UWARUNKOWANIA WDRAŻANIA INNOWACJI W PRZEDSIĘBIORSTWIE NA PRZYKŁADZIE WPROWADZANIA ZMIAN W OBASZARZE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Michał PAŁĘGA, Marcin KNAPIŃSKI, Wiesław KULMA

Streszczenie: W artykule zwrócono uwagę na podstawowe aspekty związane z problematyką wdrażania innowacji organizacyjnej w przedsiębiorstwie produkcyjnym. Przedstawiono w nim istotę oraz klasyfikację innowacji, dokonano identyfikacji podstawowych barier wdrażania innowacji, a także wskazano na wiodącą rolę czynnika ludzkiego determinującego powodzenie wprowadzania zmian. Rozważania teoretyczne w tym zakresie wzbogacone zostały o studium przypadku (case study), związany z implementacją nowych z punktu widzenia przedsiębiorstwa rozwiązań z zakresu zarządzania bezpieczeństwem informacji. Przedstawiony w artykule case stady dotyczy przeszłości.

Słowa kluczowe: bariery innowacyjności, bezpieczeństwo informacji działalność innowacyjna, innowacja, zarządzanie zmianami

1. Wstęp

Podstawową siłę napędową rozwoju każdego przedsiębiorstwa stanowią innowacje rozumiane jako nowe (ulepszone, zmodernizowane) produkty, usługi, technologie, systemy operacyjne czy metody zarządzania.

Pojęcie innowacji po raz pierwszy zostało wprowadzone do literatury ekonomicznej w 1911 roku przez Josepha Schumpetera. Według niego innowacja oznacza [1]:

1) wprowadzenie nowego towaru, z jakimi konsumenci nie mieli jeszcze do czynienia, lub nowego gatunku jakiegoś towaru;
2) wprowadzenie nowej metody produkcji jeszcze praktycznie nie wypróbowanej w danej dziedzinie przemysłu;
3) otwarcie nowego rynku, czyli takiego, na którym dany rodzaj krajowego przemysłu uprzednio nie działał i to bez względu, czy rynek ten istniał wcześniej, czy też nie;
4) zdobycie nowego źródła surowców lub półfabrykatów i to niezależnie od tego, czy źródło to istniało, czy też musiało być dopiero stworzone;
5) wprowadzenie nowej organizacji jakiegoś przemysłu, np. stworzenie monopolu bądź jego złamanie.

Definicja sformułowana przez J. Schumpetera stanowiła punkt wyjścia rozważań o znaczeniu innowacji w gospodarce. Na przestrzeni lat zarówno samo pojęcie innowacji, jak również zainteresowanie nauki problematyką innowacji ulegało systematycznej ewaluacji przede wszystkim za sprawą przemian systemu techniczno- ekonomicznego gospodarki, jakie rozpoczęły się pod koniec XX wieku. Stąd też wynika, że klasyczna koncepcja schumpeterowska ustąpiła miejsca innym, nowym koncepcjom. Współcześnie innowacje postrzega się w ujęciu wąskim (*sensu stricto*) oraz szerokim (*sensu largo*)[2]. W ujęciu

wąskim innowacja oznacza wynalazek, który znajduje zastosowanie w produkcji, z kolei ujęcie szerokie identyfikuje innowacje z procesem zarządzania, obejmującym różnorodne czynności, prowadzące do tworzenia, rozwijania i wprowadzania nowych wartości w produktach lub nowych połączeń środków i zasobów, które są nowością dla tworzącej lub wprowadzającej jej jednostki [3].

Podział przedmiotowy prezentowany w Podręczniku Oslo Manual [4] rozróżnia następujące rodzaje innowacji (rys.1.):

- produktowe – polegające na udoskonaleniu wprowadzanych na rynek produktów (ulepszenie parametrów technicznych, materiałów i półfabrykatów, funkcjonalności), które mogą dostarczyć konsumentom obiektywnie nowych bądź większych korzyści;
- procesowe (technologiczne) – będące rezultatem przyjęcia nowej metody produkcji lub realizacji usług, w tym zastosowanie w przedsiębiorstwie nowych i ulepszonych procesów technologicznych, maszyn i urządzeń, oprogramowania;
- organizacyjne – wyrażające się wprowadzeniem nowej metody organizacji: w praktyce biznesowej firmy, miejsc pracy cz też w relacjach zewnętrznych (np. nowe metody współpracy z dostawcami, nowe metody podziału obowiązków i podejmowania decyzji);
- marketingowe – oznaczające wprowadzenie nowej metody marketingowej, obejmującej ważne dla przedsiębiorstwa zmiany w wyglądzie produktu i opakowania, promocji, strategii cenowej, dystrybucji.

Rys. 1. Rodzaje innowacji
Źródło: opracowanie własne [4]

W niniejszej publikacji przedmiotem rozważań są uwarunkowania wdrażania innowacji organizacyjnej, polegającej na wprowadzeniu w strukturę wybranego przedsiębiorstwa produkcyjnego nowego systemu zarządzania bezpieczeństwem informacji, opracowanego w oparciu o identyfikację i ocenę zagrożeń bezpieczeństwa informacji i zawierającego kierunki działań zmierzające do zapobiegania ich powstawaniu. Ze względu na zakres opracowania szczegółowa charakterystyka ww. systemu została pominięta. Celem artykułu jest przede wszystkim wskazanie możliwych do wystąpienia barier związanych z wdrażaniem innowacji oraz wskazanie sposobów ich pokonywania. W opinii autorów, niniejsza publikacja ma charakter utylitarny, związany z dostarczeniem informacji nt. czynników determinujących wprowadzanie zmian organizacyjnych.

2. Wybrane uwarunkowania wdrażania zmian w zarządzaniu bezpieczeństwem informacji

Wdrażanie skutecznego programu zmian zarządzania bezpieczeństwem przetwarzanych w przedsiębiorstwie danych i informacji jest decyzją strategiczną, a zarazem wymagającą pokonania wielu różnych przeszkód i barier. Podobnie, jak w przypadku każdego projektu wdrażania innowacji, wprowadzanie wszelkich zmian i przedsięwzięć ukierunkowanych na poprawę poziomu bezpieczeństwa informacji jest procesem dokonującym się w warunkach zmiennego otoczenia zewnętrznego i wewnętrznego. Wobec powyższego zakłada się, że każda organizacja zobligowana jest do **wypracowania indywidualnej strategii wprowadzania zmian**, która swoim zakresem będzie integrowała wymagania stawiane ze strony rynku i otoczenia z własnymi możliwościami przedsiębiorstwa [5]. Jak pisze [6] *„taka strategia, rozumiana jako pewna koncepcja zasadniczych celów firmy a zarazem zestaw decyzji, dopasowujących jej potencjał, organizację i działalność do zmieniającego się otoczenia, powinna precyzować konkretne reguły sterowania zmianami i wprowadzania ich do praktyki”*. Niezbędne w tym zakresie jest **pełne zaangażowanie najwyższego kierownictwa**, które powinno informować personel o poziomie zaawansowania prac oraz przekonywać ich do wdrażanych przeobrażeń [7]. W praktyce gospodarczej kierownictwo zarządzając zmianami powinno koncentrować się przede wszystkim na [6]:

- rozpowszechnianiu poglądu o potrzebie wprowadzenia zmian oraz przekonywaniu pracowników, że proponowane zmiany są słuszne;
- opracowaniu i popularyzowaniu wizji przyszłej roli działalności przedsiębiorstwa na tle rynku;
- prezentowaniu korzyści wynikających z wdrażanych zmian, zarówno w skali globalnej organizacji, jak również dla indywidualnego pracownika;
- argumentowaniu słuszności podejmowanych zmian, właściwym przygotowaniu i zaplanowaniu procesu ich wprowadzania;
- upowszechnianiu zmian przez osoby mające autorytet;
- kształtowaniu nastroju organizacyjnego ukierunkowanego na relacje między współpracownikami, otwartość i zaufanie pozwalające niwelować wszelkie obawy i trudności oraz wspólnie rozwiązywać pojawiające się problemy;
- przyjęciu przez kierownictwo postawy inicjatora i rzecznika nowości.

Reasumując można więc stwierdzić, że to przede wszystkim od inicjatywy, staranności i determinacji kierownictwa zależy stopień realizacji celów oraz sukcesów związanych z wdrażaniem innowacji, jakie są możliwe do osiągnięcia przez przedsiębiorstwo. Wobec powyższego w zakresie wprowadzania nowych metod dotyczących zarządzania bezpieczeństwem informacji, kierownictwo winno skupiać uwagę na zachodzących w jego otoczeniu zmianach, monitorować potrzeby wszystkich zainteresowanych podmiotów, rozumieć je oraz szybko i umiejętnie na nie reagować.

Oczywistym jest, że rozwój współczesnej organizacji gospodarczej dyktowany jest poprzez funkcje pozyskiwania danych i informacji, a co się z tym wiąże ich ochrony. Nie sposób wyobrazić sobie tych funkcji bez dostatecznej wizji racjonalizowania systemu zarządzania bezpieczeństwem informacji oraz podejmowania różnego typu inicjatyw w tym zakresie.

To właśnie na kierownictwie najwyższego szczebla zarządzania spoczywa obowiązek ustanawiania polityki bezpieczeństwa, definiowania celów w odniesieniu do ochrony informacji, zagwarantowania odpowiednich środków profilaktycznych oraz diagnozowania

aktualnego stanu bezpieczeństwa.

Skuteczne funkcjonowanie systemu bezpieczeństwa informacji zapewnia **jasny i zrozumiały podział ról i obowiązków**. Zaangażowane w poprawę stanu bezpieczeństwa kierownictwo nadzoruje, aby wszyscy pracownicy znali swoje zadania oraz schematy postępowania. Zrozumiały podział ról i obowiązków w odniesieniu do bezpieczeństwa informacji jest jednym z podstawowych mechanizmów ograniczania błędu ludzkiego.

Jak podaje literatura przedmiotu [8,9,10] ważnym zadaniem w zakresie wdrażania zmian jest zaangażowanie w ten proces wszystkich zainteresowanych jednostek i podmiotów już w jego początkowej fazie wprowadzania oraz spójnego scalenia interesów organizacji oraz celów realizowanych zmian z indywidualnymi potrzebami i motywacjami [11].

Z prezentowanych treści wynika, że w procesie wprowadzania zmian uczestniczyć powinni wszyscy pracownicy jednostki organizacyjnej. Niemniej jednak zakres ich aktywności determinowany jest przez poszczególne etapy tego procesu. Z pewnością inne będzie zaangażowanie personelu w początkowej fazie obejmującej zbieranie i wymianę informacji oraz diagnozę organizacyjną, inne zaś podczas właściwego procesu przygotowywania i realizacji zmiany [12].

W myśl współczesnych koncepcji zarządzania zasobami ludzkimi **wspólne wyznaczanie celów organizacji** przez kierownictwo przy współudziale podwładnych wpływa motywująco na personel niższego szczebla. Partycypacja pracowników sprawia, że czują się oni współautorami celów bezpieczeństwa, co przyczynia się do wzrostu poczucia odpowiedzialności i zwiększania zaangażowania w ich realizację. Osoby takie chętniej i bez destrukcyjnego przymusu podejmują wszelkie działania oraz mobilizują pozostałych współpracowników w swoim otoczeniu. Należy jednak zwrócić uwagę, że partycypacja pracowników zakłada ciągłe i systematyczne włączanie podwładnych w ustalanie celów, a nie działania wybiórcze, dotyczące tylko sytuacji najtrudniejszych do rozwiązania [13,14, 15,16]. Wówczas pracownicy będą czuli, że ich przełożony zrzuca na nich odpowiedzialność za powodzenie określonego przedsięwzięcia. Postawa taka może jedynie wywołać skutek przeciwny do zamierzonego, czyli wpływać demotywująco na personel organizacji.

Wśród istotnych czynników determinujących efektywny proces doskonalenia systemu zarządzania bezpieczeństwem informacji bezsprzecznie należy wskazać także **nakłady finansowe oraz nakłady czasu i pracy**, jakie będzie musiało ponieść przedsiębiorstwo. Kluczowe znaczenie ma ich postrzeganie. Warto, aby kierownictwo rozpatrywało je w kategorii inwestycji, aniżeli nieuzasadnionych kosztów. Przejawem takiego właśnie myślenia będzie dokładnie zaplanowany budżet realizacji całego projektu, poprzedzony wnikliwą analizą kosztów związaną z implementacją odpowiednich mechanizmów ochronnych. Nawet szacunkowa znajomość kosztów pozwoli zapobiec sytuacji, w której przedsiębiorstwo będzie zmuszone wycofać się z realizacji przedsięwzięcia lub w znacznym stopniu ograniczyć jego zakres.

Rozważając strukturę nakładów finansowych związanych z doskonaleniem systemu bezpieczeństwa informacji uwzględnić trzeba m.in. zakup środków trwałych (takich jak: sprzęt komputerowy, oprogramowanie, licencje itp., materiały biurowe, dodatkowe wyposażenie pomieszczeń). Oprócz tego zaangażowania kapitału finansowego wymaga przygotowanie nowego stanowiska pracy, zorganizowanie oraz przeprowadzenie szkoleń dla całego personelu przedsiębiorstwa, a także usługi firm konsultingowych. Całkowity zakres kosztów jest kwestią indywidualną, wynikającą z wielkości jednostki gospodarczej oraz jej braków i potrzeb.

Poza powyżej wskazanymi warunkami ważną rolę odgrywa w tej sytuacji również czynnik ludzki.

Praktyka gospodarcza wskazuje, że głównymi barierami w realizacji procesu wdrażania innowacji w organizacji są [12, 17, 18]:

- lęk i niechęć pracowników przed nowością;
- przyzwyczajenie do starego;
- niechęć i brak zaangażowania pracowników;
- brak świadomości potrzeb zmian w organizacji;
- brak dostatecznej wiedzy;
- nieprzestrzeganie instrukcji i poleceń;
- przyjmowanie „drogi na skróty".

Niezmiernie ważne w procesie wdrażania zmian jest **zaangażowanie całego personelu**, począwszy od kadry kierowniczej najwyższego szczebla, poprzez kierowników i menadżerów średniego szczebla, skończywszy na pracownikach szeregowych. Partycypacja personelu wykonawczego powinna odbywać się na poziomie opracowywania systemu, jego wdrażania, a także doskonalenia. Z przyczyn przedstawionych powyżej nie jest to jednak zadanie proste, ale jak najbardziej potrzebne. Każdy pracownik organizacji posiada swój potencjał w postaci wiedzy, doświadczenia życiowego i zawodowego, umiejętności, talentów, inteligencji. Pełne ich wykorzystanie w procesie implementacji innowacji może stanowić o skuteczności realizowanego projektu. Niestety, przeciwwagę dla nich często stanowi opór pracowników, który może przejawiać się niechęcią, zachowaniami pasywnymi, a w wyjątkowych sytuacjach także postawą agresywną [19]. Źródłami tego typu zachowań są najczęściej [12]:

- brak wystarczającej wiedzy i przekonania nt. potrzeb inicjowanych zmian;
- niewłaściwy system komunikowania planowanych zmian;
- obawy przed następstwami nowego rozwiązania, adaptacją do nowych warunków, utratą dotychczasowego komfortu, itp.;
- brak zaufania do twórców i wykonawców wdrażanej innowacji;
- niska samoocena pracowników, która eskalowana jest w skutek nie włączania ich w prace związane z realizacją zmian;
- pasywne postawy personelu, takie jak np. niska potrzeba samorealizacji, niska potrzeba osiągnięć, słaba odporność na stres, niezdolność do podejmowania ryzyka;
- pejoratywne doświadczenia z wcześniej wdrażanych zmian;
- niewystarczające środki przeznaczone na realizację innowacji.

Wobec powyższego, **przezwyciężanie oporów pracowników wobec zmian** stanowi jeden z czynników determinujących sukces ich wdrażania w przedsiębiorstwie. Wynika z tego, że brak aprobaty personelu dla podejmowanej reorganizacji wzbudzać może różnego rodzaju niepożądane postawy i zachowania zatrudnionych [12]. Aby im zapobiec bądź ograniczyć zakres ich występowania menadżerowie organizacji mogą korzystać z wielu sprawdzonych rozwiązań, wśród których dominują: [20]

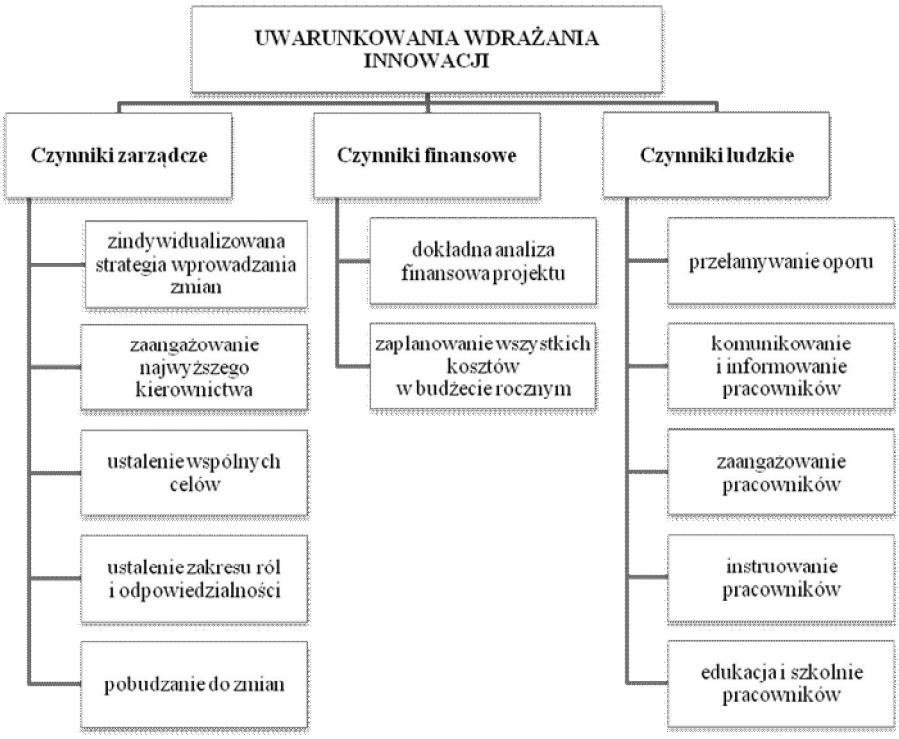
- dokładne informowanie wszystkich pracowników, których zmiany dotyczą o ich przyczynach i celach;
- aktywne uczestnictwo zatrudnionych w planowaniu i realizacji innowacji;
- budowanie warunków sprzyjających komunikacji i wspólnemu rozwiązywaniu pojawiających się problemów;
- uwzględnianie panujących już relacji międzyludzkich;
- wyraźne promowanie inicjatorów zmian;

- wystrzeganie się rozwiązań rewolucyjnych;
- współpraca z doradcami zewnętrznymi;
- możliwie szybka stabilizacja wprowadzanych zmian.

Dodatkowym czynnikiem, uzupełniającym zaprezentowane mechanizmy zapobiegające występowaniu oporu pracowników wobec zmian jest **aktywna i otwarta komunikacja ograniczająca ich niepewność**. Brak dostosowania właściwej komunikacji do potrzeb wynikających z wdrażania innowacji jest w opinii pracowników najczęstszym powodem niepowodzeń programów zmian [12]. Przyjmuje się zatem, że pracownikom powinna zostać przekazana rzetelna wiedza odnośnie istoty wprowadzonych w przedsiębiorstwie przeobrażeń oraz wynikających dla nich bezpośrednich konsekwencji (jak np. modyfikacja zakresu obowiązków).

Skuteczne funkcjonowanie systemu wspomagającego zarządzanie bezpieczeństwem osiągnąć można tylko, wówczas gdy cały personel organizacji będzie przekonany o słuszności wprowadzanych przepisów, procedur i instrukcji. Wobec tego, nieodzownym elementem procesu wdrożeniowego jest **szkolenie oraz edukacja pracowników**. Program oraz treść szkoleń powinny być każdorazowo dostosowywane do predyspozycji oraz zdolności intelektualnych słuchaczy, tak aby wszyscy uczestnicy poza wszelką wątpliwością potrafili przekazywaną im wiedzę zastosować w odniesieniu do rzeczywistych sytuacji.

Uwarunkowania skutecznego wdrażania innowacji w przedsiębiorstwie w ujęciu graficznym prezentuje rysunek 2.



Rys. 2. Warunki wdrażania systemu bezpieczeństwa informacji
Źródło: Opracowanie własne

3. Projekt wdrażania zmian w zakresie zarządzania bezpieczeństwem informacji dla wybranej jednostce organizacyjnej – case study

Przyjmuję się, że wdrażanie systemu zarządzania bezpieczeństwem informacji ściśle powiązane będzie z innymi działaniami jednostki organizacyjnej. Dlatego też moment rozpoczęcia wdrażania systemu jest niezwykle ważny i wybrany zostanie taki, który nie będzie kolidował z codzienną pracą. Nie zaleca się rozpoczynania wdrażania systemu bezpieczeństwa w momentach niezwykle ważnych dla przedsiębiorstwa, takich jak: wypuszczanie na rynek nowych produktów, przekształcenia organizacyjne, a także przed świętami, czy dłuższymi przerwami pracy.

Ponadto, należy zaznaczyć, iż sukces implementacji systemu uzależniony będzie od właściwego ukształtowania hierarchii oraz zależności pomiędzy pracownikami. Wymaga to zatem stworzenia ścisłego systemu odpowiedzialności i zależności między pracownikami przedsiębiorstwa, z jasnymi zasadami delegowania uprawnień. Sytuacja, gdy dwie osoby będą miały taki sam zakres odpowiedzialności oraz uprawnień może powodować zakłócenia w systemie bezpieczeństwa, a także prowadzić do utraty jego wiarygodności oraz konieczności istnienia.

Zakłada się, że planowy proces wdrożenia zmian w zakresie zarządzania bezpieczeństwem informacji w przedsiębiorstwie przebiegać będzie zgodnie z następującymi etapami (rys.3).

Etap pierwszy – stanowić będą działania marketingowe ukierunkowane na wskazanie potrzeby implementacji systemu, przełamywanie oporu pracowników do wprowadzanych zmian oraz pobudzanie ich do działań związanych z reorganizacją w przedsiębiorstwie. Na tym etapie szczególne znaczenie ma aktywna i otwarta komunikacja ograniczająca niepewność pracowników. W tym przypadku będzie ona realizowana za pośrednictwem kampanii informacyjnej, promującej korzyści z wdrażanego systemu.

Zanim to jednak nastąpi, kadra kierownicza, a w szczególności najwyższe kierownictwo musi przekonać się o potrzebie wdrażania systemu, zainteresować się problemem oraz uwierzyć w sens wprowadzanych zmian. Służyć temu mają: zebrania podczas których podejmowana będzie tematyka zarządzania bezpieczeństwem informacji, udział kierownictwa w szkoleniach i konferencjach z tej problematyki oraz wszelkiego rodzaju rozmowy nieformalne.

Niezbędne jest także przeprowadzenie szkolenia kierownictwa, które będzie miało na celu:

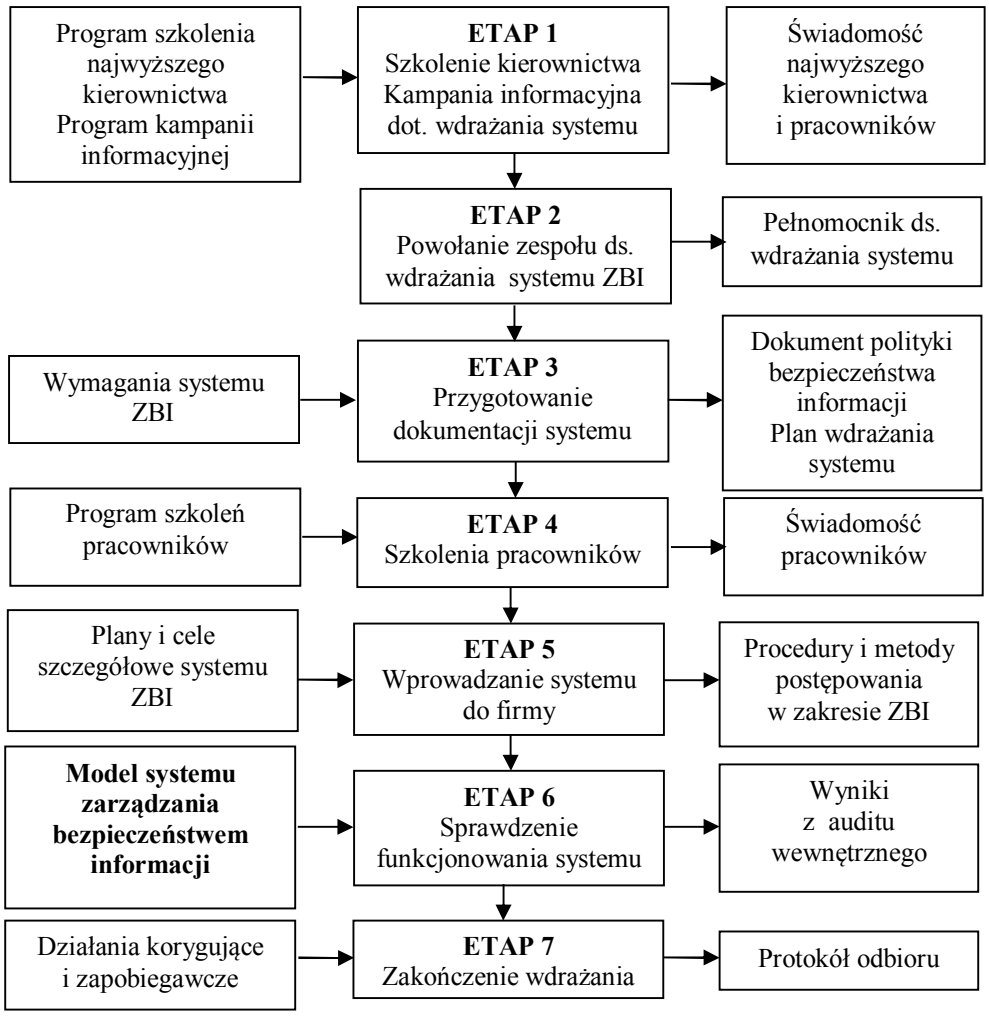
- przekazanie merytorycznej wiedzy z zakresu zarządzania bezpieczeństwem informacji;
- przekazanie informacji dotyczących procesu implementacji systemu w jednostce organizacyjnej oraz jego ewentualnych niebezpieczeństw oraz ich skutków;
- promowanie systemu bezpieczeństwa;
- propagowanie systemu wśród grupy osób, które są przeciwnikami systemu i stawiają one opór wobec wprowadzanych zmian.

Zakłada się, że w badanej jednostce gospodarczej inicjatorem wdrażania systemu będzie prezes zarządu spółki.

Etap drugi – dotyczyć będzie przedsięwzięć związanych z przygotowaniami organizacyjnymi przedsiębiorstwa.

Na początku tego etapu zostanie powołany specjalny zespół, którym zarządzać będzie przedstawiciel kierownictwa ds. wdrażania systemu zarządzania bezpieczeństwem

informacji. Pozostałymi jego członkami będą przedstawiciele wszystkich komórek organizacyjnych przedsiębiorstwa. Oprócz tego w skład zespołu wdrożeniowego wchodzić będzie konsultant zewnętrzny, posiadający doświadczenie we wdrażaniu systemów zarządzania bezpieczeństwem informacji. Zadaniem tego zespołu będzie przede wszystkim nadzór nad projektowaniem i wdrażaniem systemu.



Rys. 3. Algorytm wdrażania modelu systemu zarządzania bezpieczeństwem informacji
Źródło: opracowanie własne na podstawie wyników przeprowadzonych badań

Etap trzeci – koncentrować się będzie na sporządzeniu odpowiedniej dokumentacji (polityki bezpieczeństwa informacji), ustanowieniu celów i planów szczegółowych związanych z usuwaniem niedociągnięć stwierdzonych podczas procesu analizy ryzyka utraty bezpieczeństwa informacji. Ponadto, etap ten obejmować będzie także przystosowanie pomieszczeń do nowych wymagań oraz zastosowanie odpowiednich zabezpieczeń (np. instalację sprzętu, oprogramowania i innych urządzeń).

Etap czwarty – stanowić będą szkolenia dla wszystkich pracowników przedsiębiorstwa. Cykl szkoleń powinien podzielony być na bloki tematyczne, podczas których personelowi zostanie przekazana wiedza w zakresie:

- ogólnego funkcjonowania wdrażanego w przedsiębiorstwie modelu systemu zarządzania bezpieczeństwem informacji;
- szczegółowego działania poszczególnych podsystemów zarządzania bezpieczeństwem informacji;
- szczegółowego przedstawienia kompetencji, zakresu obowiązków i odpowiedzialności oraz procedur w zakresie bezpieczeństwa informacji dla każdego stanowiska pracy w przedsiębiorstwie;
- omówienia wpływu systemu na obowiązujące dotychczas procesy pracy oraz zmian, jakie spowoduje implementacja systemu;
- zaprezentowanie szczegółów dotyczących postępowania pracowników na terenie zakładu pracy i po za nim, np. w zakresie okazywania przepustek, sposobu postępowania z kartami wejściowymi i uwierzytelniającymi, sposobu konwersacji z pracownikami innych działów oraz osobami postronnymi na tematy służbowe, trybu wymiany dokumentów itd.

Etap piąty – składać się będzie z systematycznego wprowadzania poszczególnych zmian w zakresie zarządzania bezpieczeństwem informacji do komórek organizacyjnych przedsiębiorstwa. W szczególności etap ten dotyczyć będzie opracowywania i wdrażania nowych procedur i metod postępowania. Przyjmuje się, że implementacja systemu odbywać się w znacznych odstępach czasu, tak aby pracownicy mieli możliwość adaptacji do wprowadzanych zmian. Odpowiednio przyjęty przedział czasowy wdrażania systemu pozwoli na wykrycie i usunięcie wszelkich jego błędów i niedociągnięć.

Etap szósty – stanowić będzie sprawdzenie funkcjonowania systemu w praktyce, obejmujące monitorowanie i audytowanie oraz działania korygujące i zapobiegawcze.

Etap siódmy – oznaczać będzie formalne zakończenie implementacji systemu, potwierdzone odebraniem prac przez najwyższe kierownictwo jednostki organizacyjnej (zarząd) oraz podpisaniem protokołu odbioru.

W oparciu o powyżej przedstawione etapy sporządzono ramowy plan wdrażania systemu zarządzania bezpieczeństwem informacji dla wybranej jednostki gospodarczej, z podziałem na zadania oraz zakres odpowiedzialności (tab. 1).

Tab. 1. Plan wdrażania systemu zarządzania bezpieczeństwem informacji dla wybranej jednostki gospodarczej

Lp.	**Zadanie do wykonania**	**Odpowiedzialne komórki (osoby)**
1.	Powołanie zespołu ds. wdrażania systemu zarządzania bezpieczeństwem informacji (ZBI)	– Prezes zarządu
2.	Określenie i zakomunikowanie odpowiedzialności za wdrażanie systemu i związanych z nimi uprawnień	– Pełnomocnik ds. wdrażania systemu ZBI
3.	Zorganizowanie i przeprowadzenie szkoleń dla kadry kierowniczej w zakresie zarządzania bezpieczeństwem informacji	– Dział szkoleń
4.	Opracowanie projektu polityki bezpieczeństwa informacji	– Pełnomocnik ds. wdrażania systemu ZBI
5.	Konsultowanie polityki z pracownikami	– Kierownicy komórek organizacyjnych
6.	Ustanowienie polityki bezpieczeństwa informacji	– Zarząd

Lp.	Zadanie do wykonania	Odpowiedzialne komórki (osoby)
7.	Opublikowanie polityki bezpieczeństwa informacji	– Pełnomocnik ds. wdrażania systemu ZBI
8.	Określenie propozycji celów ogólnych systemu ZBI	– Kierownicy jednostek organizacyjnych – Pełnomocnik ds. wdrażania systemu ZBI
9.	Ustalenie i zatwierdzenie celów ogólnych systemu ZBI	– Najwyższe kierownictwo – Kierownicy jednostek organizacyjnych
10.	Określenie planów i celów szczegółowych związanych realizacją celów ogólnych oraz usuwaniem stwierdzonych podczas analizy ryzyka niedociągnięć	– Kierownicy jednostek organizacyjnych przy współpracy z pozostałymi pracownikami
11.	Opracowanie programu kampanii informacyjnej dot. wdrożenia systemu	– Pełnomocnik ds. wdrażania systemu ZBI
12.	Przeprowadzenie kampanii informacyjnej dot. wdrożenia systemu	– Dział szkoleń
13.	Opracowanie programów i przeprowadzenie szkoleń dot. zagadnień związanych z funkcjonowaniem systemu ZBI dla całego personelu przedsiębiorstwa	– Pełnomocnik ds. wdrażania systemu ZBI Dział szkoleń
14.	Opracowanie szczegółowych procedur i metod postępowania	– Pełnomocnik ds. wdrażania systemu ZBI – Główny specjalista ds. BI
15.	Wdrażanie procedur i metod postępowania	– Użytkownicy procedur
16.	Wyznaczenie osób do prowadzenia auditów wewnętrznych systemu ZBI	– Pełnomocnik ds. wdrażania systemu ZBI
17.	Zorganizowanie i przeprowadzenie szkoleń auditorów wewnętrznych systemu ZBI	– Dział szkoleń
18.	Opracowanie procedury auditowania systemu ZBI	– Pełnomocnik ds. wdrażania systemu ZBI
19.	Przeprowadzenie auditu wewnętrznego systemu ZBI	– Pełnomocnik ds. wdrażania systemu ZBI
20.	Podsumowanie wyników z przeprowadzonego auditu wewnętrznego systemu	– Pełnomocnik ds. wdrażania systemu ZBI
21.	Formalne zakończenie wdrażania systemu (podpisanie protokołu odbioru)	– Prezes zarządu

Źródło: Opracowanie własne na podstawie wyników przeprowadzonych badań

4. Podsumowanie

Innowacje są elementarnym czynnikiem determinującym rozwój przedsiębiorstwa. Z kolei firmom, które nie wdrażają innowacji grozi stagnacja oraz pozostanie w tyle za konkurencją. Wdrażając innowacje przedsiębiorstwo może skutecznie reagować na wszelkie zmiany zachodzące na rynku, odpowiadając na potrzeby swoich odbiorców. Osiągnięcie oczekiwanych korzyści, płynących z wprowadzanych zmian wymaga

zaangażowania jednostki w poszczególne etapy procesu innowacyjnego, tj. powstanie pomysłu na innowację, jej opracowanie, wdrożenie, promocję i sprzedaż na rynku, dyfuzję oraz dalszy rozwój w czasie [21]. Stąd też podjęcie rozważań w zakresie identyfikacji uwarunkowań wdrażania innowacji jest potrzebne i uzasadnione.

Innowacje mogą być oceniane jako nowe rozwiązania w odniesieniu do przedsiębiorstwa bądź gospodarki regionalnej, krajowej lub międzynarodowej. W niniejszej publikacji innowacja traktowana jest jako wprowadzenie nowego z punktu widzenia przedsiębiorstwa systemu zarządzania bezpieczeństwem informacji, który zapewni skuteczną ochronę najważniejszych ich aktywów oraz pozwali na osiągnięcie wielu wymiernych korzyści. Zaliczyć do nich można m.in.: zgodność z wymaganiami prawnymi, ochronę interesów organizacji, jej partnerów biznesowych i klientów, wzrost świadomości pracowników, usprawnienie sytemu komunikacji w firmie, a przez to zmniejszenie ryzyka związanego z ujawnieniem, modyfikacją lub utratą informacji, poprawę wiarygodności organizacji jako zaufanego partnera biznesowego, a także wzrost konkurencyjności na rynku. Wszystkie wskazane elementy w sposób pośredni bądź bezpośredni przekładają się na pozytywny efekt ekonomiczny (zysk), stanowiący główny cel innowacji.

Bariery występujące podczas wdrażania innowacji można podzielić na trzy zasadnicze grupy: bariery związane z zarządzaniem, bariery finansowe oraz bariery związane z czynnikiem ludzkim (personelem).

Bariery związane z czynnikiem zarządczym dotyczą przede wszystkim braku:

- długookresowej strategii działania organizacji;
- zindywidualizowanej strategii wdrażania innowacji i pobudzania do zmian;
- mierzalnych celów przedsiębiorstwa;
- zdefiniowanych procedur postępowania (w tym określenia ról i zakresu odpowiedzialności).

Bariery finansowe wiążą się przede wszystkim z ograniczonymi zasobami finansowymi, przeznaczonymi na realizację określonego przedsięwzięcia.

Z kolei wśród barier wynikających z czynnika ludzkiego, do najważniejszych należą:

- niedostateczne zmotywowanie pracowników;
- bariery mentalnościowe kadry zarządzającej oraz pozostałych pracowników;
- brak wystarczających kwalifikacji kadry zarządzającej oraz personelu wykonawczego;
- brak odpowiedniej liczby pracowników;
- brak odpowiednich kanałów komunikacyjnych wewnątrz przedsiębiorstwa.

Literatura

1. Schumpeter J.A., Teoria rozwoju gospodarczego, PWN, Warszawa 1960.
2. Jasiński A.H., Innowacje i polityka innowacyjna, Uniwersytet w Białymstoku, Białystok 1997.
3. Niedzielski P, Rychlik K., Innowacje i Kreatywność, Uniwersytet Szczeciński, Szczecin 2006.
4. Oslo Manual. Guidelines for Collecting and Interpreting Technological Innovation Data, 3rd Edition, OECD/Eurostat, Paris 2005.
5. Grajewski P., Koncepcja struktury organizacji procesowej, TNOiK, Toruń 2003.
6. Penc J., Strategie zarządzania. Strategie dziedzinowe i ich realizacja, zintegrowane zarządzanie strategiczne, Placet, Warszawa 1995.

7. Srzednicki A., Sokołowicz W., ISO – system zapewnienia jakości, C.H. Beck, Warszawa 2000.
8. Bartnicki M., Jak kształtować przebieg zmian organizacyjnych, Personel, 1998, nr 2.
9. Bartnicki M., Przełamywanie oporów. Jak kształtować przebieg zmian organizacyjnych?, Personel, 1998, nr 3.
10. Bartnicki M., Zarządzanie zmianą w przedsiębiorstwie, AE, Katowice 1998.
11. Grouard B., Meston F., Kierowanie zmianami w przedsiębiorstwie. Jak osiągnąć sukces?, Poltext, Warszawa 1997.
12. Brzeziński M. (red.), Zarządzanie innowacjami technicznymi i organizacyjnymi, Difin, Warszawa 2001.
13. Kożusznik B., Zachowania człowieka w organizacji, PWE, Warszawa 2002.
14. McKenna E., Beech N., Zarządzanie zasobami ludzkimi, Gebethner & Ska, Warszawa 1997.
15. Stabryła A., Podstawy zarządzania firmą, PWN, Warszawa 1995.
16. Wołowski F., Zawiła Niedźwicki J., Bezpieczeństwo systemów informacyjnych, edu – Libri, 2015.
17. Knosala R., Boratyńska – Sala A., Juryczyk – Bunkowska M., Zarządzanie innowacjami, PWE, Warszawa 2014.
18. Sikora T. (red.), Zarządzanie jakością według normy ISO serii 9000:2000, AE, Kraków 2005.
19. Bagiński J., Strategia zmian, Ekonomika i Organizacja Przedsiębiorstwa 1995, nr 10.
20. Mielczarek M., Schody do nieba, czyli etapy rozwoju grupy zadaniowej, Przegląd Organizacji 1996, nr 11.
21. Janosz W., Kozioł K., Determinanty działalności innowacyjnej przedsiębiorstw, PWE, Warszawa 2007.

Mgr inż. Michał PAŁĘGA
Dr hab. inż. Marcin KNAPIŃSKI, prof. PCz.
Dr Wiesław KULMA
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa
Politechnika Częstochowska
42 – 201 Częstochowa, Dąbrowskiego 69
tel./fax: (0-34) 325 07 90
e-mail: mpalega@wip.pcz.pl
knap@wip.pcz.pl
wkulma@wip.pcz.pl