

Małgorzata Pawłowicz

**Nowa jakość
projektów
teleinformatycznych
a bezpieczeństwo
organizacji Policji**

Szczytno 2016

Recenzja

dr hab. Jacek Dworzecki, prof. WSPol

Redakcja wydawcy

Agnieszka Kamińska

Justyna Zaryczna

Projekt okładki

Jan Napiórkowski



© Wszelkie prawa zastrzeżone — Wyższa Szkoła Policji w Szczytnie 2016

ISBN 978-83-7462-510-4

e-ISBN 978-83-7462-511-1

Skład, druk i oprawa:

Dział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie

12-100 Szczytno, ul. Marszałka Józefa Piłsudskiego 111

tel. 89 621 51 02, fax 89 621 54 48

e-mail: wwip@wspol.edu.pl

Objętość: 12,03 ark. wyd. (1 ark. wyd. = 40 tys. znaków typograficznych)

Spis treści

Wykaz skrótów i podstawowe wyjaśnienia terminologiczne	5
Wstęp	9
ROZDZIAŁ I	
Teleinformatyka policyjna w obliczu globalnej informatyzacji	15
ROZDZIAŁ II	
Jakość projektów teleinformatycznych w Policji	21
1. Pojęcie jakości projektów teleinformatycznych	21
2. Obowiązujące uwarunkowania w obszarze zarządzania projektami teleinformatycznymi w Policji	53
3. Zdolność pionu teleinformatyki policyjnej do zapewnienia wysokiej jakości projektów teleinformatycznych	73
4. Wnioski	75
ROZDZIAŁ III	
Organizacyjno-prawne kierunki zmian w obszarze zarządzania projektami teleinformatycznymi w Policji	77
1. Uzasadnienie potrzeby zmian w zarządzaniu projektami teleinformatycznymi w Policji	77
2. Kierunki zmian w zarządzaniu projektami teleinformatycznymi w Policji	89
3. Wnioski	111
ROZDZIAŁ IV	
Metodyka zarządzania projektami teleinformatycznymi w Policji	113
1. Zarządzanie projektami teleinformatycznymi w Policji jako organizacji sektora publicznego	114
2. Elementy ogólnodostępnych metod zarządzania projektami teleinformatycznymi właściwe do zastosowania w Policji	117
3. Koncepcja metodyki zarządzania projektami teleinformatycznymi w Policji	138
4. Wnioski	158
ROZDZIAŁ V	
Wpływ rezultatów projektów teleinformatycznych w Policji na bezpieczeństwo organizacji	161
1. Bezpieczeństwo Policji jako organizacji	161
2. Rola teleinformatyki w kształtowaniu bezpieczeństwa Policji	169
3. Efekty podejścia projektowego stosowanego w teleinformatyce policyjnej	174

4. Prognoza skutków zmian proponowanych w obszarze zarządzania projektami teleinformatycznymi w Policji	178
5. Wnioski	183
Zakończenie	185
Bibliografia	189
Literatura	189
Akty prawne	196
Źródła internetowe.....	198
Wykaz tabel	201
Wykaz wykresów	202
Wykaz rysunków	203
Wykaz szablonów dokumentów	204

Wykaz skrótów i podstawowe wyjaśnienia terminologiczne

BŁiI KGP — Biuro Łączności i Informatyki Komendy Głównej Policji.

IT — information technology (tłum. technologia informacyjna) — całokształt zagadnień, metod i środków oraz działań służących wszechstronnemu posługiwaniu się informacją¹.

jednostka organizacyjna Policji — Komenda Główna Policji, komenda wojewódzka (stołeczna) Policji, Wyższa Szkoła Policji w Szczytnie, szkoła policyjna, Centralne Laboratorium Kryminalistyczne Policji.

KGP — Komenda Główna Policji.

komórka merytoryczna — wyodrębniona część struktury organizacyjnej, właściwa w zakresie produktu: wydziały BŁiI KGP, komórki organizacyjne KGP, komend wojewódzkich (stołecznej) Policji, Wyższej Szkoły Policji w Szczytnie, szkół policyjnych oraz Centralnego Laboratorium Kryminalistycznego Policji.

KSP — Komenda Stołeczna Policji.

KWP — komenda wojewódzka Policji.

PMBok® — Project Management Body of Knowledge — zbiór standardów i rozwiązań w dziedzinie zarządzania projektami, zebranych i opublikowanych przez członków Project Management Institute². W 1998 r. American National Standards Institute zaakceptował to rozwiązanie jako narodowy standard zarządzania projektami³.

PMI — Project Management Institute — międzynarodowy instytut zrzeszający kierowników projektów, który powstał w 1969 r. w Pensylwanii, w USA, jako stowarzyszenie *non profit* profesjonalistów w dziedzinie zarządzania projektami⁴.

proces — ustrukturyzowany zbiór działań zaprojektowany w celu osiągnięcia konkretnego celu. Proces pobiera jeden lub większą liczbę określonych elementów wejściowych i przekształca je w określone elementy wyjściowe⁵.

produkt — element wejściowy lub wyjściowy, w formie materialnej lub niematerialnej, który można wcześniej opisać, wytworzyć i sprawdzić⁶. W Policji:

¹ M. Kręglewski, *Technologia Informacyjna TI*, <<http://www.staff.amu.edu.pl/~zcht/pliki/Technologia%20Informacyjna.pdf>>, 5 sierpnia 2014 r.

² PMBOK Guide and Standards, informacja umieszczona na stronie internetowej organizacji Project Management Institute, <<http://www.pmi.org/PMBOK-Guide-and-Standards.aspx>>, 5 sierpnia 2014 r.

³ A. Koszłajda, *Zarządzanie projektami IT. Przewodnik po metodykach*, Gliwice 2010, s. 31–32.

⁴ Informacje dotyczące organizacji Project Management Institute, umieszczone na stronie internetowej <<http://www.pmi.org/>>, 5 sierpnia 2014 r.

⁵ W. Kosieradzki, *PRINCE2: 2009 Glossary of Terms — Polish*, wersja 1.2, AXELOS Limited 2012, s. 25, <https://www.axelos.com/Corporate/media/Files/Glossaries/PRINCE2-2009-Glossary-of-terms_PL-v1-2.pdf>, 16 października 2015 r.

⁶ Tamże.

system teleinformatyczny zakupiony, wybudowany lub zmodernizowany w ramach przedsięwzięcia teleinformatycznego.

Prince2® — PProjects IN a Controlled Environment (tłum. projekty w sterowanym środowisku) — metodyka zarządzania ustanowiona w 1989 r. przez brytyjską agencję rządową Central Computer and Telecommunications Agency (CCTA). Stanowi rozwinięcie metodyki PROMPT (ang. Project Resource Organisation Management Planning Technique) opracowanej przez firmę Simpect Systems Ltd. w 1975 r., stosowanej do prowadzenia projektów informatycznych sponzorowanych przez rząd brytyjski. Zuniwersalizowana wersja Prince2 pozostaje zarejestrowanym znakiem organizacji Office of Government Commerce (OGC), której częścią jest CCTA⁷.

projekt teleinformatyczny — tymczasowa organizacja powołana w celu zrealizowania jednorazowej sekwencji powiązanych działań, dla której zdefiniowano zakres, koszt i termin wykonania, z zamiarem osiągnięcia ustalonego celu.

przedsięwzięcie teleinformatyczne — całokształt działań prowadzonych w jednostkach organizacyjnych Policji obejmujących inicjowanie, przygotowanie, realizację i zamknięcie jednego lub wielu powiązanych projektów teleinformatycznych oraz przekazanie uzyskanych w wyniku tych działań produktów do eksploatacji.

SIS — System Informacyjny Schengen — baza danych, w której generowane są określone przepisami kategorie danych osób i przedmiotów, poszukiwanych i wprowadzanych do systemu przez państwa strefy Schengen na podstawie rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz decyzji Rady 2007/533/WSiSW z 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II).

SIWZ — specyfikacja istotnych warunków zamówienia — podstawowy dokument podczas postępowania o udzielenie zamówienia publicznego. Uregulowany co do zakresu w art. 36 ustawy z 29 stycznia 2004 r. — Prawo zamówień publicznych⁸.

system teleinformatyczny — zespół współpracujących urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego⁹.

urządzenie końcowe — urządzenie elektryczne lub elektroniczne (lub jego podzespół), dołączane bezpośrednio lub pośrednio, przeznaczone do zapewniania telekomunikacji z policyjnym systemem teleinformatycznym.

⁷ A. Korczowski, G. Lasek, *Zarządzanie projektami — Metodyka PRINCE2*, materiały szkoleniowe, v. 2.21, Warszawa 2008, s. 8.

⁸ J. Szatan, *Specyfikacja istotnych warunków zamówienia* [w:] *Encyklopedia zarządzania „M-files”* [online], <http://mfiles.pl/pl/index.php/Specyfikacja_Istotnych_Warunk%C3%B3w_Zam%C3%B3wienia>, 6 września 2013 r.

⁹ Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn. DzU z 2013 r., poz. 1422).

Żeby istnieć, trzeba uczestniczyć
Antoine de Saint-Exupéry

Wstęp

Rozwój technologii informacyjno-komunikacyjnych staje się coraz istotniejszym czynnikiem zmian społeczno-gospodarczych w otaczającym świecie. „Nowoczesne rozwiązania, które zdominowały trendy współczesnej globalizacji, stanowią czynnik, który wywiera trudny do przecenienia wpływ na prawie wszystkie sfery życia i działalności człowieka”¹⁰. W coraz większym stopniu zaczynamy rozumieć, że jakość naszego życia zależy od udanych zastosowań informatyki oraz związanych z tym kosztów. Ta tendencja będzie się z pewnością nasilać¹¹. Globalna cyfryzacja wywiera ogromne piętno na sposobie myślenia, działania i pojmowania współczesnej rzeczywistości. Generuje w ten sposób zmiany, których istotą jest potrzeba dostosowania się do otoczenia. „Co więcej, nie są to wyłącznie drobne zmiany, modyfikacji bowiem podlegają też sposoby funkcjonowania, organizacji i prowadzenia działalności przez firmy i inne instytucje. Technologie towarzyszą nam niemal na każdym kroku, przyczyniając się jednocześnie do transformacji procesów biznesowych. Nie ulega wątpliwości, że ich wykorzystanie może wymagać zmian nie tylko w sferze technicznej, ale też zmian o charakterze organizacyjnym, w komunikacji z pracownikami i klientami, w procesie kształcenia i nabywania kompetencji, a także w innych obszarach funkcjonowania. Ma więc konsekwencje zarówno dla indywidualnych użytkowników, jak i całych instytucji”¹².

Prowadzone tu rozważania dotyczą obszaru, który staje się bezsprzecznym liderem przemian zachodzących w otaczającym nas świecie i odzwierciedla skutki powszechnej transformacji systemowej, która kreuje zjawisko gospodarki opartej na wiedzy jako podstawowym czynnikiem rozwoju społeczeństw¹³. Na przykładzie Policji jako potężnej, zhierarchizowanej formacji, funkcjonującej w dynamicznie zmieniającym się otoczeniu, dysponującej środkami pochodzącymi w przeważającej części z budżetu państwa, przeprowadzona została analiza i ocena stanu przygotowania do podejmowania złożonych, trudnych wyzwań w obszarze przedsięwzięć teleinformatycznych, których rezultaty przekładają się w istotny sposób na bezpieczeństwo całej organizacji.

Policja jako organizacja musi uczestniczyć w procesie globalnej informatyzacji. W trosce o swoje bezpieczeństwo, działając w określonej rzeczywistości, powinna nadszperkować za najsilniejszymi trendami rozwojowymi. Wobec gwałtownie postępującego

¹⁰ M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Siedlce 2009, s. 158.

¹¹ J. Górski (red.), *Inżynieria oprogramowania w projekcie informatycznym*, Warszawa 1999, s. 11.

¹² D. Batorski (red.), *Cyfrowa gospodarka. Kluczowe trendy rewolucji cyfrowej. Diagnoza, prognozy, strategie reakcji*, Warszawa 2012, s. 7.

¹³ K. Piech, *Gospodarka oparta na wiedzy i jej rozwój w Polsce*, „E-Mentor” 2004, nr 4 (6), s. 37.

rozwoju technologicznego ten udział powinien być świadomy, uporządkowany i dojrzały. Intensywność zmian obserwowanych w otoczeniu sprawia, że kluczowym dla organizacji pojęciem staje się wpływ jakości prowadzonych projektów teleinformatycznych na jej bezpieczeństwo. Zachwyty informatyzacją może nie tylko wesprzeć proces wzrostu wydajności organizacji, lecz także stać się zagrożeniem dla tych organizacji, które nie dostrzegły światowego trendu innowacyjności i nie potrafią poradzić sobie z jego postępującym charakterem. Warto jest pochylić się nad uwarunkowaniami jakości przedsięwzięć, prowadzonych w pionie teleinformatyki policyjnej, które służyć mają skutecznej i efektywnej realizacji celów całej organizacji. „W myśleniu o bezpieczeństwie — jednym z najbardziej pożądanym i cenionym przez ludzkość dóbr wyróżnić można dwie zasadnicze strategie. Pierwsza koncentruje się na działaniach przygotowujących do ochrony przed zagrożeniami, druga zaś skupia się na takim kształtowaniu otoczenia, aby oddalać i minimalizować możliwości pojawiania się tychże”¹⁴. Określenie bezpieczeństwa potrzebą podmiotową o charakterze egzystencjalnym powoduje, że podmioty, dążąc do jego zapewnienia, nie mogą podejmować tylko działań negatywnych, nakierowanych na eliminowanie zagrożeń. Organizacje podejmują także stawiane przed nimi wyzwania i starają się kształtować swoje bezpieczeństwo metodami pozytywnymi również wtedy, gdy nie doświadczają zagrożeń¹⁵. Zważywszy na dwójakość w postrzeganiu zagrożenia, które z jednej strony jest odczuciem czysto subiektywnym, wynikającym z oceny występujących zjawisk, z drugiej zaś — obiektywnym czynnikiem, powodującym stan niepewności i obaw¹⁶, najczęściej uznawane jest ono za istniejące, gdy „w człowieku rodzi się obawa o utratę wysoko cenionych wartości”¹⁷. Zmieniającej się rzeczywistości i postępującej informatyzacji nie można nie zauważyć i nie da się powstrzymać. „Z procesami adaptacyjnymi organizacji do otoczenia wiąże się niepewność, wynikająca z trudności rejestrowania oraz przewidywalności zmian, dokonujących się w otoczeniu zewnętrznym, jak również w samej organizacji. Od szybkości i sposobu reagowania organizacji na zmienne warunki otoczenia zależy jej skuteczność i sprawność, dlatego zrozumienie otoczenia jest sprawą niezwykle ważną”¹⁸. Policja musi więc podjąć skuteczne działania w krytycznych aktualnie obszarach, które pomogą jej sprostać nowym sytuacjom i przeciwdziałać potencjalnym negatywnym ich skutkom, aby mogła poprawnie realizować swoją misję. Wymaga to również określonych przedsięwzięć technicznych i ich utrzymywania, niezależnie od istnienia

¹⁴ W. Fehler, *Zagrożenie — kluczowa kategoria bezpieczeństwa* [w:] K. Jałoszyński, B. Wiśniewski, T. Wojtuszek (red. nauk.), *Współczesne postrzeganie bezpieczeństwa. Materiały z konferencji zorganizowanej przez Wyższą Szkołę Administracji w Bielsku-Białej 23 listopada 2006 r.*, Bielsko-Biała 2007, s. 41.

¹⁵ R. Zięba, *O tożsamości nauk o bezpieczeństwie*, „Zeszyty Naukowe Akademii Obrony Narodowej” 2012, nr 1 (86), s. 11.

¹⁶ S. Korycki, *System bezpieczeństwa Polski*, Warszawa 1994, s. 54.

¹⁷ T. Tomaszewski, *Wstęp do psychologii*, Warszawa 1971, s. 124.

¹⁸ K. Krzakiewicz (red. nauk.), *Podstawy organizacji i zarządzania*, Poznań 1994, s. 40.

jakiegokolwiek zagrożenia¹⁹. Żeby efektywnie wykorzystywać szanse, jakie przynosi postępująca informatyzacja, i jednocześnie minimalizować niepożądane rezultaty tego zjawiska, należy znaleźć właściwe podejście i mechanizmy, które zapewnią organizacji zdolność do trwania, przetrwania i rozwoju.

W rozdziale pierwszym niniejszej pracy zobrazowano problem, w obliczu którego stanęła dzisiaj teleinformatyka policyjna. W dobie wszechobecnej informatyzacji wskazana została potrzeba budowy bezpieczeństwa Policji na podstawie jakości rozwiązań IT.

Rozdział drugi poświęcony został zagadnieniu jakości projektów teleinformatycznych realizowanych w Policji. Wychodząc od powszechnie przyjętych definicji projektów, określono kryteria oceny ich rezultatów. Korzystając z wiedzy teoretycznej oraz badań przeprowadzonych w dziedzinie zarządzania projektami, wskazane zostały kluczowe aspekty, istotne dla zapewnienia efektywnego prowadzenia przedsięwzięć teleinformatycznych. Wysoka jakość rezultatów projektów teleinformatycznych winna być troską i celem organizacji, która chce zapewnić sobie bezpieczeństwo w postaci dogodnych warunków do doskonalenia i rozwoju. Na podstawie analizy piśmiennictwa podkreślono istotę oceny wartości użytkowej rezultatów projektów teleinformatycznych. Satysfakcja użytkownika, jakkolwiek krytyczna dla sukcesu projektu, nie jest bowiem powszechnie stosowanym wymogiem obligatoryjnym. Poszukiwanie sprawdzonego podejścia do zarządzania projektami ukierunkowane zostało na metodę budowania jakości rozumianej jako „sposób myślenia, który powoduje, że stosuje się i bez przerwy poszukuje najlepszych rozwiązań”²⁰. Określone zostały kluczowe elementy zarządzania projektami przez jakość, które zakładają, że doskonalenie z założenia powinno stanowić stały, mierzalny cel, służący ulepszeniu, poprawie, identyfikowaniu problemów i dysfunkcji. Dostosowana do potrzeb organizacji metoda oraz projakościowe podejście do prowadzenia przedsięwzięć teleinformatycznych omówione zostały w ujęciu powszechnie przyjętym za najbardziej skuteczne — jako proces polegający na nieustannym dążeniu do doskonałości. Sukces projektów teleinformatycznych powiązано z wypełnieniem założeń przyjętych w strategii organizacji. Umiejętne określenie krytycznych czynników powodzenia projektu ma zapewnić ciągłość procesu tworzenia i rozwoju wytwarzanych rozwiązań teleinformatycznych oraz decydować o korzyściach i skali sukcesu osiągniętego przez organizację. Odnosząc się do stosowanych sposobów zapewnienia wysokiej jakości projektów teleinformatycznych, dokonano oceny aktualnego stanu przygotowań i zdolności Policji do wykorzystania szans i podjęcia wyzwań, jakie stawia przed nią nieubłagane postępujące zjawisko cyfryzacji.

¹⁹ Szerzej M. Paździor, *Konstytucyjne organy administracji publicznej właściwe w sprawach bezpieczeństwa narodowego* [w:] W.S. Kucharski (red. nauk.), *Zadania administracji rządowej i organów samorządu terytorialnego w zakresie bezpieczeństwa i porządku publicznego*, Lublin 2009.

²⁰ J. Pośpiech, M. Szepelawy, *Aspekty jakości europejskiego wychowania fizycznego*, „*Annales Universitatis Mariae Curie-Skłodowska*” 2005, Vol. 60, suppl. 16, nr 542, s. 404.

W rozdziale trzecim, na bazie diagnozy poziomu usług świadczonych przez pion teleinformatyki policyjnej uzasadniono potrzebę kontynuowania dotychczas przyjętego kierunku prac i zapewnienia projakościowej metody zarządzania, aby możliwe było skorzystanie z oferty innowacyjności otoczenia. Podkreśliwszy specyfikę rozwiązań IT, uznawanych powszechnie za projekty wysokiego ryzyka, wskazane zostały elementy, które w sposób istotny wpływają na poprawę jakości ich rezultatów. Skonkretyzowane zostały obszary wymagające wprowadzenia działań naprawczych i nowych rozwiązań. Opisane zmiany w podejściu do zarządzania projektami mają służyć skutecznemu wdrażaniu innowacyjnych rozwiązań i technologii, a w konsekwencji osiągnięciu celów biznesowych organizacji. Uporządkowane, dostosowane do potrzeb i możliwości organizacji podejście do realizacji projektów, przy zaangażowaniu profesjonalnych zespołów i kierownictwa organizacji, ma dawać podstawę do nowych, innowacyjnych, niestandardowych i twórczych rozwiązań. Przedyskutowano tu wady i zalety organizacji struktur, dedykowanych do prowadzenia projektów, pod kątem zastosowania w Policji jako instytucji zhierarchizowanej. Zaproponowane zmiany kierunków organizacyjno-prawnych zostały potraktowane jako siła organizująca, służąca utrwalaniu porządku. Uporządkowanie procesów wewnętrznych wpłynąć ma na zwiększenie wydajności pionu teleinformatyki policyjnej do sprawnego reagowania na szanse i wyzwania, jakie stawia przed nim rewolucja w świecie technologii.

Założenia budowy użytecznej metodyki zarządzania projektami teleinformatycznymi w Policji przedstawiono w sposób szczegółowy w rozdziale czwartym. Główną przesłanką opracowania metody zarządzania projektami była potrzeba wdrożenia narzędzia dostosowanego do możliwości i zidentyfikowanych potrzeb organizacji. Zaproponowane zostało heurystyczne podejście oparte na twórczym myśleniu²¹, poprzedzone analizą ogólnodostępnych metod zarządzania projektami IT. Działania zarządcze oraz dobrane do ich specyfiki techniki i narzędzia mają wspomagać aktualnie nierozwiązane kwestie, zwiększając tym samym szanse powodzenia rezultatów planowanych przedsięwzięć.

W rozdziale piątym wykazany został związek pomiędzy jakością wdrażanych rozwiązań teleinformatycznych w Policji a jej bezpieczeństwem. Poruszona problematyka bezpieczeństwa daje obraz ewolucji tego pojęcia. Na podstawie istniejących definicji i poglądów omówiony został jego fenomen w różnych kontekstach. Przedstawiona potrzeba nowego spojrzenia na bezpieczeństwo Policji wynika ze zmian cywilizacyjnych, których główne kierunki wytyczają: globalna informatyzacja, płynna rzeczywistość, pogłębiająca się specjalizacja, atomizacja jednostek²². Społeczeństwo informacyjne wymusza ciągły rozwój metod

²¹ M. Jełowicki, W. Kieżun, Z. Leoński, B. Ostapczuk, *Teoria organizacji i kierownictwa*, Warszawa 1979, s. 223.

²² A. Mrozek, *Zarządzanie bezpieczeństwem organizacji o strukturze heterarchicznej*, „Securitologia. Zeszyty Naukowe European Association for Security” 2011, nr 2 (14), s. 88–100.

zbierania, przetwarzania i wykorzystywania informacji w procesach rozwojowych²³. Zważywszy na wymagania, przed jakimi obecnie stoi ludzkość, pojęcie bezpieczeństwa Policji odniesiono do kondycji organizacji, która, aby trwać i rozwijać się, musi umiejętnie reagować na zmiany w otoczeniu i nadążać za postępowaniem cywilizacyjnym. Utrzymując, że bezpieczeństwo jest jedną z najważniejszych potrzeb egzystencjonalnych i stanowi wartość dla organizacji, niniejsza praca wykazuje, że w obszarze teleinformatyki staje się ono funkcją jakości wdrażanych rozwiązań i technologii. Może być traktowane jako wyzwanie, ale również jako zagrożenie, postrzegane jako sytuacje, które nie są przez podmiot uświadamiane albo są dostrzegane zbyt późno, co wiąże się z poważnymi konsekwencjami²⁴.

Policja, podobnie jak inne instytucje sektora publicznego, dostarcza specyficzne usługi dla społeczeństwa, zarządzanie którymi musi być oparte na odpowiedzialności za konkretne wyniki, gwarantujące jednocześnie przestrzeganie zasad racjonalizacji i celowości wydatków publicznych²⁵. Wymagają więc właściwie dobranego podejścia, zbudowanego na kulturze organizacji otwartej na innowacje, zbieżnego ze szczególnymi uwarunkowaniami ekonomicznymi, prawnymi i organizacyjnymi, aby mogły realizować misję państwa. Umiejętne radzenie sobie z wyzwaniami, jakie stawia przed Policją otoczenie, oznacza konieczność dostosowania się do nowych trendów i coraz bardziej wymagających technologii.

W prowadzonych rozważaniach wykorzystane zostały wyniki badań opracowanych na potrzeby rozprawy doktorskiej autorki, pt. *Organizacyjno-prawne kierunki zmian zarządzania projektami teleinformatycznymi w Policji*. Wykorzystane opinie uczestników przedsięwzięć IT zrealizowanych w Policji uzupełniły ocenę aktualnego stanu gotowości Policji do podejmowania wyzwań w obszarze IT i pozwoliły opracować pożądane kierunki zmian, które przyczynią się do zapewnienia długofalowego rozwoju całej organizacji.

Jako autorowi pozostaje mi wierzyć, że prowadzone w niniejszej publikacji rozważania przyczynią się do nowego spojrzenia na kwestie bezpieczeństwa Policji. Bezprecedensowa złożoność i niepewność dzisiejszego otoczenia w połączeniu z burzliwym rozwojem technologii informacyjnych i wzrastającą dynamicznością organizacji powodują, że zmiany wymaga całe podejście do sposobu generowania wyborów strategicznych²⁶. Adaptacja nowego podejścia do zagadnień teleinformatyki pozwoliłaby stawić czoła wyzwaniu współczesności i skutecznie budować sukces instytucji, takich jak Policja, wspierając proces wzrostu ich bezpieczeństwa.

²³ J. Strojny, B. Stankiewicz, *Wielowymiarowa analiza przedsiębiorczości — metodologia, narzędzia i znaczenie dla społeczeństwa informacyjnego*, „Przedsiębiorczość — Edukacja” 2009, nr 5, s. 117–132.

²⁴ B. Wiśniewski, *System bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne*, Szczytno 2013, s. 33.

²⁵ B. Bobińska, *Funkcjonowanie sektora publicznego jako organizacji „otwartych na klienta”*, „Zeszyty Naukowe Zachodniopomorskiej Szkoły Biznesu. Firma i Rynek” 2012, nr 1, s. 62.

²⁶ P. Płoszajski, *Organizacja przyszłości: przerażony kameleon*, Warszawa 2005, s. 5.

ROZDZIAŁ I

Teleinformatyka policyjna w obliczu globalnej informatyzacji

Schyłek XX w. to początek nowego spojrzenia na aspekty związane z pojęciem bezpieczeństwa, w tym na sposoby myślenia o bezpieczeństwie i zapewniania bezpieczeństwa. Współczesna koncepcja bezpieczeństwa obejmuje znacznie szerszy wymiar niż w przeszłości. Dawne pojęcie bezpieczeństwa obejmowało w zasadzie polityczne i militarne aspekty. Wraz z rosnącą liczbą potencjalnych źródeł zagrożeń współczesne pojmowanie bezpieczeństwa zakłada jego kompleksowe traktowanie. Obecnie zwraca się również uwagę na pozamilitarne aspekty tej problematyki oraz jej personalne i strukturalne konteksty²⁷. Dzisiaj obejmuje ono również ekonomiczne zależności i współzależności, kwestie zasobów surowcowych, ekologię, demografię, sprawy społeczne i humanitarne, zagadnienia związane z zachowaniem narodowej tożsamości i zapewnieniem właściwego udziału w rozwoju cywilizacyjnym współczesnego świata²⁸. Bezpieczeństwo jest konfiguracją sytuacji, zdarzeń, faktów, stanów rzeczy, niezależnych od ludzi, czyli czynników obiektywnych, ale także konfiguracją czynników od ludzi zależnych, subiektywnych, stanowiących konsekwencję istnienia *homo sapiens* w jego relacjach z otoczeniem²⁹. Szeroko pojmowane zjawisko bezpieczeństwa, które uznawane jest za jedną z najważniejszych potrzeb i wartości, jako atrybut³⁰ decyduje o istnieniu i perspektywicznym funkcjonowaniu danego podmiotu. Stąd bezpieczeństwo organizacji może być postrzegane w wielu wymiarach i dotyczyć wielu sfer jej działalności. W sensie praktycznym, jak ujmuje Stanisław Koziej, zapewnienie bezpieczeństwa polega na zmierzaniu do „zapewnienia możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach, poprzez wykorzystanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukcja ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów”³¹. Przyjmując, że bezpieczeństwo jest jedną z funkcji

²⁷ W. Pokruszyński, *Teoretyczne aspekty bezpieczeństwa*, Józefów 2010, s. 5.

²⁸ K. Świdorski, *Bezpieczeństwo narodowe w aspekcie polskiej racji stanu — kontekst socjologiczny*, Wrocław 2008, s. 218.

²⁹ W. Tulibacki, *Etyczne aspekty bezpieczeństwa na tle pewnych „stałych” cech natury ludzkiej* [w:] R. Rosa (red.), *Edukacja do bezpieczeństwa i pokoju w jednoczącej się Europie. Teoria i jej zastosowanie. Materiały z konferencji naukowej*, Siedlce–Chlewiska 1999, s. 33.

³⁰ J. Świniarski, *O naturze bezpieczeństwa. Prolegomena do zagadnień ogólnych*, Warszawa–Pruszków 1997, s. 170–185.

³¹ S. Koziej, *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, Toruń 2006, s. 7.

jakości³², organizacja, jako reprezentacja struktur, strategii i zbiorowości ludzkich, musi istnieć i być w odpowiedniej kondycji, aby dysponować niezbędnymi zasobami i w sposób ciągły realizować swoje cele.

Zważywszy na obserwowany w ostatnich latach ogromny postęp technologiczny i związaną z tym wszechobecną informatyzację procesów i wykorzystywanych rozwiązań, dziedziną kluczową dla rozwoju organizacji stała się teleinformatyka. Wraz z wykorzystaniem nowych technologii i narzędzi informatycznych państwa realizują swoje cele, a społeczeństwa podstawowe potrzeby. Teleinformatyka przestała być domeną wybranych działów i, stosowana wszechstronnie, w pełni decyduje o sukcesie organizacji. Niestety, zważywszy na fakt, że projekty prowadzone w obszarze teleinformatyki uznawane są za szczególnie trudne i określane jako zadania wysokiego ryzyka, specjaliści z dziedziny technologii informatycznych uważani są zarówno za kreatorów postępu cywilizacyjnego, jak i obarczani winą za nieudane przedsięwzięcia i stracone szanse³³. Badania prowadzone na świecie i opracowywane na ich podstawie statystyki pokazują, że niespełna 20% spośród ogólnej liczby projektów, planowanych w obszarze teleinformatyki, kończy się pełnym sukcesem. Należy mieć na względzie, że projekty i produkty informatyczne charakteryzuje szczególna złożoność i mogą one dotyczyć nieograniczonej liczby zmieniających się w czasie dziedzin problemowych, takich jak finanse, inżynieria techniczna, zarządzanie, które z kolei uzależnione są od zmieniającego się prawa, rynku i technologii. James R. Beniger zwraca uwagę, że obecne społeczeństwa z jednej strony są świadome zagrożeń i gotowe je ograniczać, z drugiej strony prezentują deficyt kontroli nad procesami powodowanymi w coraz większej mierze przez ekspansję nowych technologii³⁴. Fascynacja informatyzacją, wbrew naturalnym oczekiwaniom, że jej ekspansja wesprze proces wzrostu bezpieczeństwa, często przeradza się w zagrożenie dla funkcjonowania nieprzygotowanych na nie organizacji. Jest to zagrożenie powodowane przede wszystkim możliwością utraty kontroli nad technologiami, które w dynamiczny sposób kreują kierunki rozwoju. Dlatego, w trosce o dobry interes organizacji, tym większego znaczenia nabiera prawidłowe osadzenie kwestii teleinformatyki w celach organizacji i zasad związanych z jej funkcjonowaniem. Pion teleinformatyki musi być w pełni wydolny, by reagować na bieżące i docelowe potrzeby, zapewniając bezpieczeństwo organizacji przez pewność, dostępność i skuteczność wdrożonych rozwiązań teleinformatycznych.

Każda jednostka może być podmiotem bezpieczeństwa. Policja jest jedną z wiodących służb, które realizują prawny obowiązek administracji państwowej, stojąc na straży prawa. Zgodnie z treścią ustawy z 6 kwietnia 1990 r. o Policji³⁵,

³² A. Adamczyk, J. Radziulis, R. Renk, W. Hołubowicz, *Polityka bezpieczeństwa organizacji „na miarę”*, referat opublikowany w serwisie internetowym PLOUG — Polish Oracle User Group, <www.ploug.org.pl/konf_06/materialy/pdf/14_Adamczyk.pdf>, 1 lipca 2015 r.

³³ J. Górski (red.), *Inżynieria...*, wyd. cyt., s. 11.

³⁴ J.R. Beniger, *The Control Revolution, Technological and Economic Origins of the Information Society*, Cambridge 1986.

³⁵ Tekst jedn. DzU z 2015 r., poz. 355 (dalej: ustawa o Policji).

ta umundurowana i uzbrojona formacja przeznaczona jest do ochrony bezpieczeństwa ludzi i mienia oraz do utrzymywania bezpieczeństwa i porządku publicznego, stanowiąc fundament stabilnego i bezpiecznego państwa. Również realizacja nadrzędnego celu *Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej* z 2007 r. wymaga od Policji utrzymania zdolności do reagowania w przypadku wystąpienia zagrożeń bezpieczeństwa publicznego oraz bezpieczeństwa powszechnego, związanych z ochroną porządku prawnego, życia i zdrowia obywateli oraz majątku narodowego przed bezprawnymi działaniami oraz skutkami klęsk żywiołowych, katastrof naturalnych i awarii technicznych. Realizacja powyższego wymaga doskonalenia działalności wszystkich podmiotów państwowych i społecznych, których aktywność związana jest z bezpieczeństwem wewnętrznym państwa³⁶. Nadrzędnym zadaniem w zakresie informatyzacji jest powszechna implementacja rozwiązań podnoszących stan techniczny systemów i sieci teleinformatycznych oraz poziom świadczenia usług drogą elektroniczną do przeciętnego poziomu ich rozwoju w krajach Unii Europejskiej³⁷. Zapewnienie bezpieczeństwa wewnętrznego pozostaje w ścisłym związku z bezpieczeństwem narodowym, definiowanym jako najważniejsza wartość, potrzeba narodowa i priorytetowy cel działalności państwa, jednostek i grup społecznych, a jednocześnie proces obejmujący różnorodne środki, gwarantujące trwałe, wolne od zakłóceń byt i rozwój narodowy (państwa), w tym obronę państwa jako instytucji politycznej oraz ochronę jednostek i całego społeczeństwa, ich dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie lub godzą w dobra podlegające szczególnej ochronie³⁸. Pośród priorytetów strategii operacyjnej opisanych w *Strategicznym przeglądzie bezpieczeństwa narodowego*, znajdują się takie, które zakładają „utrzymanie własnej determinacji i gotowości w pełnym spektrum dziedzin, obszarów i sektorów bezpieczeństwa narodowego”³⁹. Opcje strategii preparacyjnej zakładają wykorzystanie „racjonalnie umacnianych zdolności sukcesywnie integrowanego narodowego potencjału bezpieczeństwa”⁴⁰. Wymóg realizacji celów i obowiązków ustawowych nałożonych na Policję skutkuje koniecznością zapewnienia odpowiednich zasobów i rozwiązań, które kształtować będą zdolność organizacji do trwania, współpracy z otoczeniem i perspektywicznego doskonalenia, determinując jednocześnie poziom bezpieczeństwa organizacji, bezpieczeństwa wewnętrznego i bezpieczeństwa narodowego. Zarówno bezpieczeństwo, jak i zagrożenia powodujące zakłócenia uznawanych za bezpieczne warunków funkcjonowania danego

³⁶ Biuro Bezpieczeństwa Narodowego, *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2007, s. 15.

³⁷ Tamże, s. 29.

³⁸ W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011, s. 22–31.

³⁹ Biuro Bezpieczeństwa Narodowego, *Strategiczny przegląd bezpieczeństwa narodowego — główne wnioski i rekomendacje dla Polski*, Warszawa 2012, s. 7.

⁴⁰ Tamże, s. 7–8.

podmiotu podlegają gwałtownym oraz dynamicznym przeobrażeniom⁴¹. Troska o bezpieczeństwo i wszechobecne poczucie zagrożeń spowodowane wzrostem przestępczości, rozbudowującymi się organizacjami mafijnymi i terrorystycznymi, prezentowaniem w mediach scen przemocy oraz nasilającymi się zjawiskami agresji w zachowaniach ludzi, katastrof i awarii technicznych wymusza poszukiwanie metod gwarantujących likwidację lub chociażby ograniczenie negatywnych zjawisk⁴².

Skuteczność działania Policji wymaga zapewnienia wysokiej jakości usług w obszarze teleinformatyki, który został powszechnie uznany w tym względzie za krytyczny z punktu widzenia potrzeby zapewnienia długofalowego funkcjonowania organizacji. Pion teleinformatyki musi reagować na rosnące wymagania zarówno organizacji, jak i otoczenia, uwarunkowane postępem technologicznym, potrzebami użytkownika, aktami prawa wewnętrznego czy zobowiązaniami międzynarodowymi. Wywiązywanie się z obowiązków nałożonych na Policję wymusza konieczność wdrożenia niezawodnych i często złożonych innowacyjnych rozwiązań teleinformatycznych, które z punktu widzenia funkcjonariuszy usprawnią dostęp do informacji, zapewnią ich analizę, czy uwiarygodnią sprawdzane dane. Istotne jest przy tym zapewnienie elastycznego podejścia wdrażania rozwiązań, pozostających w zgodności z założeniami, ograniczeniami, wymaganiami użytkownika końcowego i oczekiwaniami biznesowymi. W celu zapewnienia owocnej współpracy wszystkich uczestników projektów należy zadbać o zasoby, strukturę zarządzania, mechanizmy komunikacji, jak również odpowiedni poziom wiedzy i zaangażowania członków organizacji na wszystkich jej szczeblach.

Wprowadzane od 2005 r. przepisy w sprawie prowadzenia w Policji przedsięwzięć teleinformatycznych przyniosły wymierne efekty. Nowe podejście poskutkowało wzrostem liczby zrealizowanych projektów, jak również wzrostem liczby złożonych, unikatowych, nowatorskich rozwiązań. Dzięki wprowadzeniu pierwszych regulacji w obszarze zarządzania projektami, Policja poradziła sobie z terminowym wydatkowaniem funduszy pochodzących ze środków pomocowych Unii Europejskiej, które pozwoliły m.in. na sfinansowanie nowych technologii. Funkcjonujące zasady zarządzania przedsięwzięciami teleinformatycznymi ograniczały się do wskazania trybu obiegu dokumentów w kolejnych etapach prac oraz podstawowych narzędzi wspomagających przyjęty sposób prowadzenia projektów. Wymagają więc nowego spojrzenia, aktualizacji oraz uzupełnienia, aby odpowiadać na pojawiające się szanse, wyzwania oraz potrzeby organizacji i otoczenia.

Spójne aplikacje informatyczne i ogólnodostępne policyjne bazy danych służące do gromadzenia, utrzymania i przetwarzania przez Policję informacji, prowadzenia

⁴¹ B. Wiśniewski (red. nauk.), *Bezpieczeństwo w teorii i badaniach naukowych*, Szczepno 2011, s. 11.

⁴² J. Fiebig, M. Róg, A. Tyburska (red.), *Bezpieczeństwo to wspólna sprawa. Ochrona bezpieczeństwa publicznego — rozwiązania systemowe w skali kraju i regionu*, Szczepno 2002, s. 3.

analiz i sporządzania statystyk, jednolite narzędzia uwierzytelniania i autoryzacji, zapewnienie sprawnej komunikacji i transmisji danych w czasie rzeczywistym — to potrzeby funkcjonariuszy, których realizacja wymaga podjęcia wyzwania i wprowadzenia udoskonaleń i usankcjonowania praktyk zmierzających do wprowadzenia zmian organizacyjno-prawnych i prawidłowego osadzenia w Policji kwestii jakości projektów IT. Niewątpliwie brak obligatoryjnie stosowanego spójnego podejścia do zarządzania projektami teleinformatycznymi w Policji, formalnych uregulowań w tym zakresie oraz kultury organizacji ogranicza możliwości oraz sprawność prowadzenia przedsięwzięć, w szczególności zadań złożonych, skomplikowanych technologicznie, w których wymagana jest szeroka wiedza, dyscyplina oraz zaangażowanie użytkownika końcowego. Wdrożenie metodyki zarządzania projektami IT w Policji ma zwiększyć poziom jakości prowadzonych projektów, zapewniając gotowość i skuteczność organizacji do realizacji celów. Dedykowana dla Policji i dostosowana do jej potrzeb metodyka pozwoli w sposób profesjonalny prowadzić projekty, w tym usuwać napotymane problemy i minimalizować z odpowiednim wyprzedzeniem identyfikowane ryzyko. Rezultaty projektów, wprowadzając Policję w erę nowoczesnych technologii i innowacyjnych rozwiązań, zapewnią jej zdolność do profesjonalnego, efektywnego i racjonalnego wywiązywania się z nałożonych na nią obowiązków, przyczyniając się tym samym do zapewnienia bezpieczeństwa organizacji.

