014].
- Paslawski K. (2013), *Polskie firmy zagrożone z powodu BYOD*, <http://www.crn.pl/news/bezpieczenstwo/zagrozenia/2013/10/polskie-firmy-zagrozone-z-powodu-byod> [dostęp 3.02.2014].
- Porębska-Miąc T. (2009), *Wykorzystanie technologii mobilnych w zarządzaniu relacjami z klientem*, [http://www.swo.ae.katowice.pl/\\_pdf/412.pdf](http://www.swo.ae.katowice.pl/_pdf/412.pdf) [dostęp 5.01.2014].

- Synergizer (2013a), *Technologie mobilne w biznesie*, [http://www.synergizer.pl/technologie\\_mobilne/technologie-mobilne-w-biznesie/](http://www.synergizer.pl/technologie_mobilne/technologie-mobilne-w-biznesie/)
- Synergizer (2013b), *Technologie mobilne*, <http://www.synergizer.pl/produkty/technologie-mobilne/>
- Wyżnikiewicz B., Łapiński K. (2011), *Cloud computing: Elastyczność, Efektywność, Bezpieczeństwo*, Instytut Badań nad Gospodarką Rynkową, Warszawa, <http://www.ibngr.pl/Publikacje/Raporty-IBnGR/Cloud-Computing-elastycznosc-efektywnosc-bezpieczenstwo> [dostęp 4.01.2014]).

## ENTERPRISE MOBILITY MANAGEMENT

### Summary

The article focuses on issues related to the approximate mobile technologies, particularly on the problems of managing these technologies in enterprises, in the context of the changes that carries the use of new technology and mobile trends such as cloud computing and consumerization of IT.

**Keywords:** mobile technologies, consumerization, BYOD.

*Translated by Katarzyna Ciach*