

TOMASZ PROTASOWICKI¹, JERZY STANIK²

Zarządzanie technologiami ICT w Systemie Bezpieczeństwa Narodowego RP

1. Wstęp

Wykorzystanie technologii ICT stanowi jeden z kluczowych czynników umożliwiających współczesnym organizacjom m.in. sterowanie przepływem informacji i koordynowanie realizowanych procesów biznesowych. Działania te umożliwią efektywne wspomaganie ich misji z wykorzystaniem technologii i rozwiązań ICT. W praktyce polega to na inwestowaniu w te technologie i rozwiązania ICT, które wspierają realizację strategii organizacji i wynikające z niej procesy. Rodzi to potrzebę wybrania odpowiedniego podejścia do zarządzania technologiami ICT. Szczególnego znaczenia kwestie te nabierają w odniesieniu do organizacji sektora bezpieczeństwa. W artykule zaprezentowano kompleksowe spojrzenie na ten problem w kontekście specyficznej organizacji, jaką jest „System Bezpieczeństwa Narodowego RP (SBN RP), stanowiący całość sił, środków i zasobów przeznaczonych przez państwo na realizację zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowaną, utrzymaną i przygotowywaną”³. System ten intensywnie wykorzystuje technologie ICT. W trakcie przeprowadzonych w 2013 r. badań zidentyfikowano łącznie 125 systemów teleinformatycznych wspierających procesy biznesowe realizowane w ramach różnych podsystemów SBN RP⁴. Jednak w chwili obecnej nadal brakuje jednolitego komunikowania wizji, kierunku rozwoju oraz wymagań dotyczących systemów teleinformatycznych wspierających SBN RP. Do dziś nie zostały również wdrożone żadne mechanizmy, które umożliwiałyby zarządzanie w sposób

¹ Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.

² Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.

³ *Biała księga bezpieczeństwa narodowego RP*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013.

⁴ T. Protasowicki et al., *Organizacja wspomagania teleinformatycznego kierowania bezpieczeństwem narodowym RP*, AON, Warszawa 2013.

skoordynowany całym obszarem technologicznym tego systemu, w szczególności brakuje strategii informatyzacji.

Mając to na uwadze, należy stwierdzić, że istnieje potrzeba odpowiedniego podejścia do zarządzania technologiami ICT, które wymaga kompleksowego spojrzenia na ten problem w ramach całej organizacji SBN RP (rysunek 1).



Rysunek 1. Ilustracja mechanizmu zarządzania technologiami i rozwiązaniami ICT

Źródło: A. Sobczak, *Chmura w mieście, miasto w chmurze – czy samorzady potrzebują przetwarzania w chmurze i jak tam trafić?*, Ośrodek Studiów nad Cyfrowym Państwem, Warszawa 2012.

Celem niniejszej pracy było opracowanie propozycji zintegrowanego modelu (mechanizmu) umożliwiającego skoordynowane zarządzanie całym obszarem technologii ICT w ramach SBN RP. Mając na uwadze tak określony cel pracy, zaprezentowano w niej kwestie związane z opracowaniem strategii informatyzacji SBN RP, propozycje zintegrowanych mechanizmów zapewniania nadzoru (ang. *IT governance*) oraz zarządzania IT (ang. *IT management*). Szczególny nacisk położono na obszar dopasowania biznesowego i technologicznego organizacji na poziomie strategicznym oraz operacyjnym. Przedstawiono również propozycję wykorzystania modelu TIME, opracowanego przez firmę Gartner, w odniesieniu do zarządzania portfelem technologii wykorzystywanych w ramach SBN RP.

2. Integracja nadzoru i zarządzania IT

Analiza literatury dotyczącej obszaru IT dokonywana z perspektywy nauk o organizacji i zarządzaniu wskazuje, że często występującym problemem jest odróżnienie w organizacji nadzoru IT od zarządzania IT. R. Peterson podaje

różnice między tymi dwoma pojęciami. Domena zarządzania IT to skuteczne i efektywne świadczenie usług oraz dostarczanie produktów IT, a także zarządzanie operacyjne IT. Z kolei nadzór IT odpowiada za zapewnienie: (1) zgodności stosowanych technologii i rozwiązań ICT z bieżącymi wymaganiami pozwalającymi osiągnąć oczekiwaną efektywność aktualnie realizowanych w organizacji procesów oraz (2) wymaganych przekształceń w obszarze IT organizacji i jego dopasowania do przyszłych wyzwań biznesowych⁵. Wynika stąd wprost, że nadzór IT jest zorientowany na kontrolę zgodności bieżących działań w obszarze IT z uzgodnionymi celami oraz wspieranie podejmowania decyzji strategicznych dotyczących określenia przyszłych potrzeb i celów obszaru IT. Z kolei zarządzanie IT skupia się na: zarządzaniu obszarem IT na poziomie operacyjnym, dążeniu do uzyskania doskonałości operacyjnej obszaru IT, skutecznym i efektywnym świadczeniu usług oraz dostarczaniu produktów do ich odbiorców, a także zarządzaniu rozwojem i eksploatacją rozwiązań ICT. Relacje pomiędzy nadzorem i zarządzaniem IT w modelu zintegrowanym zilustrowano na poniższym diagramie (rysunek 2).



Rysunek 2. Ilustracja relacji pomiędzy nadzorem i zarządzaniem IT

Źródło: opracowanie własne.

⁵ R. Peterson, *Integration Strategies and Tactics for Information Technology Governance*, w: *Strategies for Information Technology Governance*, red. W. Van Grembergen, Idea Group Publishing, 2003.

3. Strategia informatyzacji SBN RP

Strategia informatyzacji SBN RP powinna stanowić długookresowy plan działań związanych z tworzeniem, nabywaniem, wdrażaniem, wycofywaniem całości rozwiązań ICT i zarządzaniem nią w ramach wszystkich podmiotów tworzących tę organizację. Pozwoli to zharmonizować jej działalność w obszarze technologii ICT z jej głównymi celami strategicznymi. Oczekuje się, że dzięki temu technologie ICT dadzą określoną wartość biznesową organizacji, m.in. poprzez skoncentrowanie uwagi na optymalizacji i racjonalizacji wydatków na technologie ICT. Głównym celem stworzenia strategii informatyzacji SBN RP musi być zatem skorelowanie warstwy technologicznej z postulowanym modelem operacyjnym oraz przyjętą strategią tej organizacji. Wymaga to udzielenia odpowiedzi na następujące pytania⁶:

- Czy stosowane technologie i rozwiązania ICT są dostosowane do potrzeb organizacji wynikających z realizowanych przez nią procesów biznesowych?
- Czy proces wdrażania nowych technologii i rozwiązań ICT przebiega właściwie i jaki jest jego charakter – stopniowy czy rewolucyjny?
- Jaki jest poziom środków finansowych, które organizacja może przeznaczyć na nowe technologie ICT?
- Czy skuteczne wsparcie procesów biznesowych wymaga tworzenia rozwiązań ICT od podstaw, czy możliwe jest dostosowanie rozwiązań dostępnych na rynku pod kątem specyficznych wymagań organizacji?
- Jakie korzyści mogą być uzyskane przez organizację wskutek wdrożenia określonych technologii i rozwiązań ICT?
- W jaki sposób należy zorganizować całokształt zadań z zakresu zarządzania technologiami ICT w organizacji, aby były one realizowane z najwyższą możliwą efektywnością?

Przyjęcie i wdrożenie określonej strategii informatyzacji rodzą daleko idące konsekwencje dla SBN RP. Relacje warstwy biznesowej i technologicznej są dwukierunkowe. Oznacza to, że zmiany w zakresie procesów biznesowych organizacji często wymuszają zmianę stosowanych rozwiązań lub technologii ICT, ale również że zmiany w obszarze technologicznym mogą spowodować wiele istotnych następstw dla warstwy biznesowej organizacji. W trakcie tworzenia

⁶ T. Reponen, *The role of learning in information systems planning and implementation*, w: *Information Technology and Organizational Transformation*, red. R. Galliers, W. Beats, Wiley & Sons, Chichester 1998, s. 134.

strategii informatyzacji SBN RP należy w szczególności mieć na względzie fakt, że wykorzystywana technologia i rozwiązania ICT muszą wspierać odtworzenie w domenie technicznej zaprojektowanego w warstwie biznesowej sposobu funkcjonowania tej organizacji. Dostosowanie struktur, funkcji i procesów organizacji powinno być zatem pochodną zmian w jej otoczeniu, a nie pochodną zmieniających się technologii ICT. Architektura środowiska ICT SBN RP musi być elastyczna i nastawiona na rozwój. Powinna zatem zapewniać łatwe dostosowanie technologii i rozwiązań ICT do wsparcia niezdefiniowanych jeszcze potrzeb biznesowych. Istotny wpływ na osiągnięcie tego typu zdolności ma przede wszystkim przyjęcie orientacji usługowej w warstwie technologicznej SBN RP, tj. stosowanych technologii, rozwiązań i infrastruktury ICT.

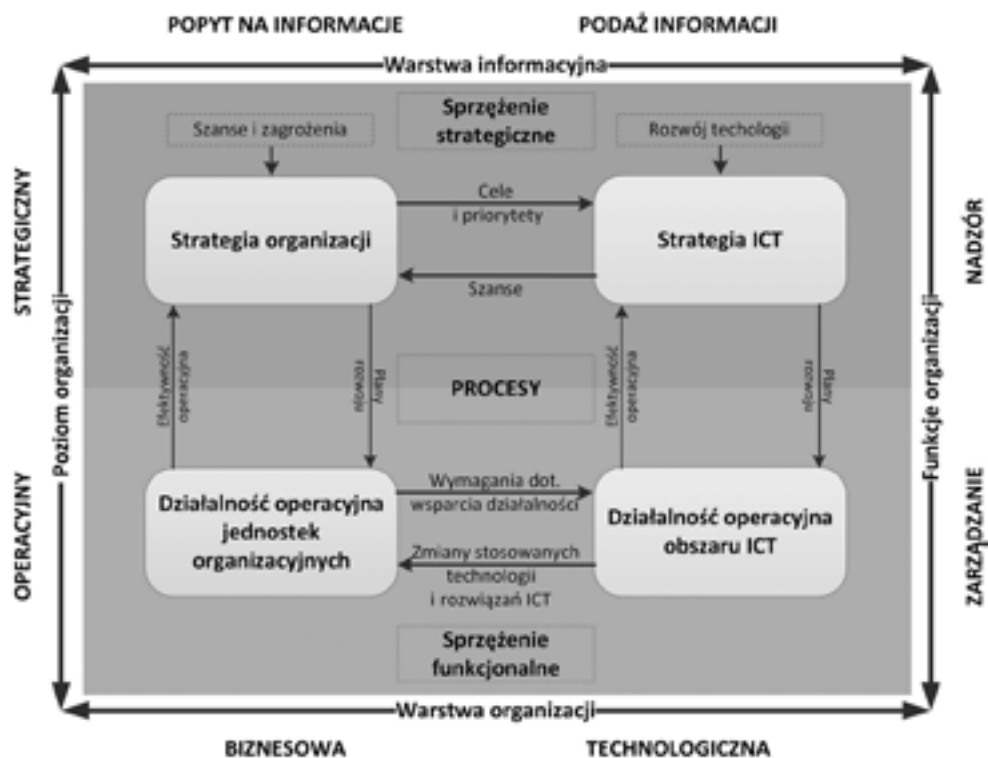
Oprócz opracowania i przyjęcia strategii informatyzacji SBN RP niezbędne jest również wdrożenie mechanizmów nadzoru i zarządzania operacyjnego wykorzystaniem technologii ICT. Wynika to z faktu, że inwestycje w technologie ICT są często obciążone tzw. paradoksem produktywności. Oznacza to, że zmiany warstwy technologicznej oparte na strategii tzw. pchania technologicznego (ang. *technology push*) nie przyczyniają się do uzyskania pozytywnych efektów z przekształcenia (zmiany) organizacji. Rzeczywiste korzyści z wdrażania nowych technologii ICT bez właściwego odniesienia ich zastosowania do przyjętej strategii organizacji i wynikających z niej wymagań biznesowych okazują się tym samym mniejsze od zakładanych.

4. Mechanizmy nadzoru nad obszarem IT w SBN RP

Nadzór IT obejmuje ustalanie zakresu odpowiedzialności i struktur podejmowania decyzji w celu zapewnienia odpowiedniego wykorzystywania technologii ICT w organizacji⁷. Wprowadza on zatem strukturę powiązań między procesami i zasobami z warstwy technologicznej a strategią i celami całej organizacji. Kluczową rolą nadzoru IT jest dostarczanie wartości z zastosowania technologii ICT do wsparcia realizacji potrzeb biznesowych poprzez ich należyte wykorzystanie oraz maksymalizowanie płynących stąd korzyści. W praktyce polega to na inwestowaniu w takie technologie i rozwiązania ICT, które wspierają realizację strategii organizacji i wynikające z niej procesy operacyjne. Celem

⁷ P. Weil, J. Ross, *IT Governance. How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston 2004.

takiego podejścia jest zwiększenie wpływu technologii ICT na wzrost efektywności organizacji. Osiąga się go poprzez dopasowanie (ang. *alignment*) obszarów biznesowego i technologicznego organizacji na poziomach strategicznym i operacyjnym (rysunek 3).



Rysunek 3. Ilustracja dopasowania obszarów biznesowego i technologicznego organizacji

Źródło: opracowanie własne.

Jak wskazuje R. Orzechowski, efektywny nadzór IT w organizacji wymaga odpowiedzi na trzy podstawowe pytania⁸:

- Jakie decyzje muszą zostać podjęte w celu zapewnienia efektywnego zarządzania i wykorzystania IT?
- Kto powinien podejmować te decyzje?
- W jaki sposób decyzje te zostaną podjęte i jak będą monitorowane ich efekty?

⁸ R. Orzechowski, *Pomiar dojrzałości nadzoru IT w polskich przedsiębiorstwach*, „Kwartalnik Nauk o Przedsiębiorstwie”, nr 2, Oficyna Wydawnicza SGH, Warszawa 2013, s. 6.

Wśród decyzji podejmowanych w ramach nadzoru IT można wskazać w szczególności ustalenia dotyczące⁹:

- głównych zasad IT określających sposób, w jaki technologie ICT powinny być stosowane w organizacji;
- architektury środowiska ICT reprezentowanej w formie zestawu polityk, zależności i wyborów technologicznych mających na celu wdrożenie pożądanego modelu operacyjnego organizacji;
- infrastruktury ICT, stanowiącej fundament zdolności organizacji, decydujący o realizacji działań operacyjnych w obszarze ICT;
- potrzeb w zakresie rozwiązań ICT, reprezentowanych w formie wymagań biznesowych dotyczących nabywanych lub rozwijanych wewnętrznie rozwiązań ICT;
- inwestycji w ICT, odnoszące się do odpowiedzi na pytania: ile środków finansowych przeznaczyć w ramach inwestycji w obszarze technologii ICT oraz na co i w jakiej kolejności je przeznaczyć?

Pozwala to wybrać właściwe technologie i rozwiązania spośród dostępnych alternatywnych inwestycji, ustalić ich wagę oraz zapewnić dopasowanie tych inwestycji do strategicznych priorytetów organizacji.

Wśród podmiotów odpowiedzialnych za podejmowanie decyzji w ramach nadzoru IT w organizacji można wskazać m.in.: organy kierownicze jednostek biznesowych (lub delegowanych przez nie przedstawicieli), organy kierownicze IT, właściciele głównych procesów biznesowych, połączone organy kolegialne organizacji.

Na nadzór IT składają się struktury organizacyjne oraz procesy, które razem tworzą spójny i skuteczny system kontroli. Wdrożenie nadzoru ICT w organizacji odbywa się w pięciu fazach, obejmujących: identyfikację potrzeb, opracowanie wizji, opracowanie planu wdrożenia, wdrożenie, wdrożenie i realizację procesów nadzoru IT. Każda z nich ma ściśle zdefiniowany cel oraz jest podzielona na etapy, w ramach których są realizowane szczegółowe zadania i osiągnięte oczekiwane rezultaty.

Główne procesy nadzoru IT, umożliwiające podejmowanie decyzji oraz monitorowanie ich efektów, to: określenie celów obszaru ICT, zapewnianie kierunku strategicznego, działania operacyjne ICT, pomiar rezultatów działania obszaru ICT, ocena rezultatów działania obszaru ICT. Ich realizację w SBN RP można opierać na adaptacji i zaimplementowaniu uznanych standardów, takich jak np. COBIT, ISO/IEC 38500 lub AS 8015–2005.

⁹ Ibidem.

5. Mechanizmy zarządzania obszarem IT w SBN RP¹⁰

Zarządzanie IT jest dziedziną dynamicznie rozwijającą się na styku nauk organizacji i zarządzania oraz nauk technicznych. Obejmuje swoim zakresem zagadnienia związane zarówno z organizacją oraz zarządzaniem, jak i z obszarem dotyczącym wytwarzania oraz eksploatacji rozwiązań ICT. W chwili obecnej w zakresie teorii i praktyki występującej w przedsiębiorstwach komercyjnych oraz administracji publicznej wyraźnie zaznacza się trend postrzegania zagadnień związanych z zarządzaniem IT przez pryzmat podejścia usługowego. Powoduje to, że jednostki organizacyjne korzystające z technologii i rozwiązań ICT w celu wspomagania realizacji swoich procesów biznesowych coraz częściej nie są zainteresowane technologiami ICT jako takimi, lecz zdolnościami, jakie mogą budować przy ich aktywnym wykorzystaniu. Dotyczy to również SBN RP, w ramach którego istnieje potencjał do centralizacji świadczenia wielu usług ICT wykorzystywanych przez różne podmioty tworzące ten system. Dzięki takiemu podejściu możliwe jest podejmowanie działań zmierzających do optymalizacji kosztów wdrażania oraz eksploatacji technologii i rozwiązań ICT np. poprzez budowę wspólnych centrów usług.

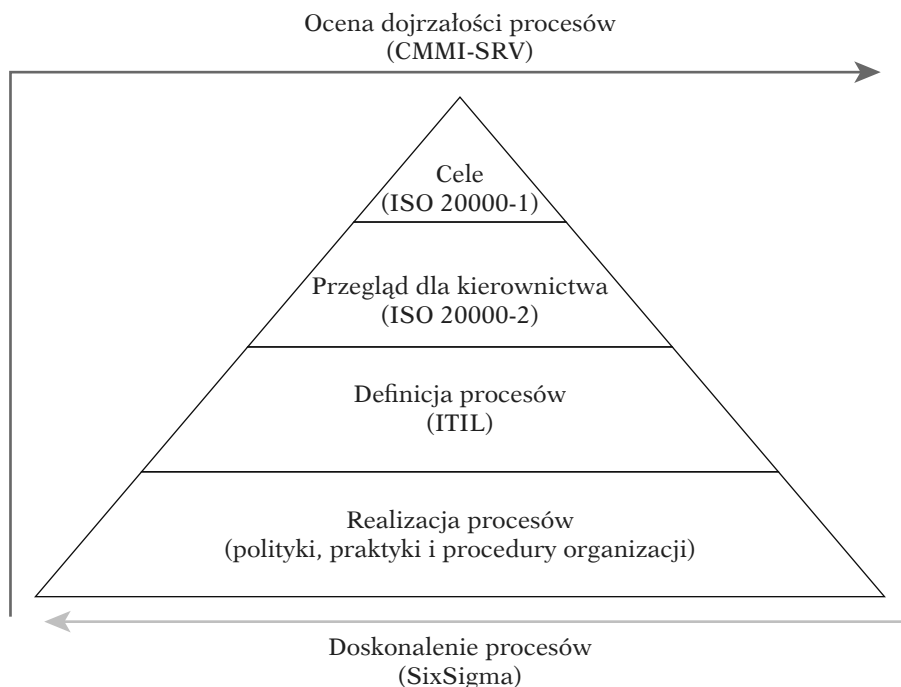
Sposób zarządzania IT w organizacji jest zależny m.in. od jej wielkości, oczekiwanych rezultatów, przyjętego modelu funkcjonowania obszaru IT (centralizacja/rozproszenie), skali jego działania, metod dostarczania wartości itp. Stosowane w praktyce podejścia do zarządzania IT bazują m.in. na:

- normie ISO/IEC 20000;
- bibliotece ITIL;
- modelu CMMI for Services;
- metodzie Six Sigma.

Wszystkie te podejścia bazowe podkreślają znaczenie nastawienia procesowego, jednak operują na różnych poziomach abstrakcji i udzielają odpowiedzi na różne pytania oraz dostarczają różnych elementów składowych niezbędnych do całościowego kierowania procesami zarządzania IT w modelu usługowym. Powstaje zatem problem stworzenia takiego systemu zarządzania IT na poziomie całego SBN RP oraz w ramach tworzących go organizacji, który pozwoli na wsparcie

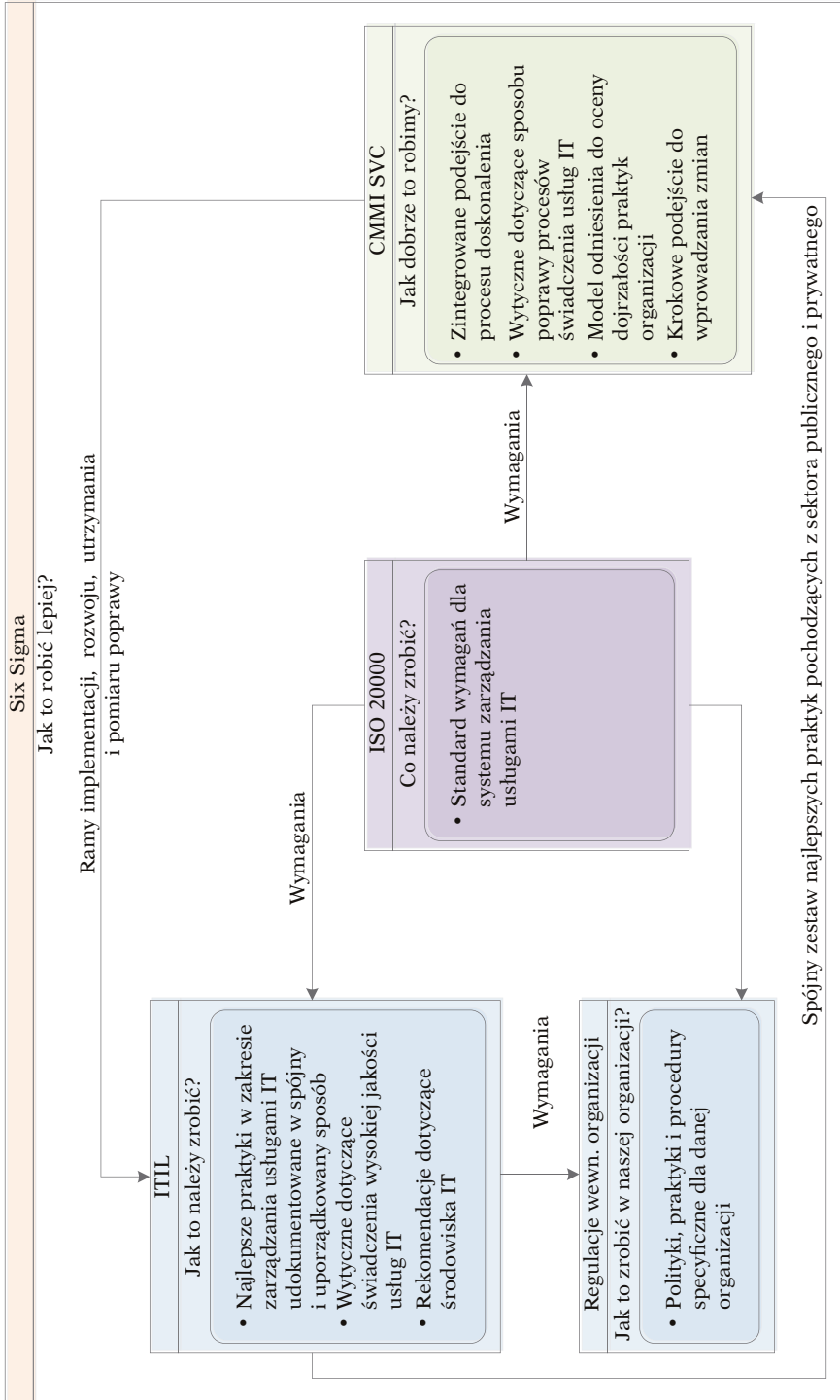
¹⁰ Niniejszy punkt opracowano na podstawie: T. Protasowicki, *Wybrane aspekty realizacji rozwiązań teleinformatycznych dla Systemu Bezpieczeństwa Narodowego RP*, w: *Inżynieria oprogramowania: badania i praktyka*, red. L. Madeyski, M. Ochodek, Nakom, Poznań-Warszawa 2014.

pełnego cyklu życia usług ICT oraz zapewni możliwość ciągłego doskonalenia procesów związanych z ich świadczeniem. Koncepcja takiego modelu zarządzania została zilustrowana na rysunkach 4 i 5. Zakłada ona takie wykorzystanie potencjału wymienionych wcześniej podejść bazowych, które pozwoli uzyskać efekt synergii i przełoży się na redukcję ryzyka, kosztów, błędów i usterek, podwyższenie efektywności i jakości oraz uzyskanie wspólnego rozumienia aspektów związanych z eksploatacją rozwiązań IT w organizacji.



Rysunek 4. Ilustracja koncepcji zarządzania operacyjnego obszarem IT

Źródło: T. Protasowicki, *Wybrane aspekty realizacji rozwiązań teleinformatycznych dla Systemu Bezpieczeństwa Narodowego RP*, w: *Inżynieria oprogramowania: badania i praktyka*, red. L. Madeyski, M. Ochodek, Nakom, Poznań–Warszawa 2014.



Rysunek 5. Ilustracja koncepcji zarządzania operacyjnego obszarem IT

Źródło: T. Protasowicki, *Wybrane aspekty realizacji rozwiązań teleinformatycznych dla Systemu Bezpieczeństwa Narodowego RP*, w: *Inżynieria oprogramowania: badania i praktyka*, red. L. Madeyski, M. Ochodek, Nakom, Poznań–Warszawa 2014.

6. Zarządzanie portfelem technologii ICT w SBN RP

Technologie ICT w wąskim rozumieniu obejmują całość środków technicznych (sprzęt, oprogramowanie, narzędzia itp.), które są stosowane w procesie gromadzenia, przechowywania, przetwarzania, przesyłania, zabezpieczania i udostępniania informacji realizowanym przez SBN RP. Systemy wsparcia teleinformatycznego SBN RP wykorzystują obecnie wiele technologii ICT. Można scharakteryzować je w uproszczeniu jako: przestarzałe, nowoczesne lub niszowe. Obecny poziom standaryzacji technologii ICT wykorzystywanych w SBN RP trzeba określić jako niski. Przede wszystkim brakuje procesu formalnego zarządzania standardami technologicznymi w SBN RP. Szczególny nacisk należy zatem położyć na wprowadzenie odpowiednich mechanizmów zarządczych, zapewniających uporządkowanie i stabilność środowiska ICT SBN RP. Z jednej strony pozwoli to uporządkować portfel technologii, z drugiej strony – umożliwi elastyczne zmiany i rozwój w obszarze systemów ICT SBN RP w odpowiedzi na dynamicznie zmieniające się potrzeby biznesowe.

Podstawowe narzędzie do budowy i oceny portfela technologicznego oraz określenia standardów technologicznych ICT SBN RP stanowi katalog komponentów technologicznych (KKT). Jego zasadniczą rolą jest utrzymywanie kompletnej listy wszystkich technologii IT używanych w podmiotach tworzących SBN RP oraz wsparcie procesu:

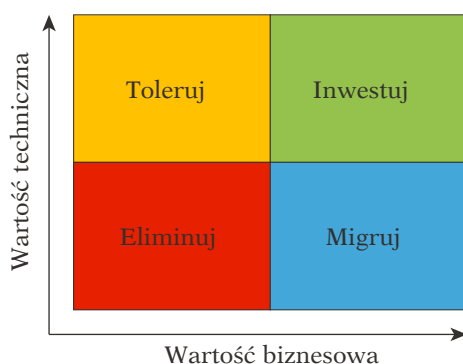
- identyfikacji wykorzystywanego sprzętu, oprogramowania i innych narzędzi ICT;
- zarządzania cyklem życia składników technologicznych;
- definiowania standardów technicznych.

Zakres informacyjny KKT musi obejmować co najmniej następujące atrybuty:

- kategorię;
- producenta;
- nazwę;
- wersję;
- strategię zarządzania technologią według modelu TIME;
- datę wycofania wsparcia producenta;
- datę wycofania rozszerzonego wsparcia producenta;
- datę wycofania z eksploatacji w SBN RP.

Ponadto KKT zawiera przypisanie technologii do wykorzystujących je systemów wsparcia teleinformatycznego SBN RP i udostępnia również słowniki wartości standardowych dla określonych atrybutów (kategoria, producent, strategia,

system wsparcia teleinformatycznego). W ramach proponowanego podejścia każdy komponent technologiczny wykorzystywany przez systemy wsparcia teleinformatycznego SBN RP i zaewidencjonowany w KKT musi mieć przypisaną jedną ze strategii postępowania opartych na modelu TIME, opracowanym przez firmę Gartner Research (rysunek 6).



Rysunek 6. Ilustracja modelu TIME Gartnera

Źródło: opracowanie własne.

Wyróżnione w ramach modelu TIME strategie to:

- **toleruj** (ang. *tolerate*) – strategia postępowania względem technologii ICT, które dostarczają pewnej wartości biznesowej o niekluczowym charakterze z perspektywy stabilności procesów realizowanych w SBN RP;
- **inwestuj** (ang. *invest*) – strategia postępowania względem technologii ICT, które mają wysoką wartość biznesową i techniczną w kontekście SBN RP;
- **migruj** (ang. *migrate*) – strategia postępowania względem technologii ICT, które mają wysoką wartość biznesową, ale są niezgodne z planowaną architekturą docelową SBN RP na poziomie technicznym lub wygasa wsparcie świadczone przez ich producentów;
- **eliminuj** (ang. *eliminate*) – strategia postępowania względem technologii ICT, które mają niską wartość biznesową oraz techniczną w kontekście SBN RP.

Wartość biznesowa (ang. *business value*) stanowi kluczowy atrybut każdej technologii, pozwalający na określenie sensu i potencjału jej wykorzystania w kontekście SBN RP. Definiuje ona znaczenie technologii ICT dla spełnienia celów biznesowych oraz realizacji procesów związanych z zaspokajaniem potrzeb społecznych w ramach SBN RP. Z kolei wartość techniczna (ang. *technical value*) stanowi istotny czynnik umożliwiający dokonanie oceny wpływu

technologii na obciążenia organizacji związane z jej utrzymaniem oraz analizy poziomu występującego w niej długu technicznego.

W efekcie zastosowania modelu TIME jest budowana macierz, która daje zintegrowany widok rozkładu poszczególnych technologii ICT w ramach portfela technologicznego SBN RP. Pozwala to na dokonanie oceny jego jakości oraz zaplanowanie i podjęcie odpowiednich działań zmierzających do wyeliminowania technologii niepożądanych, niosących istotne ryzyko dla funkcjonowania systemów wsparcia teleinformatycznego SBN RP.

7. Podsumowanie

Wykorzystanie technologii ICT stanowi jeden z kluczowych czynników umożliwiających współczesnym organizacjom m.in. sterowanie przepływem informacji i koordynowanie realizowanych przez nie procesów biznesowych. Rodzi to potrzebę zastosowania odpowiedniego podejścia do zarządzania technologiami ICT, wymagającego kompleksowego spojrzenia na ten problem w ramach całej organizacji, jaką jest SBN RP. Wymusza to w szczególności opracowanie strategii informatyzacji SBN RP oraz wdrożenie zintegrowanych mechanizmów zapewniania nadzoru IT (ang. *IT governance*) i zarządzania IT (ang. *IT management*). Działania te umożliwią efektywne wspomaganie realizacji misji tego systemu z wykorzystaniem technologii i rozwiązań ICT. W praktyce polega to na inwestowaniu w takie technologie ICT, które wspierają realizację strategii organizacji i wynikające z niej procesy operacyjne.

Dążąc do redukcji mającego swoje źródło w stosowanych technologiach ICT ryzyka dotyczącego zaburzenia realizacji procesów biznesowych, należy ustalić i wdrożyć proces zarządzania wykorzystaniem portfela technologii ICT w SBN RP. Proces ten powinien obejmować docelowo zarządzanie stosowanym oprogramowaniem i sprzętem niezbędnym do prawidłowego funkcjonowania eksploatowanych systemów wsparcia teleinformatycznego SBN RP. Wymaga to zidentyfikowania wszystkich komponentów technologicznych oraz przypisania im odpowiednich strategii postępowania opartych na modelu TIME, opracowanym przez firmę Gartner Research. Wyniki zaprezentowane w niniejszej pracy tworzą podwaliny dalszych badań, które mogą dotyczyć optymalizacji portfela technologii ICT SBN RP na podstawie kryterium ryzyka dla ciągłości działania i innych aspektów praktycznych.

Bibliografia

- Biała księga bezpieczeństwa narodowego RP*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013.
- Orzechowski R., *Pomiar dojrzałości nadzoru IT w polskich przedsiębiorstwach*, „Kwartalnik Nauk o Przedsiębiorstwie”, nr 2, Oficyna Wydawnicza SGH, Warszawa 2013.
- Protasowicki T., *Wybrane aspekty realizacji rozwiązań teleinformatycznych dla Systemu Bezpieczeństwa Narodowego RP*, w: *Inżynieria oprogramowania: badania i praktyka*, red. L. Madeyski, M. Ochodek, Nakom, Poznań–Warszawa 2014.
- Protasowicki T., *Wybrane aspekty zastosowania koncepcji architektury korporacyjnej w transformacji Systemu Bezpieczeństwa Narodowego RP*, „Zeszyty Naukowe” Uniwersytetu Szczecińskiego, „Ekonomiczne Problemy Usług”, z. 112, Szczecin 2014, s. 151–163.
- Protasowicki T., *Zintegrowana transformacja Systemu Bezpieczeństwa Narodowego RP*, „Zeszyty Naukowe” Uniwersytetu Szczecińskiego, „Ekonomiczne Problemy Usług”, z. 123, Szczecin 2016, s. 287–299.

* * *

Management of ICT in the National Security System of the Republic of Poland

Abstract

ICT is one of the key factors in enabling organizations to control the flow of information and coordinate the execution of business processes. The paper presents the problem of management of ICT in the National Security System of the Republic of Poland (SBN RP). The presented issues cover the following areas: the development of IT strategy, integrated IT governance and management of the SBN RP, and a proposal to use the TIME model for managing a portfolio of technologies used within the SBN RP.

Keywords: national security system, strategic and operational management of ICT, evaluation of ICT